UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA INDUSTRIAL

"PROPUESTA DE UN SISTEMA DE GESTIÓN DEL MANEJO Y SEGURIDAD DE LA INFORMACIÓN BAJO LAS NORMAS INTERNACIONALES ISO 27000 PARA LA COMISIÓN EJECUTIVA HIDROELÉCTRICA DEL RIO LEMPA, CEL."

PRESENTADO POR:

MARIO JOSÉ AGUILA PORTILLO

KEWIN ULISES CRUZ REYES

JUAN CARLOS HERNÁNDEZ VILLACORTA

PARA OPTAR AL TÍTULO DE:

INGENIERO INDUSTRIAL

CIUDAD UNIVERSITARIA, NOVIEMBRE DE 2009

UNIVERSIDAD DE EL SALVADOR

RECTOR :

MSc. RUFINO ANTONIO QUEZADA SÁNCHEZ

SECRETARIO GENERAL :

LIC. DOUGLAS VLADIMIR ALFARO CHÁVEZ

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO :

ING. MARIO ROBERTO NIETO LOVO

SECRETARIO :

ING. OSCAR EDUARDO MARROQUÍN HERNÁNDEZ

ESCUELA DE INGENIERÍA INDUSTRIAL

DIRECTOR :

ING. OSCAR RENÉ ERNESTO MONGE

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA INDUSTRIAL

Trabajo de Graduación previo a la opción al Grado de:

INGENIERO INDUSTRIAL

Título :

"PROPUESTA DE UN SISTEMA DE GESTIÓN DEL MANEJO Y SEGURIDAD DE LA INFORMACIÓN BAJO LAS NORMAS INTERNACIONALES ISO 27000 PARA LA COMISIÓN EJECUTIVA HIDROELÉCTRICA DEL RIO LEMPA, CEL."

Presentado por :

MARIO JOSÉ AGUILA PORTILLO
KEWIN ULISES CRUZ REYES
JUAN CARLOS HERNÁNDEZ VILLACORTA

Trabajo de Graduación Aprobado por :

Docentes Directores :

ING. DOLORES CARLOS ALEGRÍA

ING. OSCAR RENÉ ERNESTO MONGE

San Salvador, Noviembre de 2009.

Trabajo de Graduación Aprobado por:

Docentes Directores :

ING. DOLORES CARLOS ALEGRÍA

ING. OSCAR RENÉ ERNESTO MONGE

AGRADECIMIENTOS

Como grupo queremos dar nuestros agradecimientos generales con todos los involucrados en la realización de este trabajo de graduación, luego damos agradecimientos individuales de lo que nos nace de lo profundo de nuestros corazones.

A **DIOS TODOPODEROSO** que nos ha dado la vida y nos hace crecer en su amor cada día, que nos concedió la inteligencia y nos condujo a lo largo de la realización de nuestro proyecto, protegiéndonos y consolándonos. Y concediéndonos el ánimo y la fuerza para seguir adelante.

A **Nuestra Familias,** que han sido nuestro soporte emocional, físico y económico, dándonos todo lo necesario para culminar con éxito nuestra formación profesional y el Trabajo de Graduación.

A nuestros **docentes asesores,** que nos orientaron en una forma muy profesional, nos brindaron la confianza para avanzar en el trabajo y por creer en nosotros.

A **CEL,** por concedernos la oportunidad de efectuar la tesis en tan prestigiosa Institución, y por su colaboración tan generosa con nosotros.

Al Personal de la **Escuela de Ingeniería Industrial**, que nos formaron profesionalmente en el área de ingeniería industrial.

A todos ellos les estamos infinitamente agradecidos, y esperamos que Dios les recompense todo el bien que han hecho por nosotros.

Juan Hernández,
Kewin Cruz,
Mario Águila

Agradezco en primer lugar a DIOS, por iluminar mi camino a lo largo de mis años de estudios, brindándome la inteligencia y discernimiento necesarios para superar los diversos retos que la culminación de mi carrera presento.

A mis amados PADRES:

A ti mama que siempre me has brindado tu amor incondicional, tu ternura y animo en los momentos difíciles, gracias mama por estar siempre a mi lado.

A mi papa quien siempre me ha brindado sus sabios consejos a lo largo de mi vida, por dedicarme tiempo, por brindarme sus conocimientos y experiencias que sabré capitalizar a largo de mi vida profesional, por motivarme y apoyarme incondicionalmente, gracias papa siempre llevare en mi corazón todas tus enseñanzas.

Gracias padres por todo lo que soy, pues ustedes me han sabido educar, quiero que sepan que este logro se los dedico y que los amo con todo mi corazón

A mis Hermanos:

Javier, Alexis y Aida por darme su cariño y su apoyo incondicional, siempre han estado a mi lado apoyándome, brindándome su valioso tiempo y siempre que los he buscado siempre me han sabido entender.

A mis amigos:

Mario y Kewin, por todo este tiempo que hemos trabajado con mucho esfuerzo y por darnos apoyo mutuamente, Gracias Mario por brindarnos las puertas de tu casa para poder trabajar en la Tesis, de igual forma quiero agradecer a tu familia por ser tan amables y por todo el apoyo brindado. Quiero que sepan que los considero mis amigos, mis hermanos y que siempre podrán confiar y contar conmigo no importando las circunstancias.

En fin, no alcanzarían las palabras para agradecer a todas las personas que me han ayudado para alcanzar esta meta en mi vida solo pido a Dios que sepa recompensar cada uno de los buenos actos en sus vidas, siempre los llevo en mis oraciones.

JUAN CARLOS HERNANDEZ VILLACORTA

Son tantas personas a las cuales debo parte de este triunfo, de lograr alcanzar mi culminación académica, la cual es el anhelo de todos los que así lo deseamos.

Definitivamente, Dios, mi Señor, mi guía, mi Proveedor, mi Fin Ultimo; sabes lo esencial que has sido en mi posición firme de alcanzar esta meta, esta alegría, que si pudiera hacerla material, la hiciera para entregártela, pero a través de esta meta, podré siempre de tu mano alcanzar otras que espero sean para tu Gloria.

Mis padres, por darme la estabilidad emocional, económica, sentimental; para poder llegar hasta este logro, que definitivamente no hubiese podido ser realidad sin ustedes. GRACIAS por darme la posibilidad de que de mi boca salga esa palabra…FAMILIA. Gracias por creer en mí. Serán siempre mi inspiración para alcanzar mis metas, por enseñarme que todo se aprende y que todo esfuerzo es al final recompensa. Tu esfuerzo, se convirtió en tu triunfo y el mío.

A mi novia y futura esposa que siempre ha estado conmigo durante toda esta etapa importante, gracias por enseñarme que lo que realmente cuenta en las personas es la voluntad, el deseo y las ganas de superarse gracias por enseñarme que cualquier cosa se puede alcanzar cuando luchas por ella gracias por demostrarme todas las cosas buenas que soy capaz de realizar cuando me las propongo en fin, gracias por haber creído en mi y nunca perder la esperanza que llegaría a lograr una de mis metas más soñadas, por eso este trabajo también te lo dedico a ti.

A mis hermanos porque siempre ante cualquier obstáculo estuvieron presentes para brindarme la mano y solucionar los problemas que me agobiaron.

A Chepe Luis, Nelly, Juan Pablo, Alex, Ricardo, Irving, Wen, Mauricio, Laura, Martha, a todos ustedes simplemente gracias por marcar mi vida de momentos tan preciados.

A mis amigos y compañeros de tesis Mario y Juan por que en los momentos más difíciles siempre ante cualquier cosa prevaleció la sinceridad y la amistad que nos permitió lograr todo cuanto quisimos

A todos mis amigos pasados y presentes; pasados por ayudarme a crecer y madurar como persona y presentes por estar siempre conmigo apoyándome en todo las circunstancias posibles, también son parte de esta alegría, LOS RECUERDO.

KEWIN ULISES CRUZ REYES

El tiempo está a favor de los pequeños de los desnudos, de los olvidados el tiempo está a favor de buenos sueños y se pronuncia a golpe saturado. El Salvador y el tiempo la suma del coraje se han convertido en sol violento y han emprendido claro viaje…

Nunca me imagine llegar a este momento, pero siempre lo soñé, se que el estar escribiendo estas palabras es todo un honor y privilegio que la mayoría de los jóvenes de este país no alcanzan a cumplir por razones socio-económicas, para ellos va mi respeto y admiración.

En primer lugar quiero agradecer infinitamente a DIOS, por haber derramado su gracia y misericordia sobre este aun indigno siervo, fue su mano y su apoyo incondicional lo que me trajo hasta aquí, a El sea toda la gloria y honra por todos los tiempos.

¡Que todos los conocimientos y tecnología estén al servicio de quien mas lo necesita!

Así mismo quiero agradecer a los integrantes de mi grupo 3:16 por brindarme su apoyo, sus muestras de amino y cariño, por haber tenido la paciencia y comprensión por mis ausencias, compañer@s de lucha solo me queda decir GRACIAS!!

En segundo lugar quiero agradecer a mi familia, mi mamá Juanita, mi papi Mario, a El dedico mi esfuerzo y mi entrega, mi hermano Juan Ramón, mi hermana Marianela, mi abuelita Marina, mi tía Carmen, mis primo Víctor José, por supuesto a Marinita y a mi tío Meme, gran tipo, a ellos y ellas que son las piezas fundamentales de mi vida que me dieron el soporte durante todos estos años, que estuvieron allí respaldándome, apoyándome, enseñándome y protegiéndome, forjando mi carácter dándome esa base para lograr la estabilidad emocional, física, mental y por supuesto espiritual llena de valores y experiencias y que ayudaron a construir lo que ahora soy, amada familia infinitamente ¡GRACIAS!, desde el corazón los amo…

Así mismo quiero agradecer a mi novia Karen, por estar allí desde otra trinchera apoyándome en los momentos difíciles, por soportar muchas veces mis enojos, frustraciones y malos ratos, por tener la paciencia necesaria y compresión para escucharme y decir una palabra de aliento o simplemente callar y abrazarme, han sido muchas las aventuras que hemos emprendido juntos, aventuras que nos han llevado a ser mejor seres humanos cada día, mi gorda, mi bb, gracias por tu amor incondicional…

Y por supuesto a mis compañeros de lucha por haber estado conmigo desde el principio hasta hoy: Kewin y Juan mis compañeros de tesis que sin dudar ni un momento fueron el apoyo idóneo en este gran esfuerzo que decidimos emprender, Gracias amigos, Juan Pablo, Ricardo, Oscar, a Irving, a Wen, Eder, Leonardo, a Emerson, Néstor y tantos otros y otras que fueron parte de muchas aventuras que pasamos y que hoy a tod@s los recuerdo y agradezco… hasta siempre compañeros, amigos, hermanos….

MARIO JOSÉ AGUILA PORTILLO

ÍNDICE

INDICE DE FIGURAS

INDICE DE GRAFICOS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad, cada vez mas empresas están implementando estrategias dirigidas a preservar y manejar sus activos de información esto se puede evidenciar ya que parte de su presupuesto está siendo destinado a la gestión de la seguridad de la información.

El concepto de seguridad ha variado, acuñándose un nuevo concepto: "seguridad gestionada", que ha absorbido al de "seguridad informática"; para gestionar la seguridad de la información de una entidad se debe partir de una premisa fundamental: **"la seguridad absoluta no existe".**

Las medidas que comienzan a tomar las empresas giran en torno al nuevo concepto de gestión de la seguridad de la información. Éste tiene tres vertientes: técnica, legal y organizativa, es decir un planteamiento coherente de directrices, procedimientos y criterios que permiten, desde la dirección de las empresas, garantizar la evolución eficiente de la seguridad de los sistemas de Información, la organización afín y sus infraestructuras.

Si hablamos de las condiciones generales mundiales en cuanto a la seguridad de la información encontramos que, habrán instituciones en las cuales todo lo concerniente al tema se toma con la debida objetividad del caso, que obedece a la seriedad de los activos que son manejados por la organización tales como transacciones financieras datos de mercado entre otros.

Teniendo en cuenta que esta información que se maneja en las instituciones de manera natural y como parte de los procesos y que no necesariamente es manejada en medios electrónicos; es de gran valor y pocas veces se toman las medidas necesarias para garantizar que esta información cumple con estándares seguros, es por eso que surge en el ámbito mundial como producto de estas necesidades una familia de normas (ISO 27001:2005) encaminadas a generar los niveles mínimos que cualquier institución a nivel mundial debe poseer para poder garantizar que la información que se genera es segura.

CEL como una de las instituciones más solidas y de prestigio en el país ha determinado que la información que se genera y manipula en sus procesos claves y de apoyo, es de gran valor tanto para sus clientes como para su propio funcionamiento; encontrando la necesidad de aplicar eficientes medidas de seguridad y controles sistemáticos capaces de garantizar la integridad, confiabilidad, utilidad, disponibilidad, autenticidad y confidencialidad de la misma.

Tomando en cuenta el contexto antes mencionado y la problemática de CEL, en el siguiente documento se presenta una propuesta de Sistema de Gestión que tiene por objetivo garantizar el adecuado manejo de la información bajo las medidas de seguridad necesarias.

OBJETIVOS

GENERAL:

- Elaborar una propuesta de un Sistema de Gestión del Manejo y la Seguridad de la Información bajo la Norma Internacional ISO 27000 para La Comisión Ejecutiva Hidroeléctrica del Río Lempa CEL.

ESPECÍFICOS:

- Conocer y documentar la situación actual que posee la Comisión Ejecutiva Hidroeléctrica del Rio Lempa en cuanto al manejo y seguridad de la información.

- Diseñar un Sistema de Gestión para el manejo y Seguridad de la Información (SGSI) bajo la métrica de la norma ISO 27001:2005 para la Comisión Ejecutiva hidroeléctrica del Rio Lempa (CEL).

- Determinar la factibilidad económica financiera del sistema de Gestión de Seguridad de la Información así como establecer la Administración de la implementación y posterior operación del mismo.

- Proporcionar al proceso de Gestión Integrada una herramienta adecuada para la gestión y seguridad de la información que se adhiera de manera natural a los sistemas de gestión bajo la óptica ISO que ya posee la Comisión.

- Proporcionar a través del Sistema de Gestión de Seguridad de la Información basado en el ciclo PHVA los insumos necesarios parar iniciar el proceso de certificación bajo la norma internacional ISO 27000.

ALCANCE

- Con el desarrollo del trabajo de graduación se pretende llegar hasta la creación de una propuesta para la implementación de un Sistema de gestión del manejo y seguridad de la información, bajo las normas internacionales ISO 27000.

- El trabajo de graduación tendrá un alcance institucional, la propuesta será diseñada para La Comisión Ejecutiva Hidroeléctrica del Rio Lempa, (CEL), únicamente en sus oficinas centrales; en cuadro áreas específicamente.

    a. Gerencia de producción. (Proceso de producción).

    a. Unidad de comercialización (Proceso de Comercialización).

    b. Unidad informática Institucional (Proceso de Gestión de la Información (solo para los dos procesos anteriores).

    c. Desarrollo Humana (Proceso de recursos Humanos)

  Estas áreas son las responsables de generar los procesos claves o de negocios[1] que están directamente relacionados con el giro o razón económica de La Comisión.

[1] Ver descripción de Procesos claves y Procesos de apoyo, en Sección B, Capitulo I

LIMITACIONES

- No existe un estudio previo o investigación previa relacionada con el tema a nivel académico.

- A nivel empresarial o institucional, solo existe una organización que ha desarrollado el proceso de implementación de las normas ISO 27000, esto restringe la posibilidad de desarrollo una investigación de campo a nivel institucional.

JUSTIFICACIÓN

Para CEL, La información es un activo vital para el éxito y la continuidad en el mercado hidroeléctrico. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.
Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.
Actualmente en CEL existe una necesidad muy grande de asegurar la información por medio del desarrollo e implantación de un SGSI que garanticen la integridad, confiabilidad y disponibilidad de la misma.

De esta forma es como se nos presenta la oportunidad de desarrollar el SGSI como trabajo de graduación, dicha propuesta nace a través de un acercamiento con el Jefe de la Unidad de Gestión Integrada de La Comisión, en la cual él nos expuso la necesidad del SGSI y decidimos afrontar el reto a pesar de que en la actualidad ninguna empresa del sector privado y público (a excepción del Ministerio de Hacienda que se encuentra en fase de diseño del SGSI) ha decidido desarrollar un SGSI a través de las normas internacionales ISO 27000.
En dicha plática él nos expuso todo el panorama que se pretende alcanzar y nos enfatizo desarrollar el SGSI en los procesos claves de la Comisión los cuales son:

i. Proceso de Producción
ii. Proceso de Comercialización, y
iii. Proceso de gestión de la información.
iv. Proceso de Desarrollo Humana

En términos generales, las organizaciones y sus sistemas, procesos y procedimientos enfrentan amenazas de seguridad de un amplio rango de fuentes como por ejemplo espionaje, sabotaje, vandalismo, fuego, terremoto o inundación, etc. Lo cual nos presenta claramente la obligatoriedad de las organizaciones en preservar la integridad de la información de manera que todo aquello que este manejado por la organización sea correcto y no esté distorsionado por ninguna variable ajena al sistema, también debe de preservarse la confiabilidad en el sentido que los datos sean manejados por las personas correctas y necesarias. Además de los dos puntos tocados anteriormente se debe garantizar la disponibilidad de la información en el momento y en el lugar correcto, lo que llevara a mantener los niveles de competitividad, rentabilidad, conformidad legal o imagen institucional, necesarios para lograr los objetivos de la institución y asegurar los beneficios.

Mediante la realización de la propuesta se tendrá como beneficiario directo La Comisión Ejecutiva Hidroeléctrica del Río Lempa, El Salvador (CEL) la cual podrá aprovechar mejor sus recursos y

generar mejores beneficios lo que indirectamente tiene como beneficiarios a los usuarios de los servicios prestados por la institución, además de sentar un precedente y una base para las certificaciones de las instituciones gubernamentales que por las exigencias de un mundo cada vez más globalizado e inmerso en la información demanda que los activos intangibles sean cada vez más protegidos de manera que garanticen la calidad de estos en los aspectos importantes antes mencionados como son integridad, confiabilidad y disponibilidad y así poder prestar mejores servicios elevando la calidad de vida de la población.

El contexto internacional como el nacional hacen más corta la brecha entre la seguridad y la inseguridad dado que la incertidumbre hoy en día por los avances tecnológicos los tipos de información los métodos de recolección los procesos en el manejo de información generan a las organizaciones la obligación de salvaguardar sus tesoros que a la vez tiene que estar al alcance de las personas correctas para su buen uso, es por este sentido que un sistema de gestión de la seguridad de la información se vuelve fundamental en las organizaciones, cabe destacar que La ISO tiene ya mucho tiempo trabajando en el esquema para la certificación de su norma dedicada a los sistemas de información la que fue publicada y oficializada en el año 2007, por tanto y como consecuencia lógica de la modernidad de la norma en El Salvador no se cuenta con ningún estudio previo acerca de la implantación de esta norma ni a nivel de investigación universitario ni en instituciones públicas o privadas, cabe mencionar que la única institución nacional que se encuentra implementándola de momento sin su consecución aun es El Ministerio de Hacienda el cual de momento lo realiza de manera departamental y no en toda la organización como tal.

IMPORTANCIA

La importancia de realizar una propuesta de una plataforma para la implementación de la norma ISO 27000 surge de la necesidad de la mejora continua para la institución (CEL), así como también lograr un mejor funcionamiento y eficiencia en el manejo del recurso o activo intangible de la empresa que es la información.

Sobre la base de la información recopilada, se puede identificar la importancia de la realización del estudio, respondiendo a la siguiente pregunta:

¿Por qué es relevante el estudio?
Se identificaron los siguientes aspectos que dan respuesta a la pregunta:

- ✓ Por las cualidades y características de la información o activos que maneja La Comisión, las cuales son de tipo financiero, legales, adquisiciones y de personal; es de suma importancia establecer una estrategia de seguridad, que combata y disminuya las vulnerabilidades y amenazas de estos.
- ✓ La falta de protocolos de Gestión de activos de información hacen de la ISO 27000 un novedoso e innovador Sistema de Seguridad integrado, de reciente aprobación, en el cual se toman en cuenta todos aquellos factores que intervienen en la manipulación de la información (Sistemáticos, Tecnológicos, Culturales y Económicos).
- ✓ Actualmente no hay documentación que respalde la existencia de estudios previos, no hay mucha información con respecto a esta norma, por lo que este estudio contribuirá como estudio pionero al enriquecer la documentación y por consiguiente el conocimiento.
- ✓ En base a la investigación realizada en la Comisión sobre los siguientes aspectos en función de la seguridad de información, se pueden evidenciar los siguientes datos relevantes:
    - o Decisiones por año: decisiones por año 316; Con la implantación del SGSI se podrá disminuir los retrasos en las tomas de decisiones y cumplir en el 98% de los casos con los tiempos establecidos por el reglamento legal interno.
    - o Transacciones de documentos confidenciales: 821 por año, Reducir en un 46% la excesiva circulación de documentos e información de uso exclusivo; en manos, procesos y áreas que no sean de su competencia.
    - o Transacciones mensuales sin retorno: 86 por mes, Reducir el 18.2% de las transacciones mensuales queda sin retorno a sus emisores de préstamos, lo cual hace importante establecer protocolos de actuación que normen dicho procesos, los cuales serán determinados mediante un Sistema de Gestión adecuado.
- ✓ La norma ISO 27000 en sus anexos muestra la relación entre las normas ISO 9001 y 14001 por tanto, para CEL, institución que ya cuenta con tres de los sistemas de gestión más reconocidos

en el mundo como lo son los dos anteriores y OSHAS-18001 implantados e integrados, la posibilidad para el desarrollo de la norma ISO 27000 es sumamente favorable ya que pósese una estructura organizativa y alta gerencia familiarizada con los sistemas de gestión y sus beneficios así también se cuenta con objetivos gerenciales ya establecidos que buscan eficientizar los recursos para brindar un mejor servicio.

CAPITULO I: MARCO CONTEXTUAL DE CEL

A. GENERALIDADES DE CEL

1. Misión, Visión y Principios Básicos

a. *Visión*

Ser líderes en el aprovechamiento de energías renovables, creando bienestar económico y social para los salvadoreños.

b. Misión

Aprovechar y conservar los recursos energéticos renovables, contribuyendo al bienestar económico, social y ambiental de los salvadoreños.
Mejorar continuamente la calidad de nuestros productos, las competencias del personal y la eficacia de nuestros sistemas.

c. Principios Básicos

- Ser líderes en el aprovechamiento de energías renovables.
- Crear bienestar económico, social y ambiental para los salvadoreños, y,
- Mejorar continuamente la calidad de de nuestros productos, competencias del personal y la eficacia de nuestros sistemas.

2. Descripción General del Producto

El producto que desarrolla CEL es: Energía Eléctrica: **Kilovatios-hora (kWh).**
Otros productos:

1. Reserva para Regulación Primaria de Frecuencia;
2. Regulación Secundaria de Frecuencia (Control Automático de Generación);
3. Potencia Reactiva; Reserva Fría; y,
4. Arranque en Cero Voltaje.

3. Estructura Organizativa de CEL

La Comisión Ejecutiva Hidroeléctrica del Rio Lempa – CEL, es regida por La Junta Directiva, Presidencia y Dirección Ejecutiva. La Presidencia cuenta por el apoyo del Departamento de Auditoría General Interna, La Dirección Ejecutiva a su vez cuanta con el apoyo de seis Unidades las

cuales son; Unidad Comercial, Unidad de Estudios y Gestión corporativa, Unidad de Gestión Integrada[2], Gerencia Legal, Unidad de Adquisiciones y Contrataciones Institucionales, La Unidad de Comunicaciones.

Todo este equipo anterior de Unidades y Direcciones tiene como fin Administrar las actividades entre La Coordinación Técnica, Coordinación de Proyectos y Coordinación Administrativa Financiera.
La Coordinación Técnica cuenta con un Área de Asesoría la cual es llamada Unidad Ambiental y con una Gerencia de Producción y 5 Unidades operativas a su cargo; La Coordinación de Proyectos cuenta con dos Unidades asesoras que son Unidad de Ejecución de Proyectos y la Unidad de Gestión y Control de Proyectos; Esta coordinación cuenta con una Gerencia de Ingeniería y 3 Departamentos a su cargo; La Coordinación Administrativa Financiera cuenta con 5 Unidades Asesoras como lo son Unidad de Riesgo, Unidad de Informática Institucional, Unidad de Desarrollo Humano, Unidad de Servicios Generales y Unidad Administrativa, esta coordinación Cuenta con una Gerencia Financiera y 3 Departamentos a su cargo.

A continuación se presenta el organigrama institucional de CEL:

[2] Para mayor detalle Ver Anexo 1: Sistema de Gestión Integrada

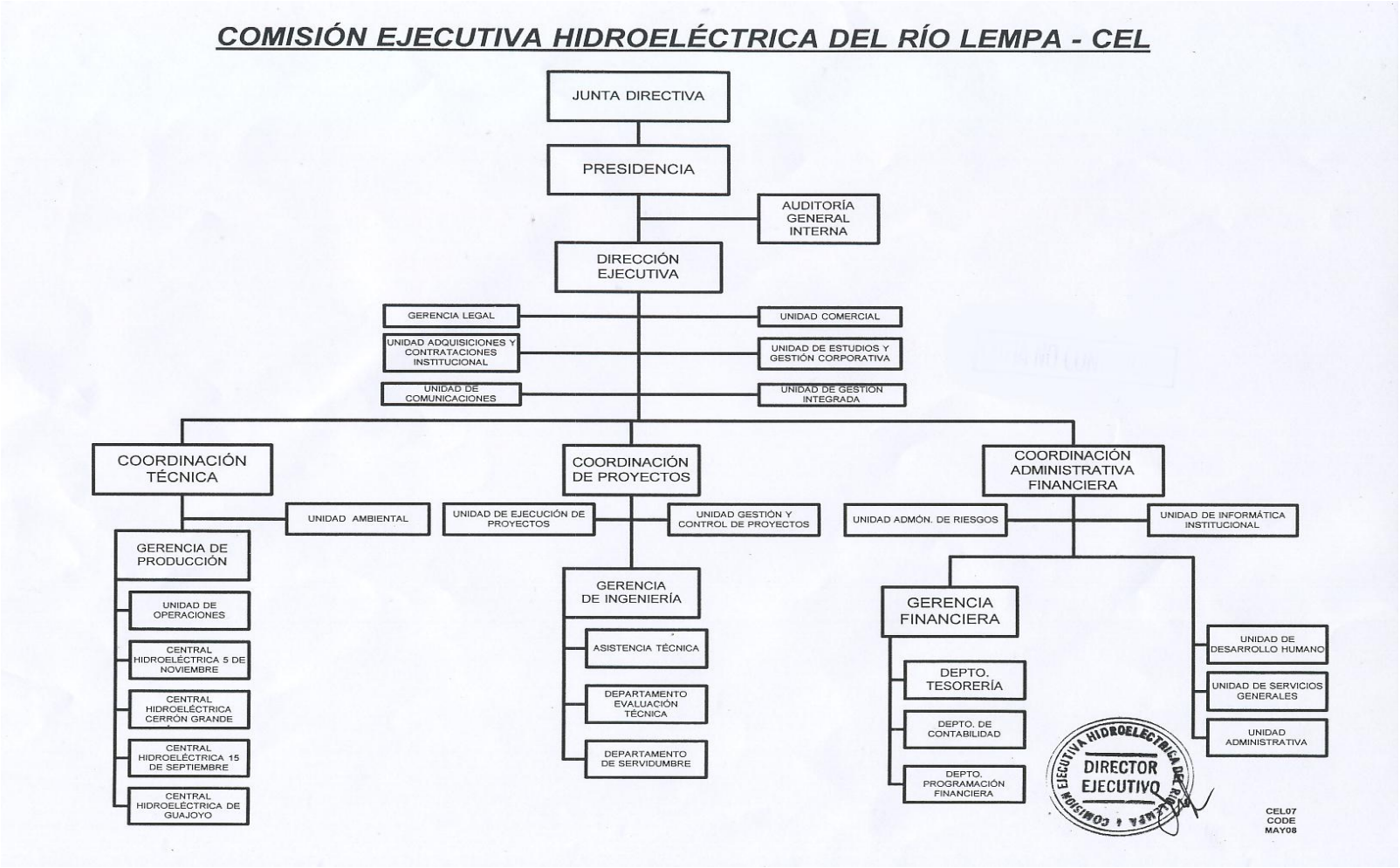


Figura 1: Estructura Organizativa de CEL

4. Estructura de las Unidades claves de CEL

a. Gerencia de Producción

La Gerencia de Producción cuenta con una Unidad de Operacion es la cual sirve como asesora, esta Gerencia Administra 4 Superintendencias las cuales son la C.H. 15 de Septiembre, C.H. Cerrón Grande, C.H. Guajóyo y C.H. 5 de Noviembre. Cada una de ellas posee como Área Asesora al Área de Bienes y Servicio y 3 Departamentos operativos los cuales son: Depto. Mecánico, Eléctrico y de Operaciones.

A continuación se presenta de manera para el organigrama:

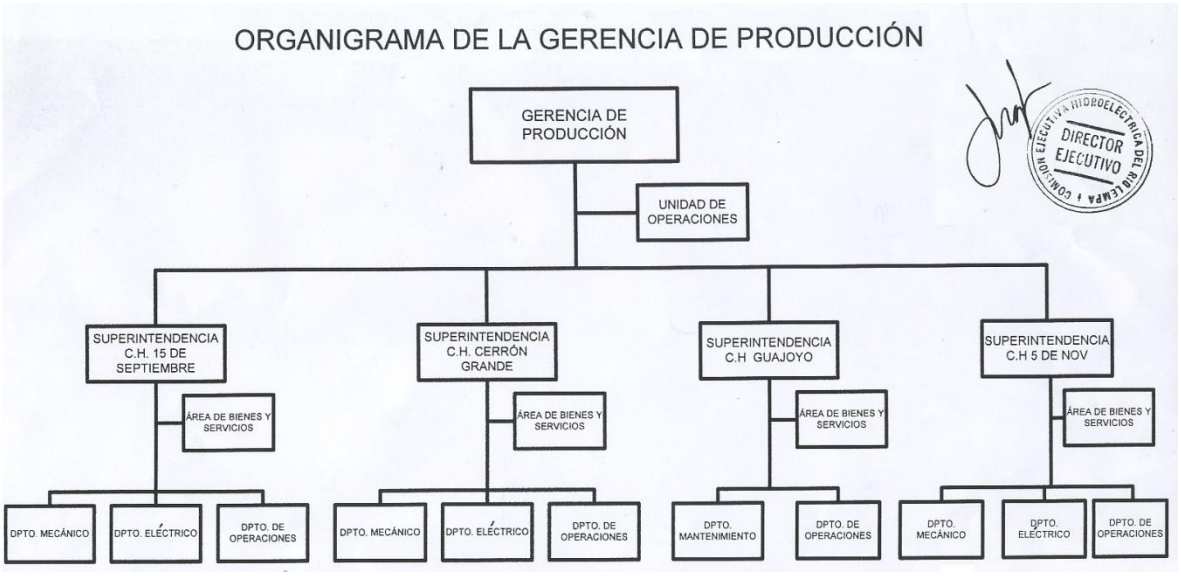


Figura 2: Estructura organizativa del proceso de producción

FUNCIÓN GENERAL

Planificar y conducir las actividades de operación de equipos y mantenimiento de las centrales generadoras de CEL, para la producción de energía eléctrica.

FUNCIONES ESPECÍFICAS

a. Velar por el cumplimiento de las normas técnicas de operación del Reglamento de Operación del Sistema de Transmisión y del Mercado Mayorista.

b. Planificar, coordinar y supervisar los programas de mantenimiento preventivo y correctivo de las centrales generadoras (Plan de Generación).

c. Gestionar para las centrales generadoras la asignación oportuna de recursos humanos, equipos, repuestos, materiales, combustibles y lubricantes necesarios para el desarrollo de las fu iones en las centrales.

d. Diseñar, mantener y mejorar el proceso general de producción hidroeléctrica.

e. Identificar e implementar nuevas tecnologías para la mejora continua de la eficacia de los sistemas, las competencias del personal y la calidad del servicio de las centrales hidroeléctricas.

b. Unidad de Comercialización

Esta unidad no posee organigrama.

FUNCIÓN GENERAL
Ejecutar la política comercial de CEL., de acuerdo con los objetivos institucionales establecidos y las indicaciones de la Dirección Ejecutiva.
FUNCIONES ESPECÍFICAS

a. Elaborar, administrar y ajustar el Plan Anual de Operación.
b. Negociar contratos de compra/venta de energía eléctrica en el mercado nacional e internacional (de corto y largo plazo) con generadores, distribuidores, comercializadores y otros clientes, tomando en cuenta las instrucciones recibidas de la Dirección Ejecutiva.
c. Elaborar y enviar a la Unidad de Transacciones (UT) las ofertas de oportunidad y/o contratos en el mercado mayorista de energía eléctrica y, remitir el pre-despacho publicado por la UT a la Gerencia de Producción.
d. Revisar modificaciones y/o propuestas de documentos, reglamentos u otros, relacionados con el marco legal del mercado mayorista, con el fin de proporcionar observaciones o comentarios comerciales y/o de mercado por parte de la Comisión.
e. Revisar el Documento de Transacciones Económicas (DTE), proporcionado por la UT, con el fin de velar por los intereses comerciales de la Comisión, e informar a la Gerencia Financiera para continuar con el proceso de facturación.
f. Proporcionar visto bueno a la facturación remitida por la Gerencia financiera y asegurar la validez de la información (por compras de energía eléctrica nacional e internacional, CUST, etc.) con el fin de proceder con el trámite de pago.
g. Proporcionar información la Gerencia Financiera para la facturación por: compras y ventas de energía eléctrica en el mercado mayorista, suministro de energía a usuarios finales, desviaciones y otros cobros a favor de CEL.

5. Estructura de las unidades de Apoyo de CEL

a. Unidad de Informática Institucional

La Unidad de Informática Institucional está Compuesta por 3 Aéreas las cuales son: Área de Desarrollo de Sistemas, Área de Administración de Base de Datos y el Área de Mantenimiento y Soporte Técnico.
A continuación se presenta de manera para el organigrama:

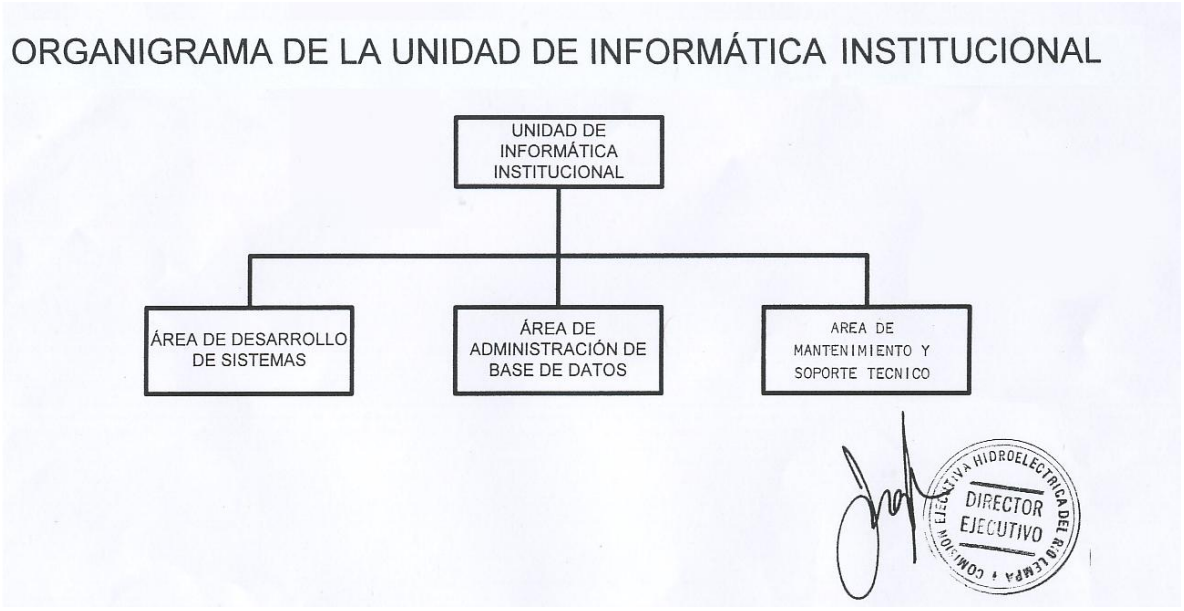


Figura 3: Estructura organizativa del proceso de Informática Institucional

FUNCIÓN GENERAL

Proveer de herramientas apropiadas para la gestión de la información, como soporte a la toma de decisiones.

FUNCIONES ESPECÍFICAS

a. Coordinar el desarrollo, implantación y mantenimiento de los sistemas de información, así como herramientas de gestión, excepto para los modelos matemáticos de optimización y administración de contratos que apoyan los participantes en el mercado eléctrico.

b. Proveer el soporte técnico y coordinar la capacitación de usuarios en el marco de uso de herramientas de informática.

c. Promover el uso legal de software en el ámbito institucional.

d. Velar por la optimización del uso de equipos y sistemas.

e. Administrar las redes y las bases de datos integradas y promover el uso de la comunicación electrónica.

f. Analizar alternativas de contratación de servicios y/o compra de equipos, evaluando estrategias frente a los cambios tecnológicos.

b. Unidad de Desarrollo Humano

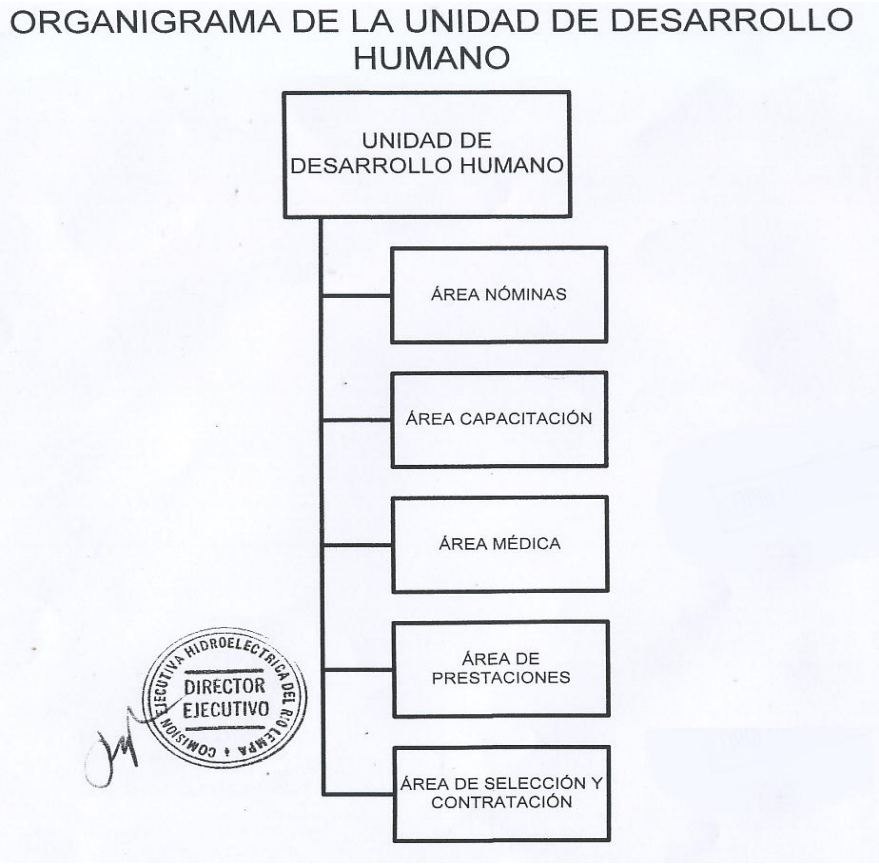


Figura 4: Estructura organizativa del proceso de Desarrollo Humano

FUNCIÓN GENERAL

Planificar, coordinar, dirigir y controlar las actividades relativas a la administración de los recursos humanos y su desarrollo, como procesos de reclutamiento, selección y contratación de personal, remuneraciones, estructura de puestos, capacitación y desarrollo, sistema de prestaciones, clima organizacional y evaluación del desempeño a nivel institucional.

FUNCIONES ESPECÍFICAS

a. Realizar los procesos de reclutamiento, selección, contratación e inducción de personal.
b. Gestionar acciones de personal como ascensos, traslados, renuncias, terminaciones de contratos e incrementos salariales.
c. Administrar y actualizar el sistema salarial y de prestaciones.
d. Administrar el centro recreativo costa CEL.
e. Elaborar planillas de pago (sueldos mensuales, bonificación, aguinaldo y vacaciones).
f. Administrar la elaboración, ejecución y medición de planes de capacitación y desarrollo del personal.
g. Velar y promover actividades para el mantenimiento de un buen clima organizacional a nivel institucional.
h. Administrar el sistema de evaluación del desempeño individual de los empleados.
i. Resguardar y controlar expedientes de personal activo y retirado.
j. Coordinar los servicios de salud proporcionados por los médicos de CEL. en Oficina Central.
k. Realizar gestiones que sean necesarias para mantener las buenas relaciones laborales con los Sindicatos y Gremiales de la Institución.

B. IDENTIFICACIÓN DE LOS PROCESOS DE CEL[3]

Los procesos declarados por la Comisión, son:

PROCESOS DE NEGOCIO (CLAVES): Son los que expresan el objeto y la razón de ser de la institución y que tienen impacto directo en el cliente externo. Son aquellos que directamente contribuyen a realizar el producto o brindar el servicio, en CEL tenemos:

- Proceso de Producción
- Proceso de Comercialización de Energía Eléctrica

PROCESOS DE APOYO: Son los procesos encargados de proveer a la organización de todos los recursos (materiales, humanos y financieros) y crear las condiciones para garantizar el exitoso desempeño de los procesos claves, básicos o fundaméntales de la entidad, en nuestro caso, tenemos:

- Proceso de Facturación y Cobro
- Proceso de Pagos
- Proceso de Administración de Riesgos
- Proceso de Gestión Integrada
- Proceso de Gestión de la Información
- Proceso de Recursos Humanos

[3] Ver Anexo 2: Elaboración, identificación y modificación de procesos

- Proceso de Gestión de Adquisiciones
- Proceso de Gestión Presupuestaria
- Proceso de Servicios Generales
- Proceso de Suscripción, Cumplimiento y Terminación de Contratos
- Proceso de Proyectos

La siguiente tabla presenta una descripción y clasificación de estos procesos:

№	DEPENDENCIA RESPONSABLE	PROCESO	TIPO (de negocio o de apoyo)
1	Gerencia de Producción	Producción	Negocio.
2	Unidad Comercial	Comercialización de Energía Eléctrica	Negocio.
3	Departamento de Tesorería	Facturación y Cobro	Apoyo.
4	Departamento de Tesorería	Pagos	Apoyo.
5	Unidad Administración de Riesgos	Administración de Riesgos	Apoyo.
6	Departamento de Administración de Contratos	Administración de Contratos	Apoyo.
7	Unidad de Adquisiciones y Contrataciones Institucional	Gestión de Adquisiciones	Apoyo.
8	Unidad de Gestión Integrada	Gestión Integrada	Apoyo.
9	Departamento de Programación Financiera	Gestión Presupuestaria	Apoyo.
10	Unidad de Informática Institucional	Gestión de la Información	Apoyo.
11	Unidad de Desarrollo Humano	Recursos Humanos	Apoyo.
12	Unidad de Servicios Generales	Servicios Generales	Apoyo.
13	Unidad de Gestión y Control de Proyectos	Proyectos	Apoyo.

Tabla 1: Descripción y clasificación de los procesos de CEL

1. Descripción de Macro Procesos (PEPSU y Desglose de Procesos con Flujo de Datos)

Conocidos también como procesos claves, ya que estos constituyen el negocio principal de CEL y que son los que abarcan la actividad económica de la institución

a. Proceso de Producción

A continuación se presenta los procedimientos[4] involucrados en el Proceso de Producción.

Dependencia	Código	Nombre del Procedimiento
Gerencia de Producción	PR041 -01	Procedimiento para realizar arranque de Unidad Generadora
	PR041-02	Procedimiento para efectuar Paro de la Unidad Generadora.
	PR041-03	Procedimiento para la variación de potencia de la Unidad Generadora.
	PR041-04	Procedimiento sistema de Alerta temprana por descargas por vertedero.
	PR041-05	Procedimiento para el restablecimiento en condición de cero voltaje
	PR041-06	Procedimiento para realizar la lectura y reporte de medición comercial.
	PR041-07	Procedimiento para la lectura y reporte de variables de generación.
	PR041-08	Procedimiento para la interrogación de relés y análisis de fallas.
	PR041-09	Procedimiento para el monitoreo y registro de datos de operación
	PR041-10	Procedimiento para el monitoreo de la instrumentación de presas.
	PR041-11	Procedimiento para el mantenimiento Preventivo del sistema de aire comprimido.
	PR041-12	Procedimiento para el mantenimiento Preventivo M sistema de bocatoma.
	PR041-13	Procedimiento para el mantenimiento Preventivo del sistema de la turbina.
	PR041-14	Procedimiento para el mantenimiento Preventivo del sistema de suministro de corriente alterna y corriente directa.
	PR041-15	Procedimiento para el mantenimiento Preventivo del Sistema de Excitación del Generador.
	PR041-16	Procedimiento para el mantenimiento Preventivo del Sistema del Generador.
	PR041-17	Procedimiento para el mantenimiento Preventivo del Sistema de protecciones eléctricas.
	PR041-18	Procedimiento para el mantenimiento Preventivo del Sistema de Medición Comercial (Simec).
	PR041-19	Procedimiento para gestión de equipos de protección personal.
	PR041-21	Procedimiento para el mantenimiento Preventivo del Sistema Regulador de Velocidad de la Turbina.
	PR041-22	Procedimiento para el mantenimiento Preventivo del Sistema de

[4] Ver Anexo 3: Elaboración, identificación y modificación de procedimientos y registros.

Gerencia de Producción		Transformador.
	PR041-27	Procedimiento para el mantenimiento Preventivo del Sistema Contraincendios.
	PR041-28	Procedimiento para el mantenimiento Preventivo del Sistema de bombas de achicamiento y sumidero.
	PR041-29	Procedimiento para el mantenimiento Preventivo del Sistema del Servicio Propio.
	PR041-30	Procedimiento para el mantenimiento Preventivo del Sistema de instrumentación.
	PR041-32	Procedimiento para el Mantenimiento Preventivo del Sistema de la planta de emergencia.
	PR041-36	Procedimiento para actividades/trabajos en espacios confinados.
	PR041-37	Procedimiento para trabajos en altura.
	PR041-63	Inspección y análisis de la disponibilidad de recursos en las Centrales Hidroeléctricas de CEL.

Tabla 2: Procedimientos involucrados en el proceso de producción.

Medio Ambiente: Oficinas en buenas condiciones y en un ambiente de seguridad, orden y limpieza (PRA25-17 y 18, PRA21-01, PRO41-123), recursos (PRA25-17,18).

Procesos de apoyo: Presupuesto (PRA38-02); compras (PRA20-02) Riesgos (PRA16-01, 02, 03 y 04). Mantenimientos Preventivo y correctivo (PRO41- de acuerdo al listado maestro)

PROCESO DE PRODUCCION

ENTRADAS (INSUMOS)		
Entradas	Requisitos	Proveedor
Predespacho	.+. Generacion programada por la UT/cumplimiento de parámetros técnicos de cada unidad por parte de la UT .+. Unidad fuera del predespacho	Unidad Comercial
Ordenes en tiempo real	.+. Requerimientos .+. Comportamiento de la demanda .+. Estado de emergencia parcial o completa del sistema.	Unidad de transacciones (U.T.)
Confirmacion de mantenimientos	Numeral 12 " Coordinacion de mantenimientos", del reglamento*.	Unidad Comercial

SUB- PROCESOS
ARRANQUE PRO41-01 PARO PRO 41-02
VARIACIONES DE POTENCIA PRO41-03, 06, 07 Y 10
SERVICIOS AUXILIARES PRO41-03 Y 05

SALIDAS (PRODUCTOS)		
Salidas	Requisitos	Cliente
Energia Electrica	Normas de calidad y Seguridad Operativa. Reglamento del sistema de transmision y del mercado mayorista	Unidad de Transacciones
Reporte diario de produccion.	Variables de Generacion PRO41-07, anexos del 1 al 4	Unidad Comercial
Informe de indisponibilidad/ Solicitud de mantenimiento		.+. Departamento de mantenimiento, electricoy mecanico de las centrales hidroelectricas .+. Unidad Comercial

5

[5] Ver Anexo 4: Herramientas y Técnicas de Ingeniería Utilizadas

Informe diario de operación	Numeral 7.9 del reglamento.*	Unidad Comercial
Proyeccion de niveles	Anualmente o cuando existan modificadores oficiales al mismo	Unidad Comercial

OPERACIÓN DE EMERGENCIA PRO41-05 Y 08

Informe de interrogacion de relés y análisis de fallas	Según lo definido en el procedimiento PRO41-08, anexo 1.2, 2.2, 3.2, y 4.2	Unidad Comercial
Informe de mensual de inyecciones	Según lo definido en el procedimiento PRO41-06, actividad No.9	Unidad Comercial
Mantenimientos mayores	Propuesta del PAMM de unidades generadoras	Unidad Comercial
Datos Operativos de Unidades	De acuerdo a lo establicido en el Reglamento de U.T.	Unidad Comercial

Infraestructura: Edificaciones adecuadas y con los recursos necesarios (PRA25-01, 02, 12, 17, y 18) Seguridad de Presas (PRO41-71), Mantenimiento de Instalaciones (PRO41-64, 65 y 67), alerta temprana (PRO41-04)

Recurso Humano: jefes de departamento, Supervisores, Operadores, Auxiliares de Operador. El detalle de competencias estan detalladas en el Tomo II del Manual de Descripcion de Puestos.

* Reglamento de Operación del Sistema de Transmision y del Mercado Mayorista

Objetivo del proceso: Producir energia electrica para cumplir el plan anual de generacion, manteniendo el indice de disponibilidad mayor o igual al 90% promedio.

INDICE DE MEDICION	FRECUENCIA DE MEDICION	INDICE DE COMPARACION
Indisponibilidad de fallas internas (IFI)	Mensual	Según detalle anexo 1
Indisponibilidad por fallas externas (IPE)	Mensual	
Indisponibilidad por mantenimiento programado (IMP)	Mensual	
Indice de cumplimiento en el mantenimiento (ICM)	Mensual	
Indice de disponibilidad (ID)	Mensual	

Figura 5: Ficha de proceso PEPSU del proceso de producción

PROCESO DE PRODUCCIÓN

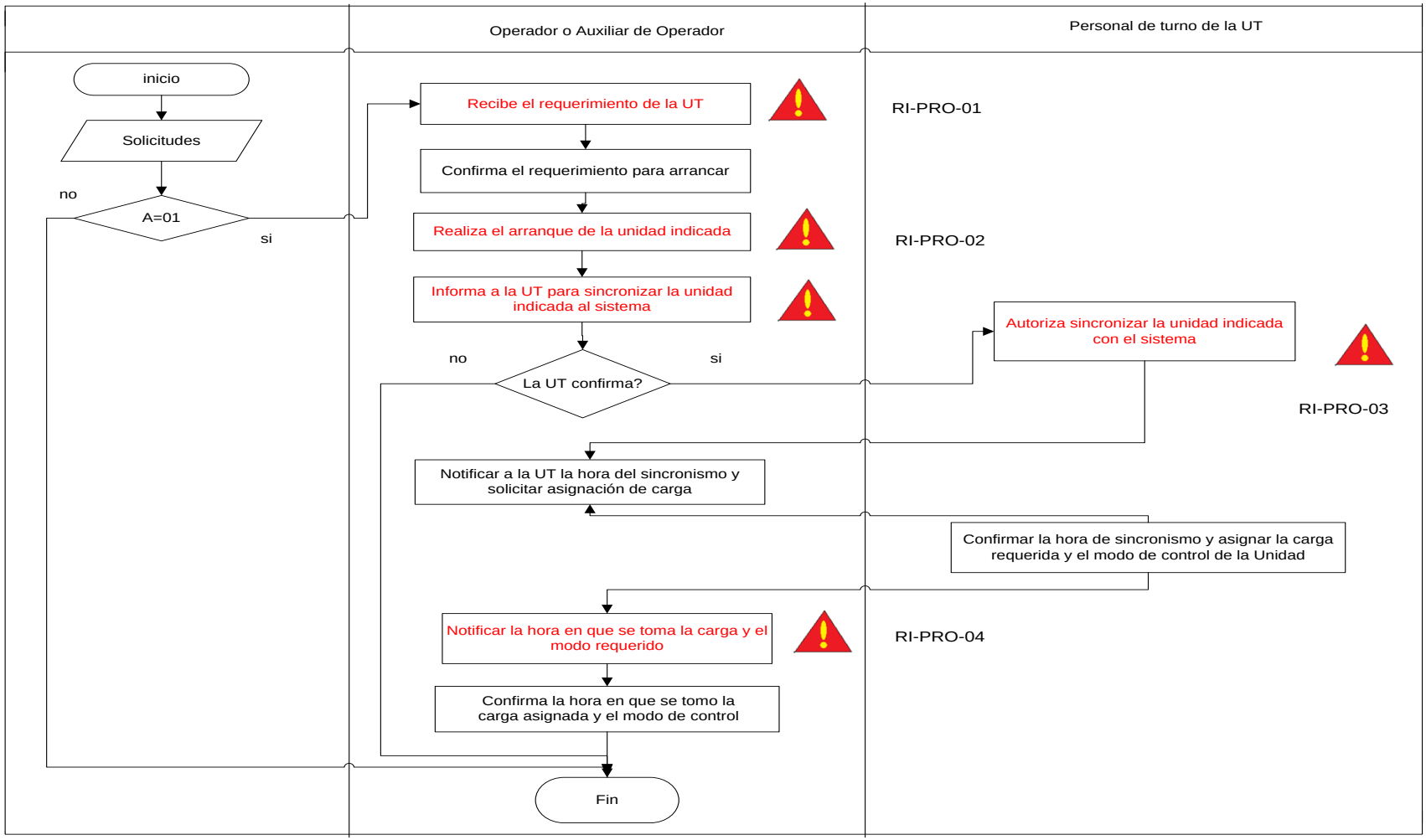
A= variable de entrada de datos

A=01, Realizar arranque de la unidad generadora
A=02, Efectuar paro de la unidad generadora
A=03, Efectuar variación de potencia de la unidad generadora
A=04, Activar sistema de alerta temprana por descargar de vertedero
A=05, Restablecimiento en condición cero voltaje
A=06, Realizar lectura y reporte de medición comercial
A=07, Lectura y reporte de variables de generación
A=08, Interrogación de relés y análisis de fallas
A=09, Monitoreo de la instrumentación de presas
A=10, Monitoreo y registro de datos de operación

A continuación se presenta el análisis de proceso, en cada uno de ellos se ha marcado con el siguiente símbolo los riesgos encontrados en cada unas de las actividades:

Figura	Significado
	Riesgo de pérdida de información
RI-PRO-XX	Riesgo de pérdida de información en el proceso de producción numero XX

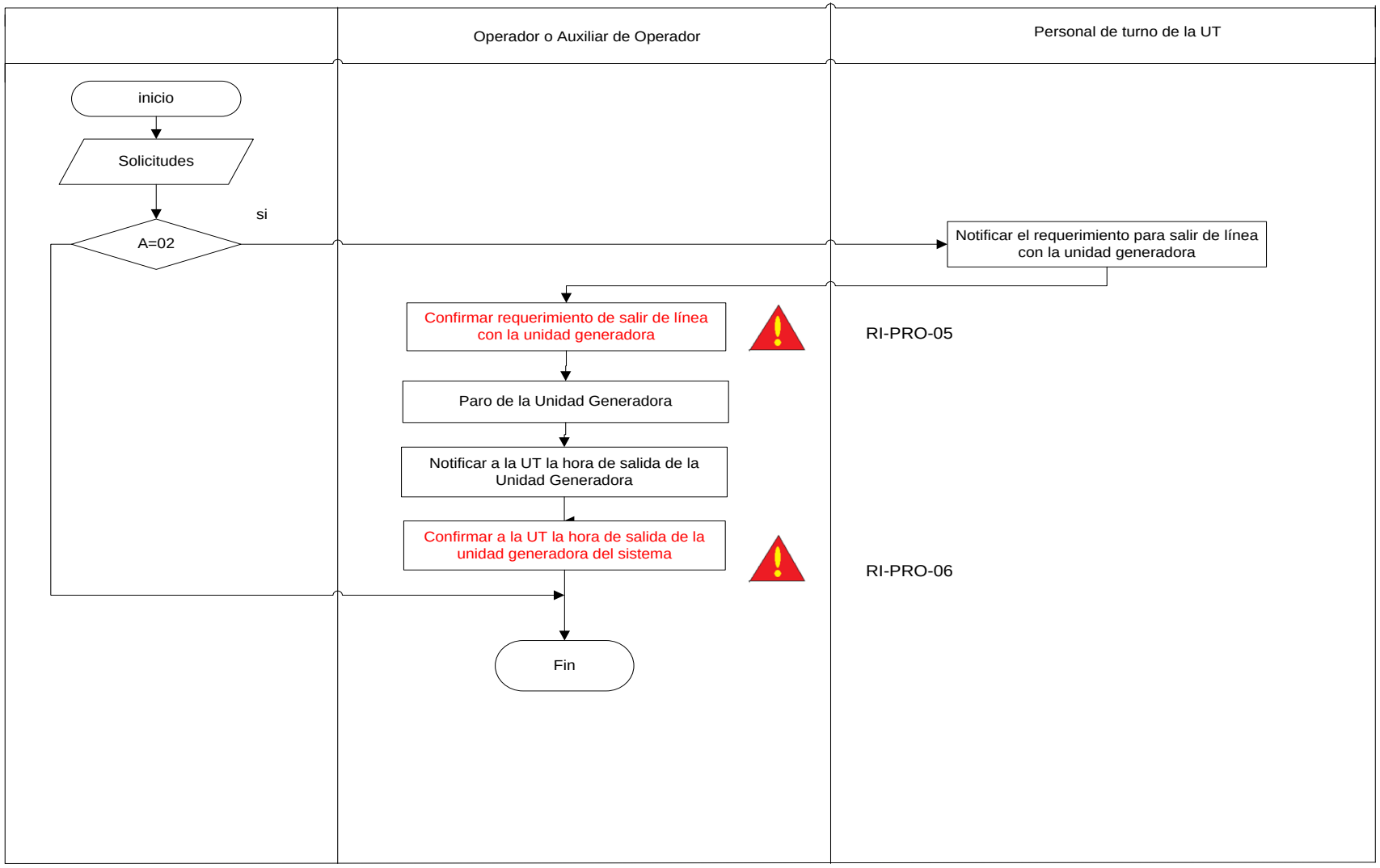
PRO 41-01 ARRANQUE DE UNIDAD GENERADORA



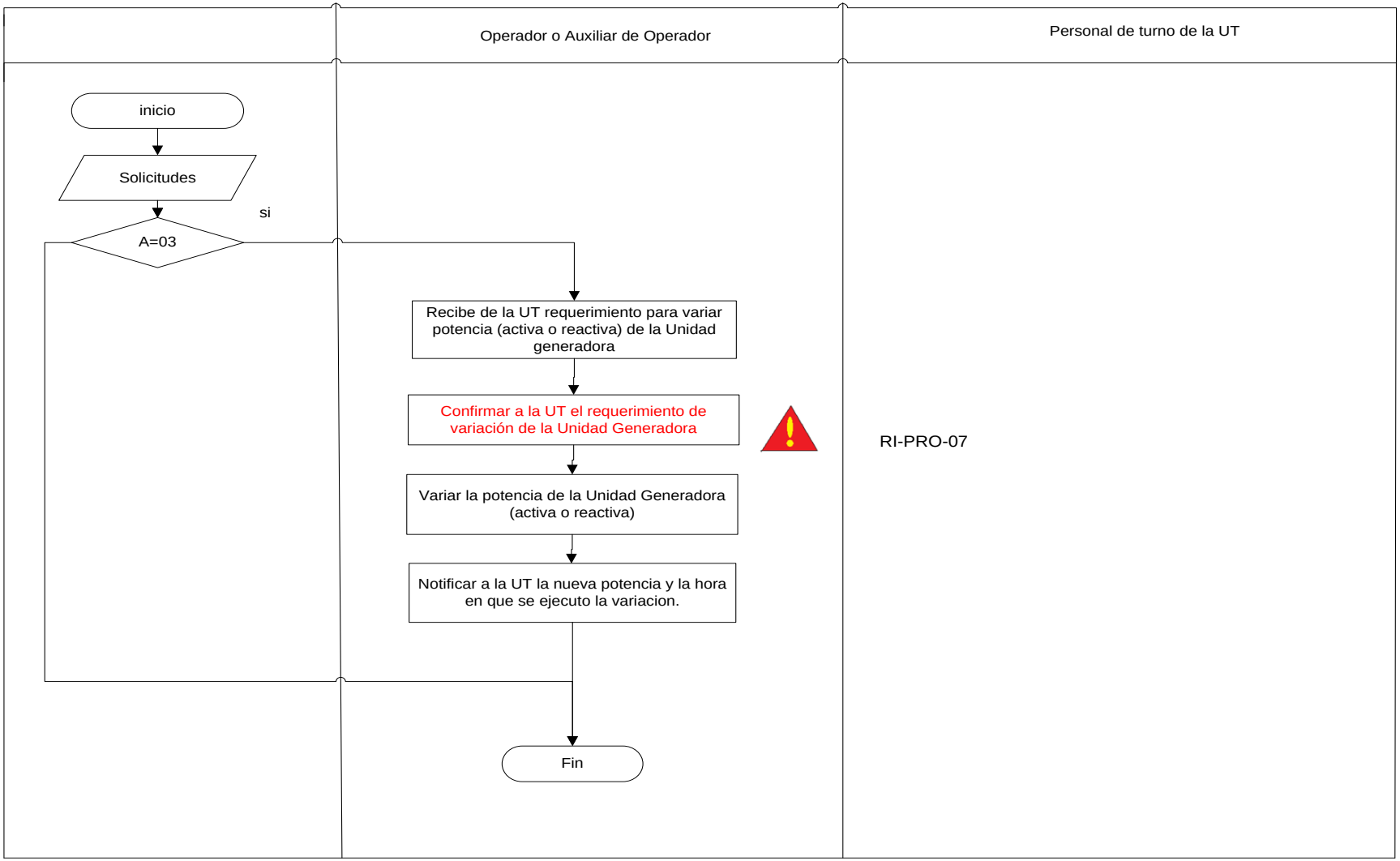
[6]

[6] Ver Anexo 4: Ver Herramientas y Técnicas de Ingeniería utilizadas

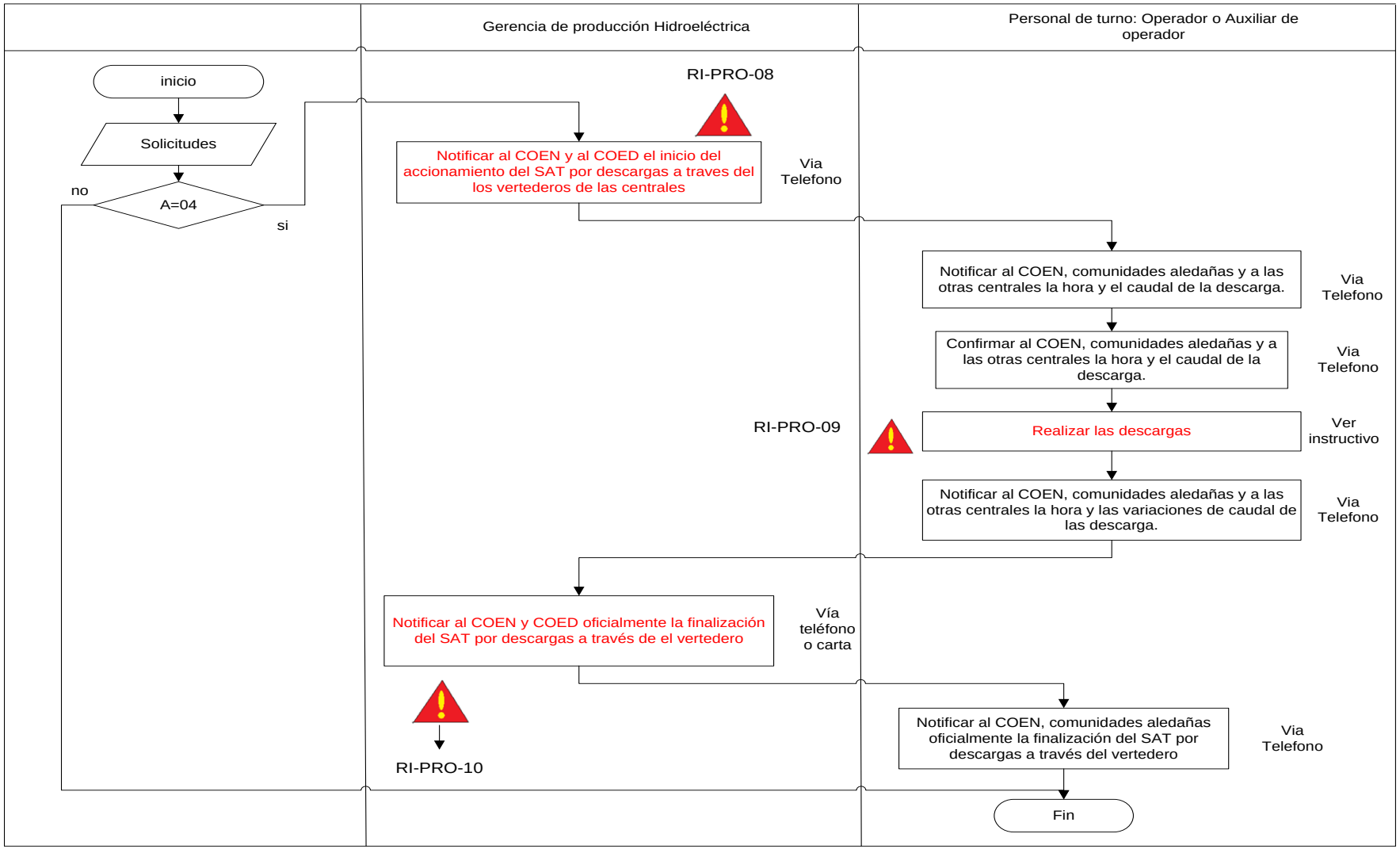
PRO 41-02 PARO DE LA UNIDAD GENERADORA.



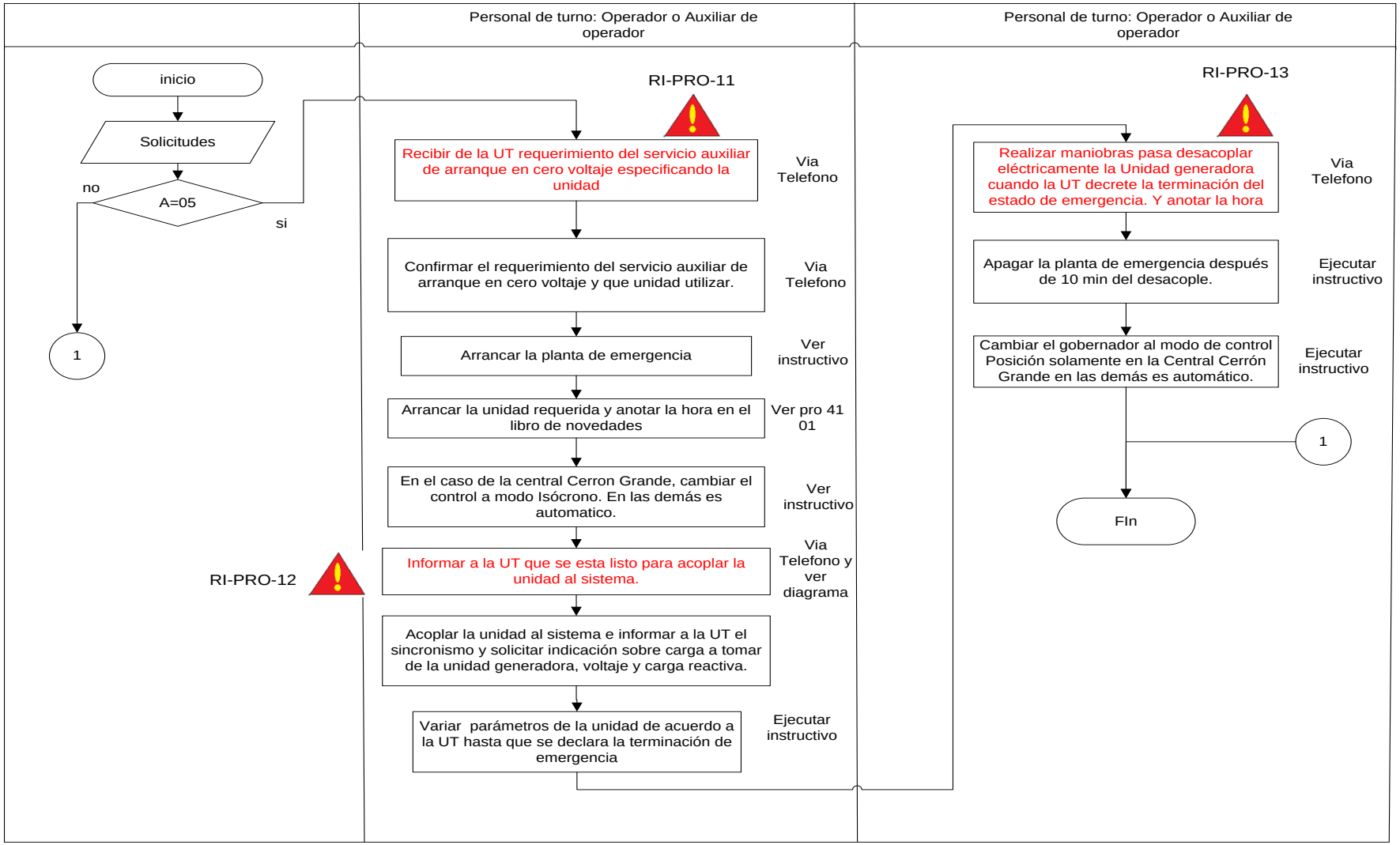
PRO 41-03 VARIACION DE POTENCIA DE LA UNIDAD GENERADORA.



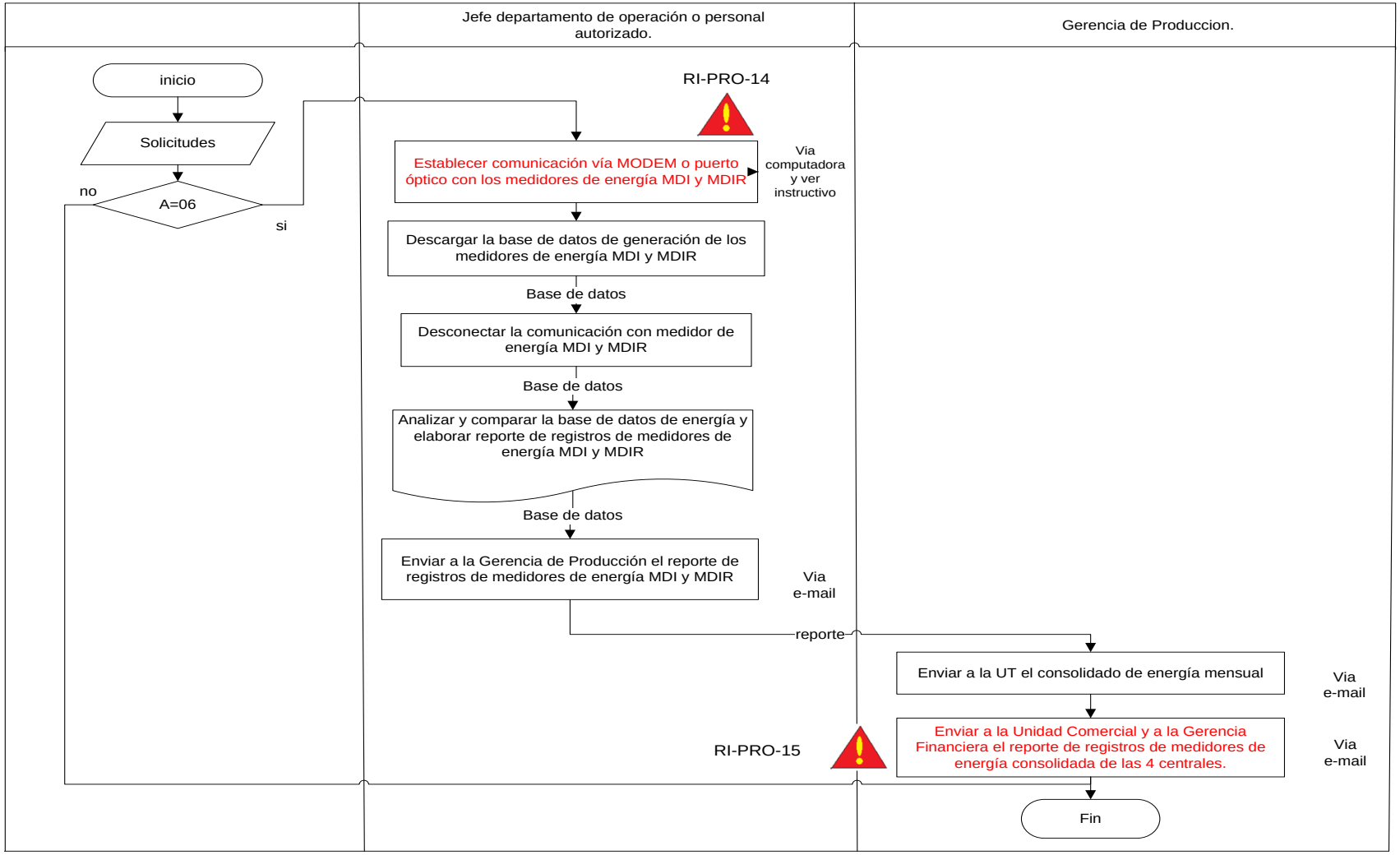
PRO 41-04 SISTEMA DE ALERTA TEMPRANA (SAT) POR DESCARGAS POR VERTEDERO



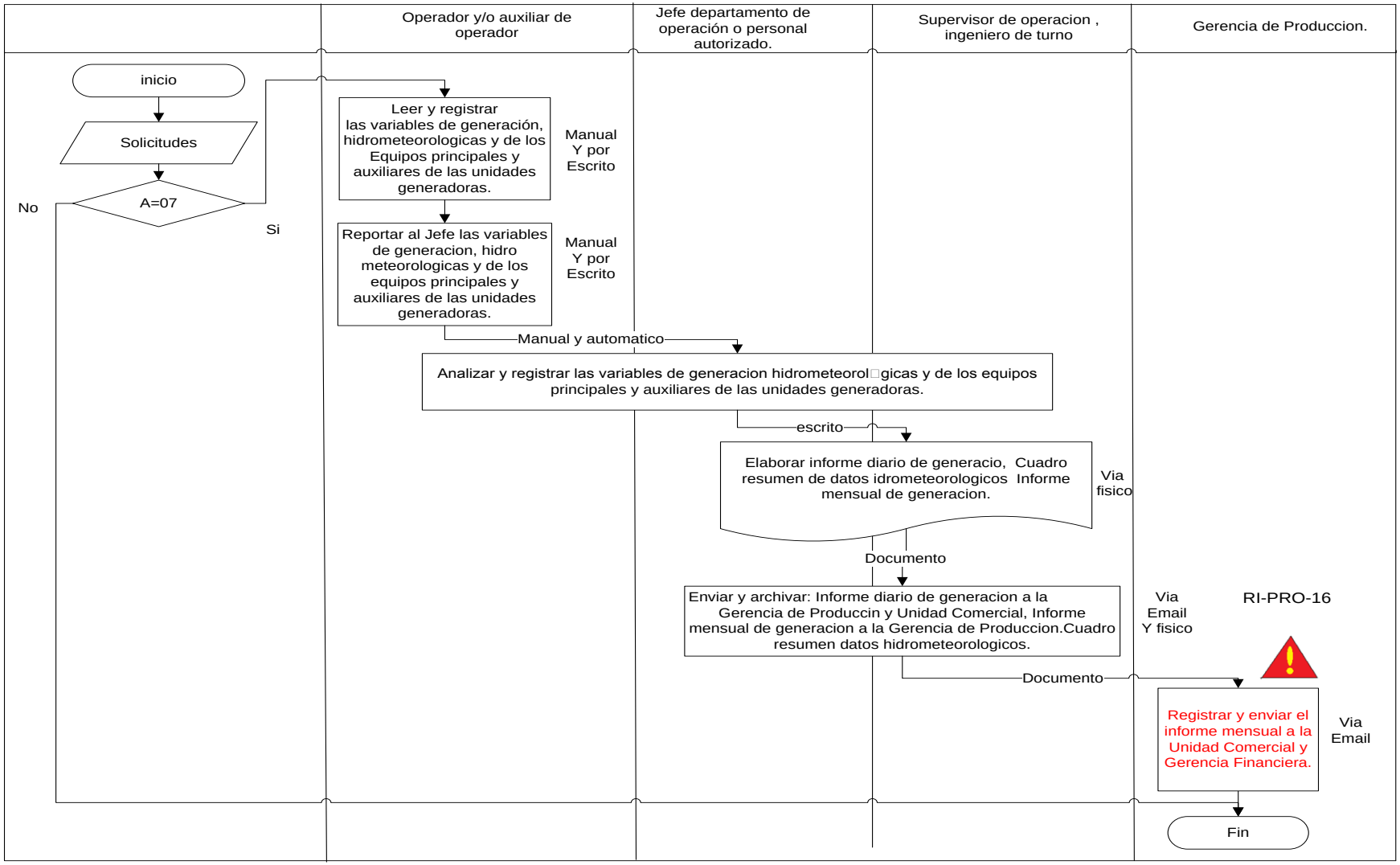
PRO 41-05 RESTABLECIMIENTO EN CONDICION DE CERO VOLTAJE



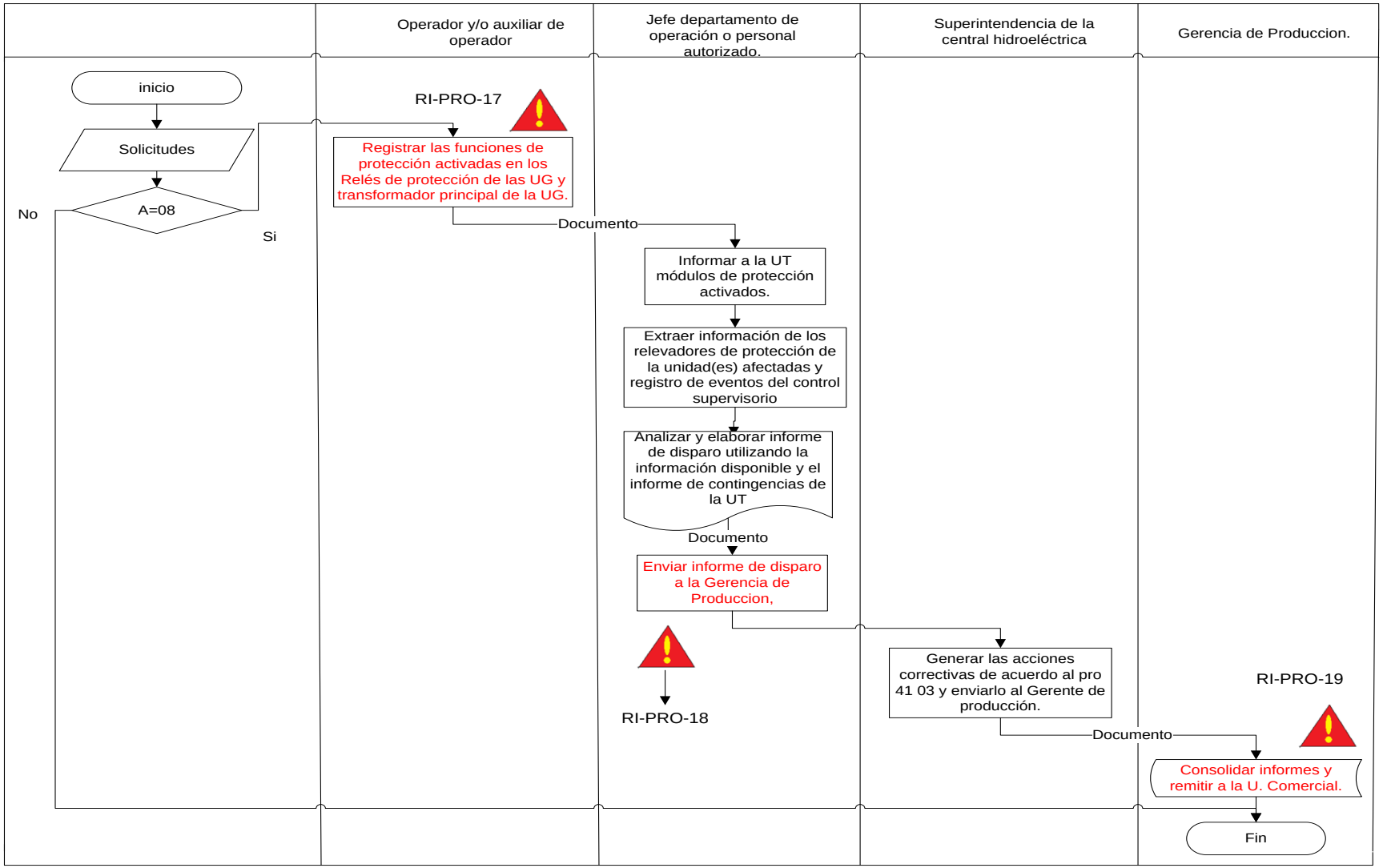
PRO 41-06 LECTURA Y REPORTE DE MEDICION COMERCIAL.



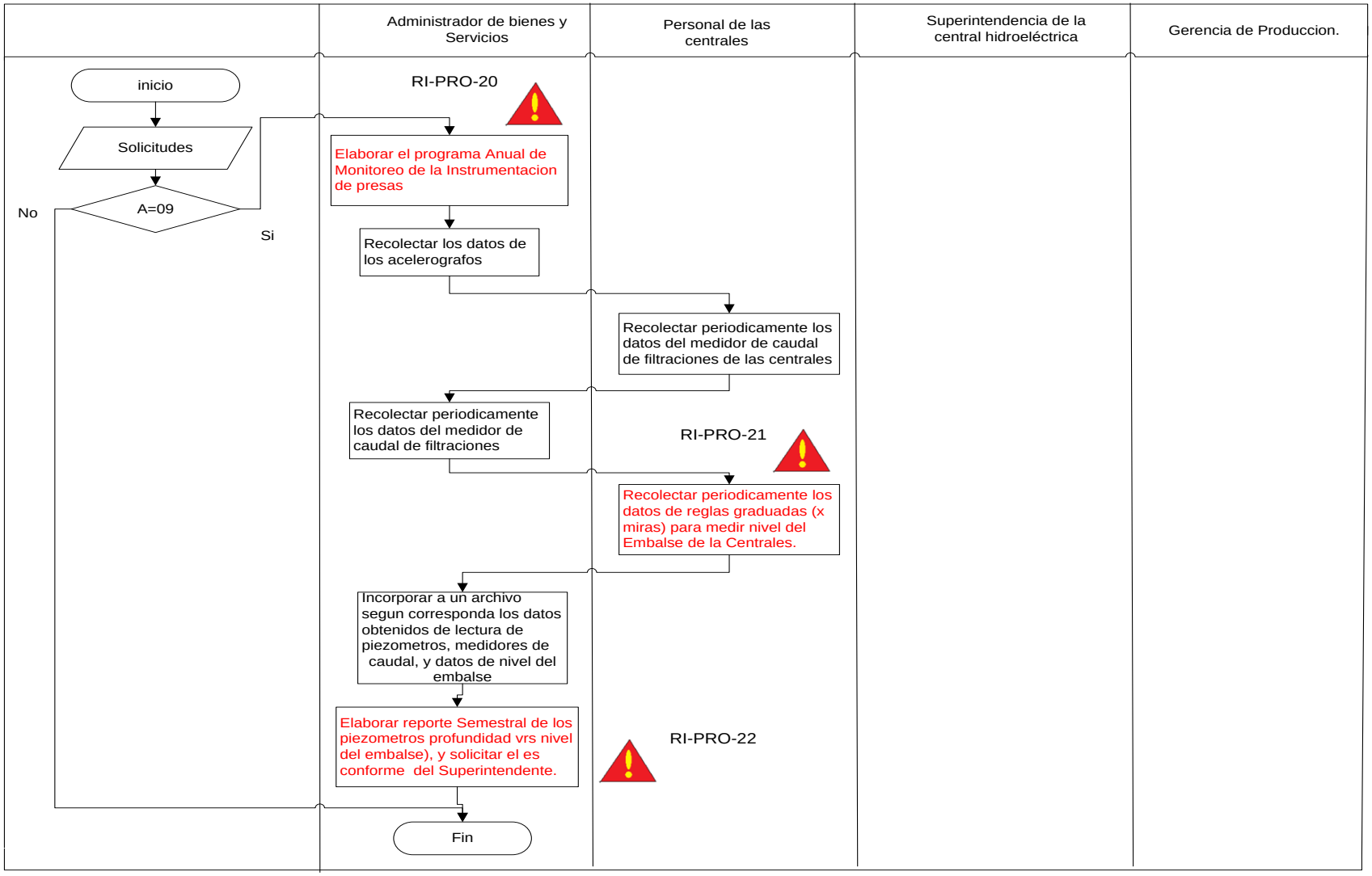
PRO 41-07 LECTURA Y REPORTE DE VARIABLES DE GENERACION



PRO 41-08 INTERROGACION DE RELÉS Y ANALISIS DE FALLAS.



PRO 41-09 PROCEDIMIENTO PARA EL MONITOREO DE LA INSTRUMENTACION DE LA PRESA



PRO 41-10 MONITOREO Y REGISTRO DE DATOS DE OPERACION

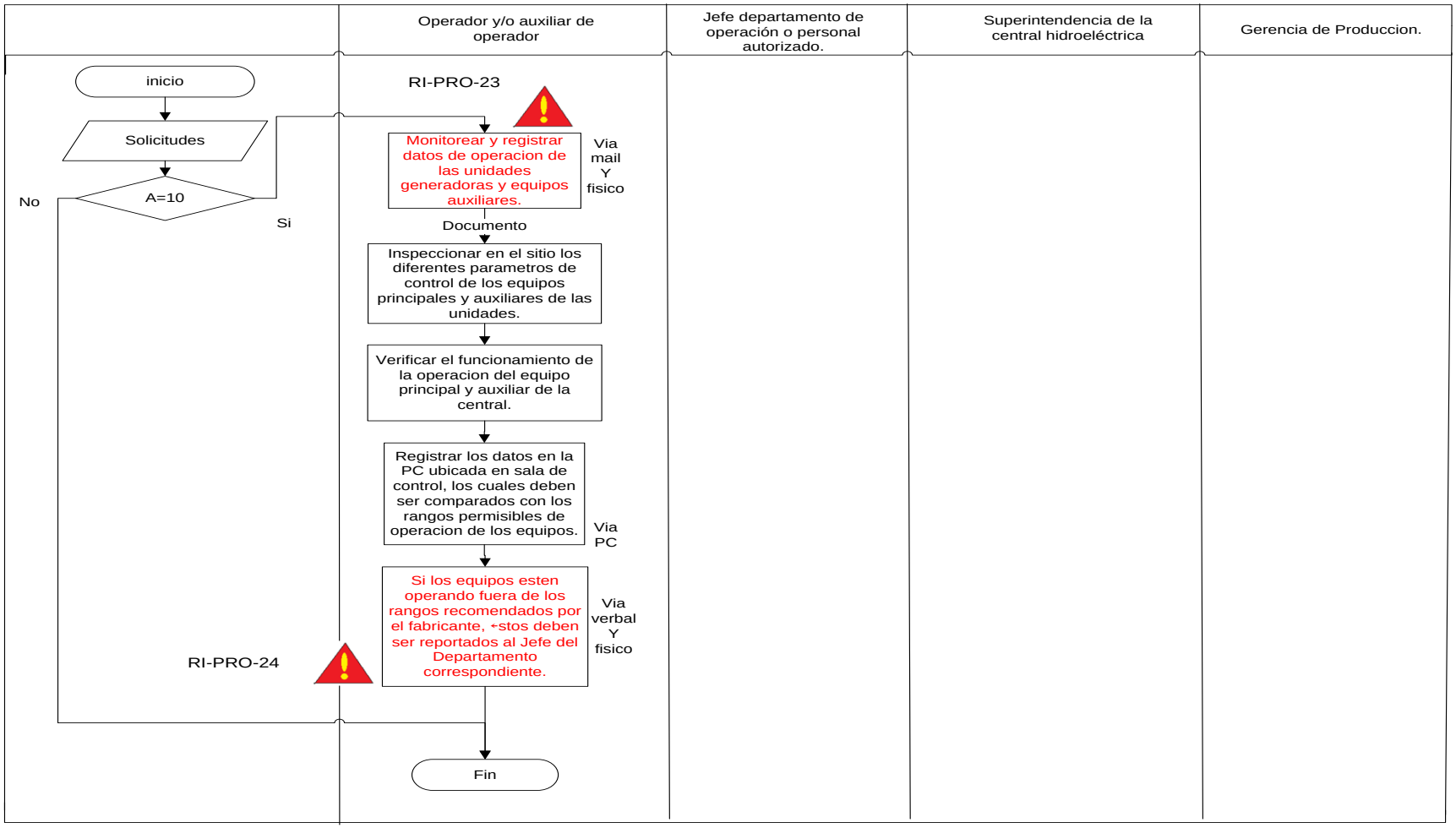


Figura 6: Flujo de proceso con flujo de datos del proceso de producción.

b. Proceso de Comercialización

A continuación se presenta los procedimientos involucrados en el proceso.

Dependencia	Código	Nombre del Procedimiento
Unidad de Comercialización	PARA09-01	Procedimiento para el control de Facturación generada en la Unidad Comercial.
	PARA09-02	Procedimiento para la administración de Transacciones Internacionales.
	PARA09-04	Procedimiento para la revisión del documento de transacciones económicas de CEL Generadora
	PARA09-10	Procedimiento para la administración comercial de contratos de distribución.
	PARA09-11	Procedimiento para la impugnación y corrección de facturas en contratos de distribución.
	PARA09-12	Procedimiento para la administración comercial de contratos de suministro.
	PARA09-13	Procedimiento para la facturación e informe de transacciones por comercialización de energía eléctrica auto suministros y otros usuarios finales.
	PARA09-17	Procedimiento para el diseño, negociación y redacción de contratos de comercialización de energía, potencia y servicios auxiliares.
	PARA09-24	Procedimiento para elaborar el plan anual de mantenimientos mayores (PAMM).
	PARA09-25	Procedimiento para la determinación del manejo óptimo de los embalses y su seguimiento mensual.
	PARA09-26	Procedimiento para la administración de datos hidrológicos.
	PARA09-27	Procedimiento para el plan anual de generación.
	PARA09-28	Procedimiento para la elaboración de pronósticos utilizando modelos de optimización.
	PARA09-29	Procedimiento para el manejo de modelos de optimización en mediano y largo plazo.
	PARA09-30	Procedimiento para la elaboración del pre-despacho oficial de CEL.
	PARA09-38	Procedimiento para realizar el trámite de indisponibilidades de unidades generadoras
	PARA09-42	Procedimiento para solicitar facturación a la Gerencia Financiera.
	PARA09-43	Procedimiento para dar el Visto Bueno a la facturación emitida por acreedores.
	PARA09-44	Procedimiento para la elaboración de oferta de inyección en el mercado mayorista.

Tabla 3: Procedimientos involucrados en el proceso de comercialización.

Medio Ambiente: Oficinas en buenas condiciones y en un ambiente de seguridad, orden y limpieza (PRA25-17 y 19, PRA41-123 y PRA06-01)

Procesos de apoyo: PRA-09-01, 09-17, 09-24, 09-29, 09-13

PROCESO GENERAL DE COMERCIALIZACION DE ENERGIA ELECTRICA

ENTRADAS (INSUMOS)			SUB-PROCESOS	SALIDAS (PRODUCTOS)		
ENTRADAS	REQUISITOS	PROVEEDOR		SALIDAS	REQUISITOS	CLIENTE
Politica de comercializacion	Politica de Precios, generacion, ingresos, importaciones, exportaciones, manejo de embalses, planes de contingencias, politica de marginacion.	Junta Directiva y Direccion Ejecutiva	Oferta de inyeccion	Datos del mercado mayorista	Acceso al Host de la Unidad Comercial (Ver Anexo No. 7 de este proceso)	Director ejecutivo/Gerencia de produccion
Requerimiento de Ingresos	Remitir la ultima semana del mes de diciembre el requerimiento minimo financiero anual, detallado por mes, para el año siguiente. Los ajustes o revisiones al mismo, a mas tardar en los dos (2) ultimos dias habiles de cada mes previo al de su ejecucion.	Programacion Financiera / Gerencia Financiera.	PRA-09-10, 09-25, 09-27, 09-38, 09-44	Informe semanal y seguimiento de la politica de comercializacion	Presentacion semanal (precio MRS, generacion, ingresos, importación/exportación, niveles de enbalse, marginaciones, otros) y recomendaciones generales para el seguimiento de la politica de comercializacion.	Junta Directiva y Director Ejecutivo
Contratos firmados	Contratos: Precio, Cantidad (MV), etc.	Secretaria		Plan anual de generacion	Presentacion que incluye el manejo de embalses, pronostico de precios, descensos programados, etc.	Junta Directiva y Director Ejecutivo

Informacion de mercado	Base de datos, pagina web de UT y pagina web del OMCA, (ver Anexo 1 de este proceso), Documento de transacciones economicas (DTE) (PARA-09-04) y correspondencia con ambas entidades.	U.T./OMCA
Mantenimientos mayores	Propuestas del PAMM, de unidades generadoras de CEL.	Gerencia de produccion
	Programa anual de mantenimientos mayores (PAMM) de unidades, subestaciones y lineas, de acuerdo al Plan Anual oficial enviado por la UT (ver Anexo No 2 de este proceso) (actividad No 12, PARA-09-24)	UT
Marco regulatorio	Leyes, reglamentos, normas acuerdos y otros documentos relacionados con el sector electrico.	Ministerio de economia y SIGET

Oferta de retiro
PRA-09-27

Plan anual de operaciones	Variaciones (cuando existiesen), en la revision mensual de la generacion proyectada versusla generacion real	Junta Directiva y Director Ejecutivo
Oferta de inyeccion en el Mercado Mayorista	Cumplimiento del reclutamiento de operaciones de la UT	Unidad de Transacciones
Predespacho	Generacion Programada por la UT para cada una de las unidades generadoras, según el formato de la UT, PARA-09-30 Anexo No.2	Gerencia de produccion.
Informe diario de operación de la UT	Informe para consulta en el Host de la Unidad Comercial detallado por hora, operador y comentarios.	Gerencia de produccion.

Reporte diario de generacion	Variables de generacion (Ver Anexo No. 3 de este proceso) para todas las centrales	Gerencia de produccion
Informe mensual de inyecciones	Resumen mensual horario por unidad (cantidad bruta, neta y consumo propio en MWh)	Gerencia de produccion
Informe de indisponibilidades/ Solicitud de mantenimientos	Solicitud de interrupciones según lo indicado en el anexo No.1 del PARA-09-38, y Anexo No. 4 de este proceso	Gerencia de produccion
	Respuesta verbal o escrita de las interrupciones que no proceden o no son autorizadas	⇨ UT

Oferta de mercado
PRA-09-02, 09-27 ⇨

Confirmacion de mantenimientos	Hoja de solicitud de interrupciones (indisponibilidades) con el conforme de la UC (ver Anexo No. 4 de este proceso). Correspondencia recibida de la UT, de las interrupciones que no son autorizadas por la UT.	Gerencia de produccion.
Proyeccion de niveles	cuando se elabore el Plan Anual y cuando existan modificaciones al mismo.	
Plan anual de generacion y precios	Remision de hoja, en formato exce, detallado por mes, desglosado por central, totalizado y con la proyeccion de precio mensual. Actualizacion mensual (ver Anexo No. 5 de este proceso)	Gerencia Financiera
Proyeccion de generacion de precios	Proyeccion anual por central de generacion y precio(ver Anexo No. 6 de este proceso)	

Informe de interrogacion de relès y analisis de fallas	Descripcion y analisis de fallas especificando central, unidad generadora, fecha de falla, hora, fecha de envio, analisis, del registro oscilografico, tiempo de indisponibilidad, firma y sello, de acuerdo al resumen de relevadores operados (RC-41-000)		Oferta de comercializacion	Datos para facturacion por energia en contratos y desviaciones negativas	.+. Consumo en MWh y valor monetario .+. Fecha del periodo del servicio .+. Especificar el nombre del cliente al que se le factura y los tipos de cargos a aplicar .+. Firma y sello de la unidad Comercial y analista r	Gerencia Financiera
	Informe oficial de fallas (de acuerdo a pagina Web de UT, zona de miembros, menu, reporte de interrupciones de equipos: idm, inicio, fin, duracion, descripcion, MW, Kwh no servidos, responsable).		PRA-09-10.	Datos para facturacion por suministro de energia electrica a empleados	Remitir los informes de consumo en forma impresa firmados por el analista que los alaboro y por medio de memorandum, detallando el periodo de facturacion que corresponde y el bloque de informes que se envia, asi como cargar la base de la unidad comercial	Gerencia Financiera

Reporte de cobros y pagos	Retroalimentacion de cobros y pagos, via correo electronico, indicando monto, cliente/proveedor, fecha de cobro/Pago, numero de factura y de cheque o nota de abono	Departamento de Tesoreria	Procesamiento de Datos	Datos para facturacion por energia electrica en Autosuministro.	Remitir con Memorandum los informes de consumo de forma impresa, Firmados por el analista que los elaboro, detallando el periodo de facturacion que corresponde y el bloque de informes que se envia a tesoreria	Gerencia Finaciera
Datos operativos de las centrales Hidroelectricas	De acuerdo a lo establecido en el Anexo del reglamento de operaciones de la UT debidamente actualizado (minimos, maximos de potencia y cualquier otro dato que considere necesario proporcionar la Gerencia de Produccion)	Gerencia de produccion	PRA-09-04, 09-10, 09-12, 09-26, 09-28, 09-30, 09-42, 09-43	Datos para facturacion por energia en Mercado Regulador del Sistema (MRS) y Mercado Electrico Regional (MER)	Firmar, otorgando el visto bueno, a los comprobantes de liquidacion y comprobantes de Credito Fiscal	
					Memorandum con el desglose del DTE. Informando cuanto corresponde a energia en el valor monetario y en MWh aplicados, y los rubros adicionales que se reflejan en dicho documento.	

Infraestructura: Edificaciones adecuadas y con los recursos necesarios para ejecutar el trabajo (PRA-25-01,02,12,17 y 18)	Recursos Humanos: 1 Jefe de Unidad, 1 secretaria, 7 analistas, ver datalle en competencias en el tomo 1 del MCP

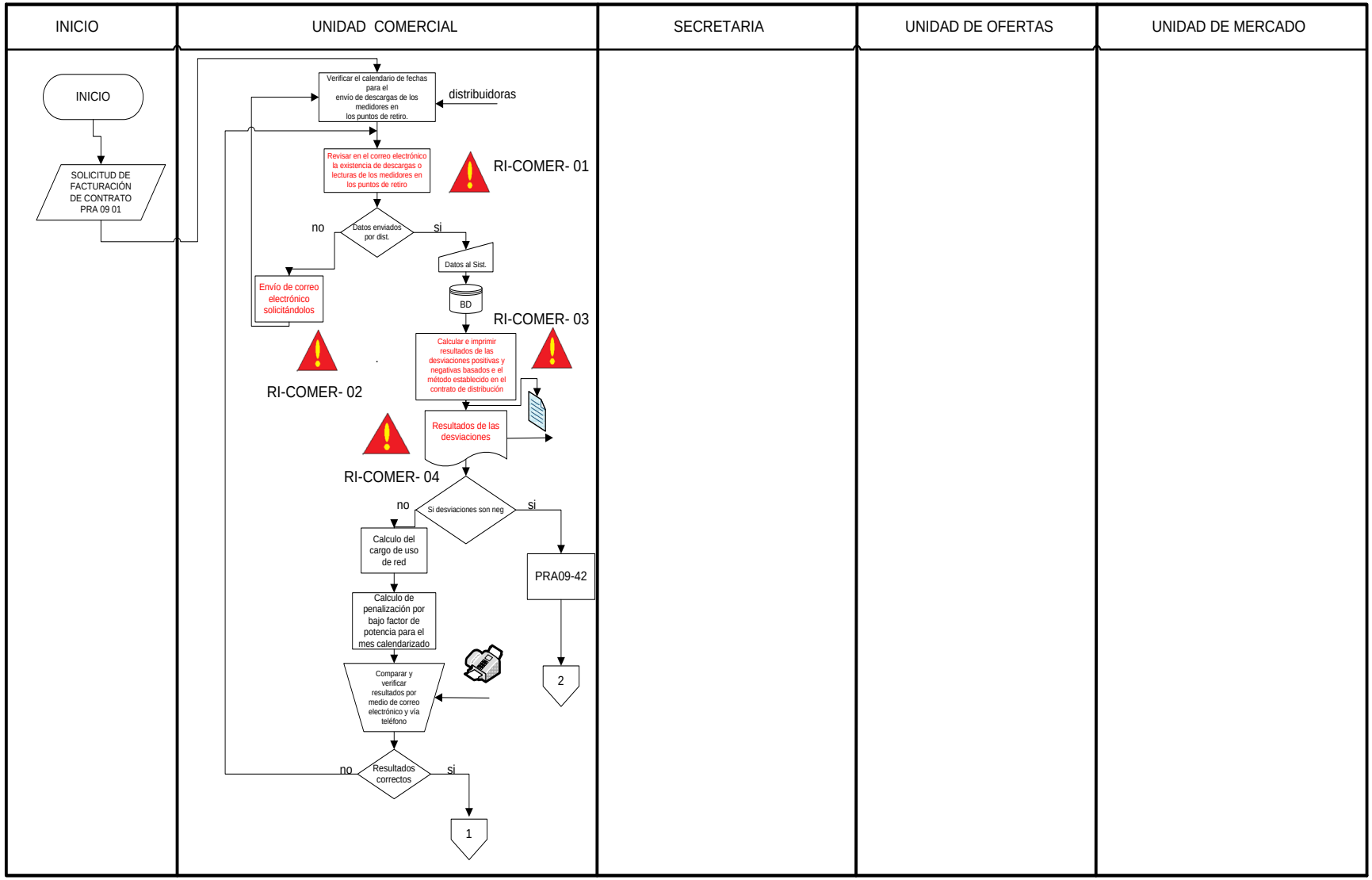
Objetivo General del Proceso: Administrar y ejecutar el Plan Anual de Operación, optimizando la materia prime, los precios y los ingresos de la Comision

INDICE DE MEDICION	FRECUENCIA DE MEDICION	INDICE DE COMPARACION
generacion ofertada vrs. Generacion predespachada	Mensual	Mas o menos 5 %
Generacion odertada vrs. Generacion despachada	Mensual	Mas o menos 5 %
Ingreso Real vrs. Requerimiento financiero	Mensual	No menor al 90%
Generacion real vrs Generacion proyectada	Mensual	No menor al 6%
Precio Real vrs. Precio proyectado	Mensual	No menor al 6%

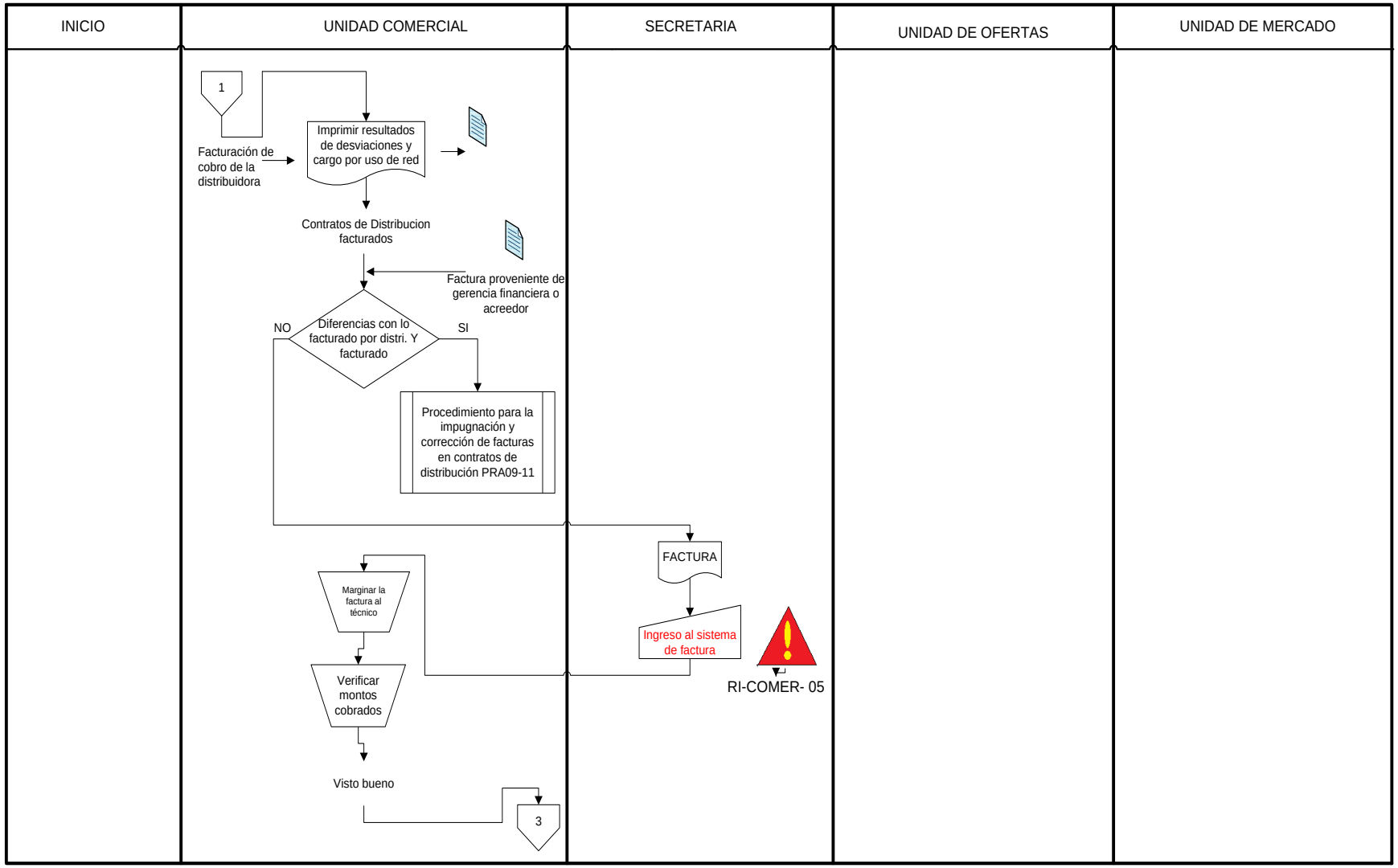
Definiciones	
OMCA	Operador del mercado Centroamericano
UT	Unidad de Transacciones
UC	Unidad Comercial
Direccion UT	www.ut.com.sv
Direccion OMCA	www.enteoperador.org
DTE	Documento de Transacciones Economicas

Figura 7: Ficha de proceso PEPSU del proceso de Comercialización

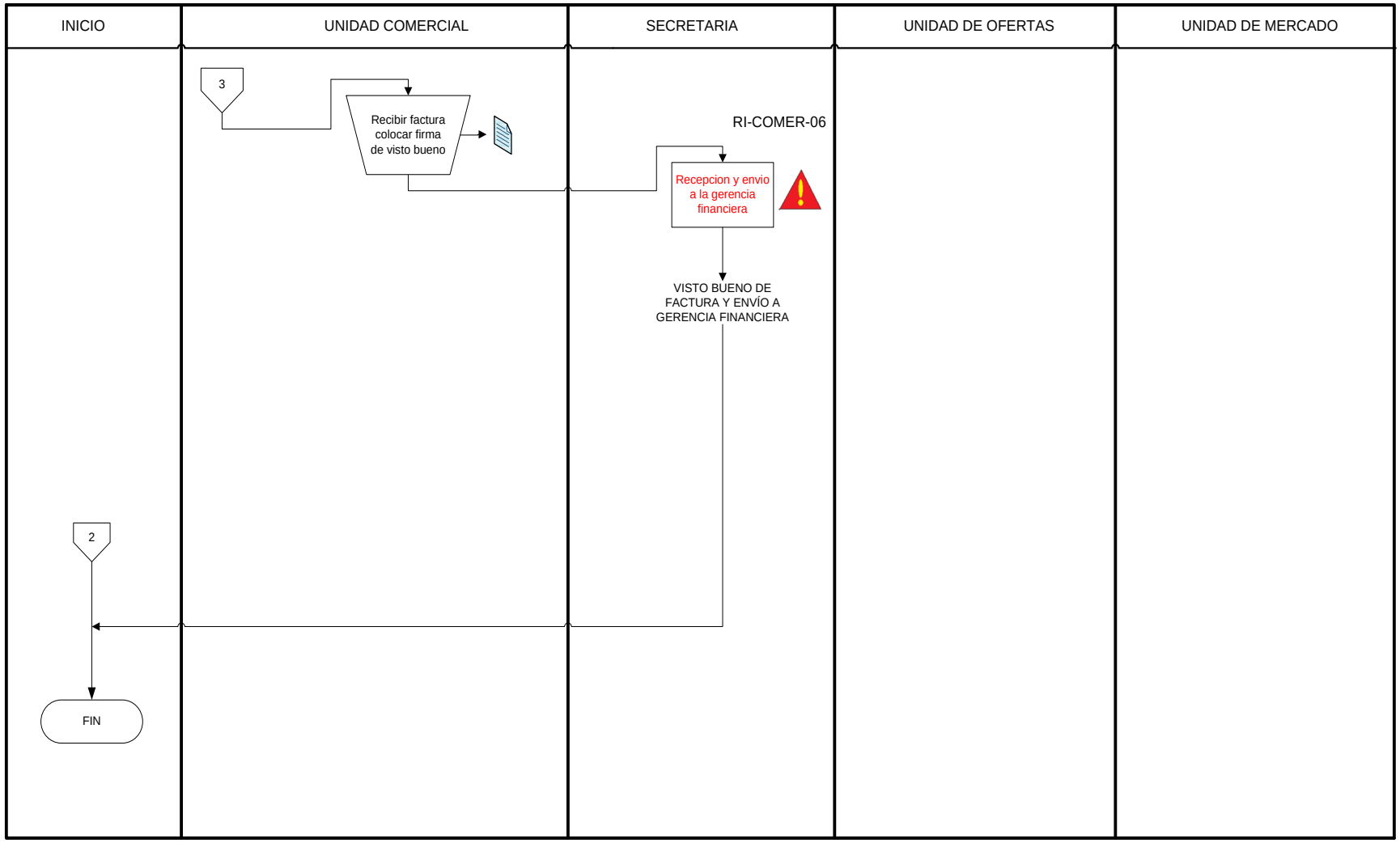
Desglose de proceso con Flujo de Datos: PROCESO GENERAL DE COMERCIALIZACIÓN



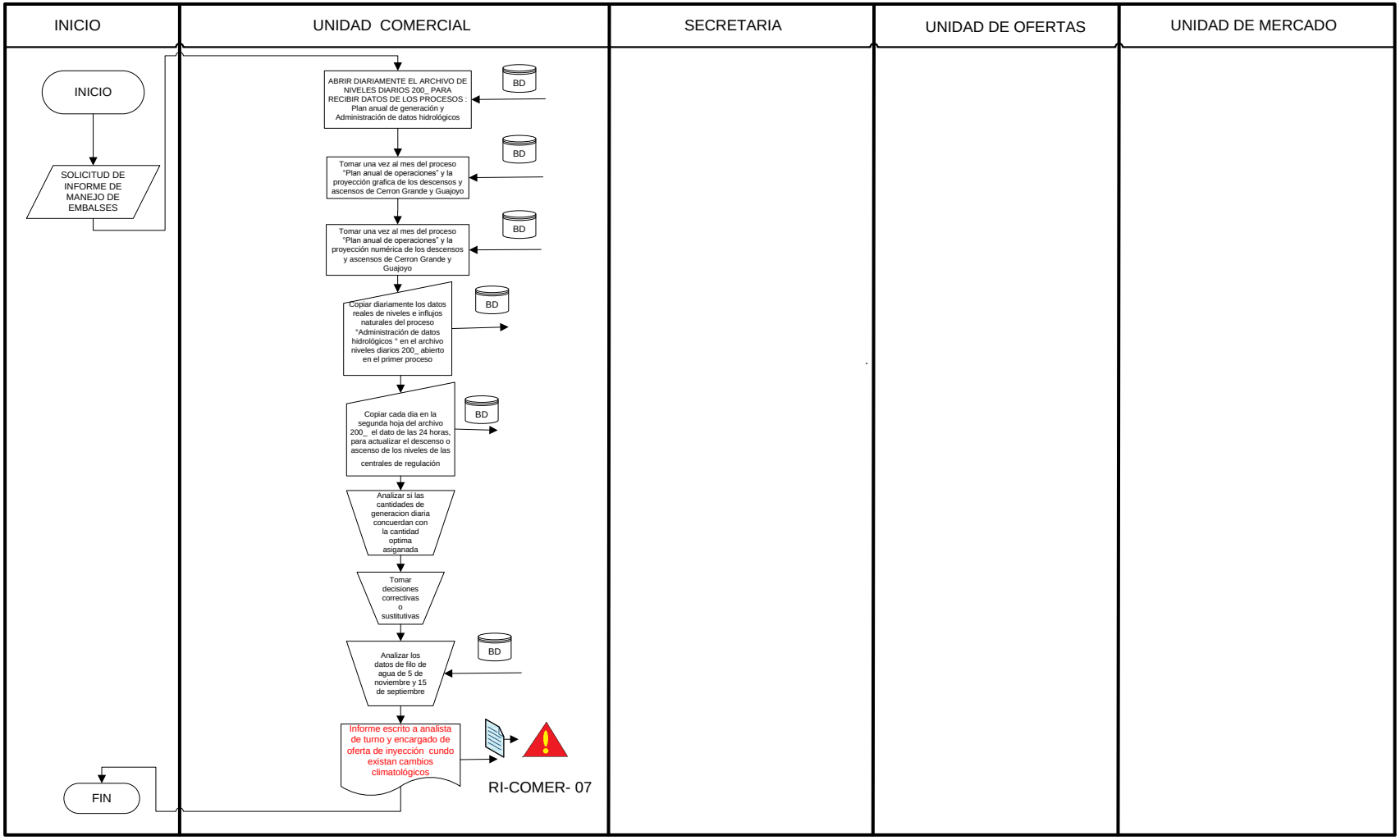
Desglose de proceso con Flujo de Datos: PROCESO GENERAL DE COMERCIALIZACIÓN



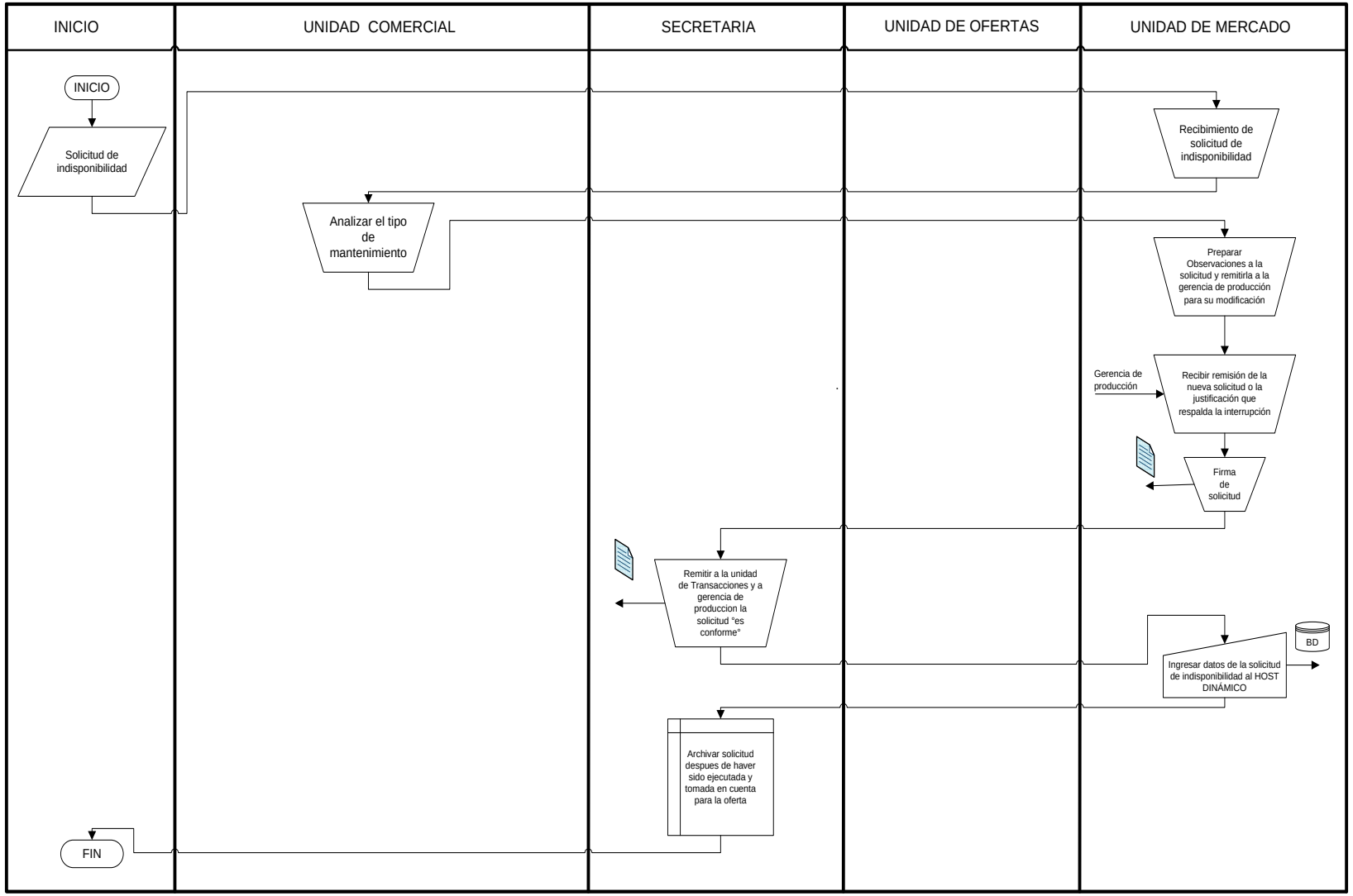
Desglose de proceso con Flujo de Datos: PROCESO GENERAL DE COMERCIALIZACIÓN



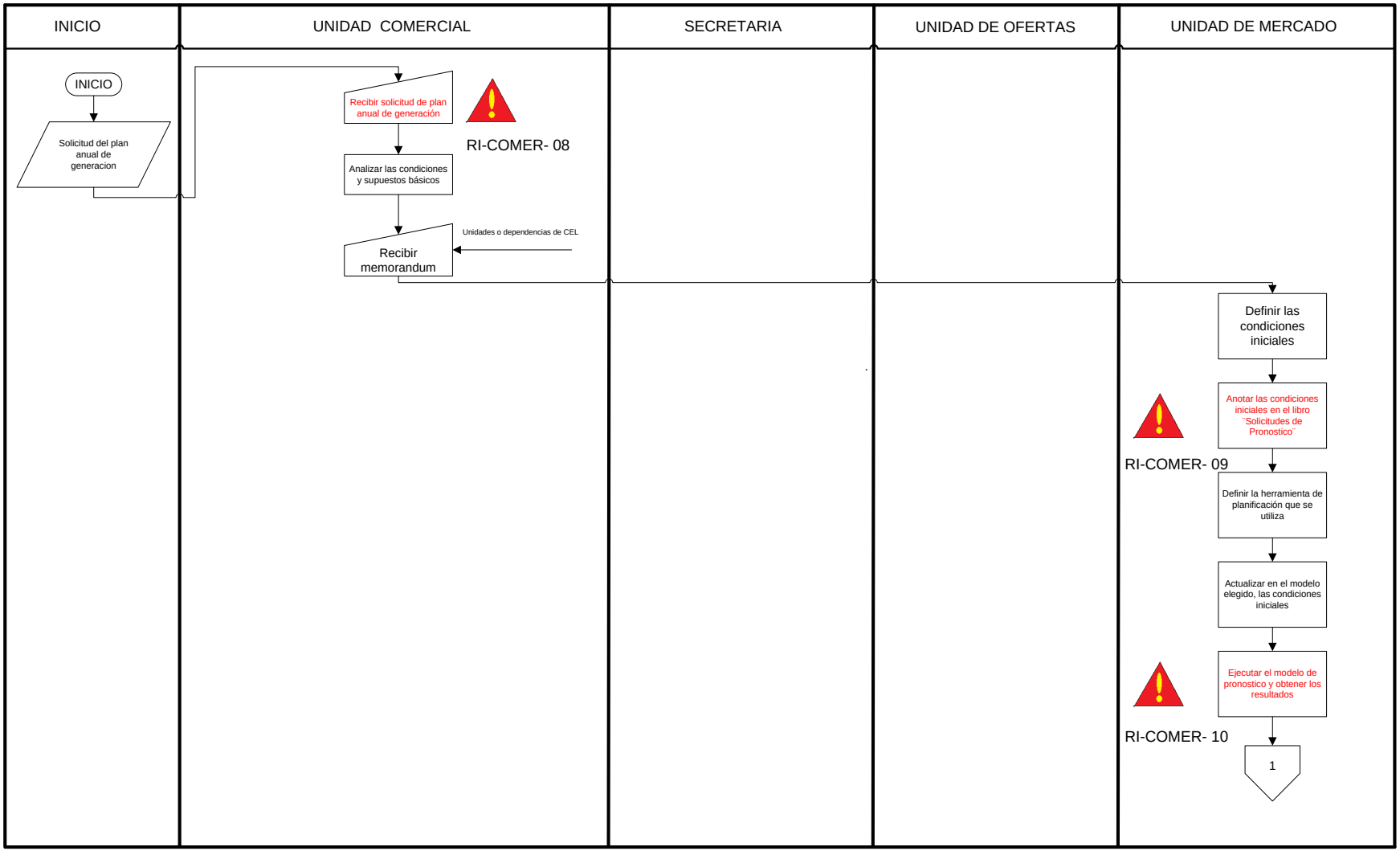
Desglose de proceso con Flujo de Datos: PROCESO GENERAL DE COMERCIALIZACIÓN



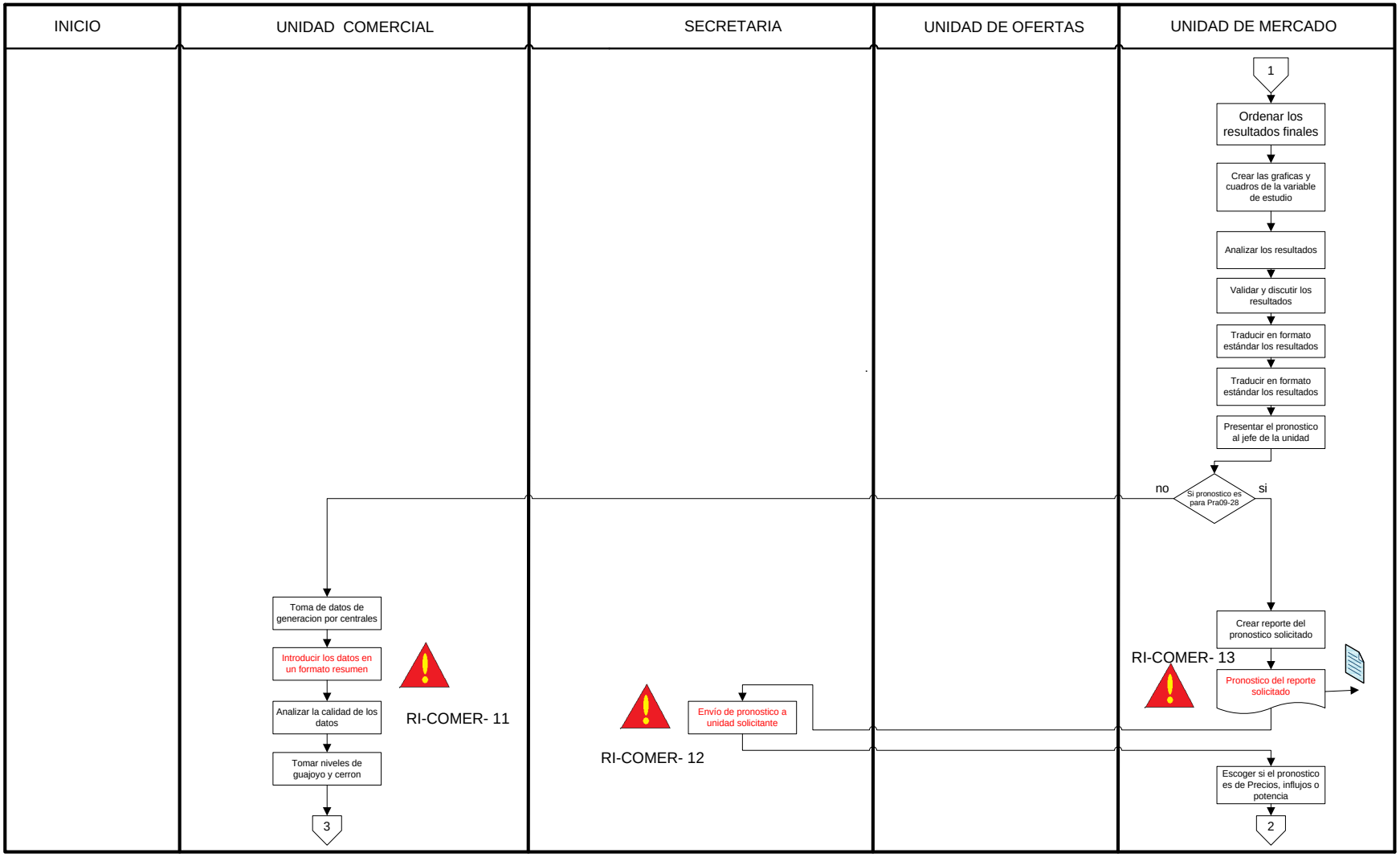
Desglose de proceso con Flujo de Datos: PROCESO GENERAL DE COMERCIALIZACIÓN



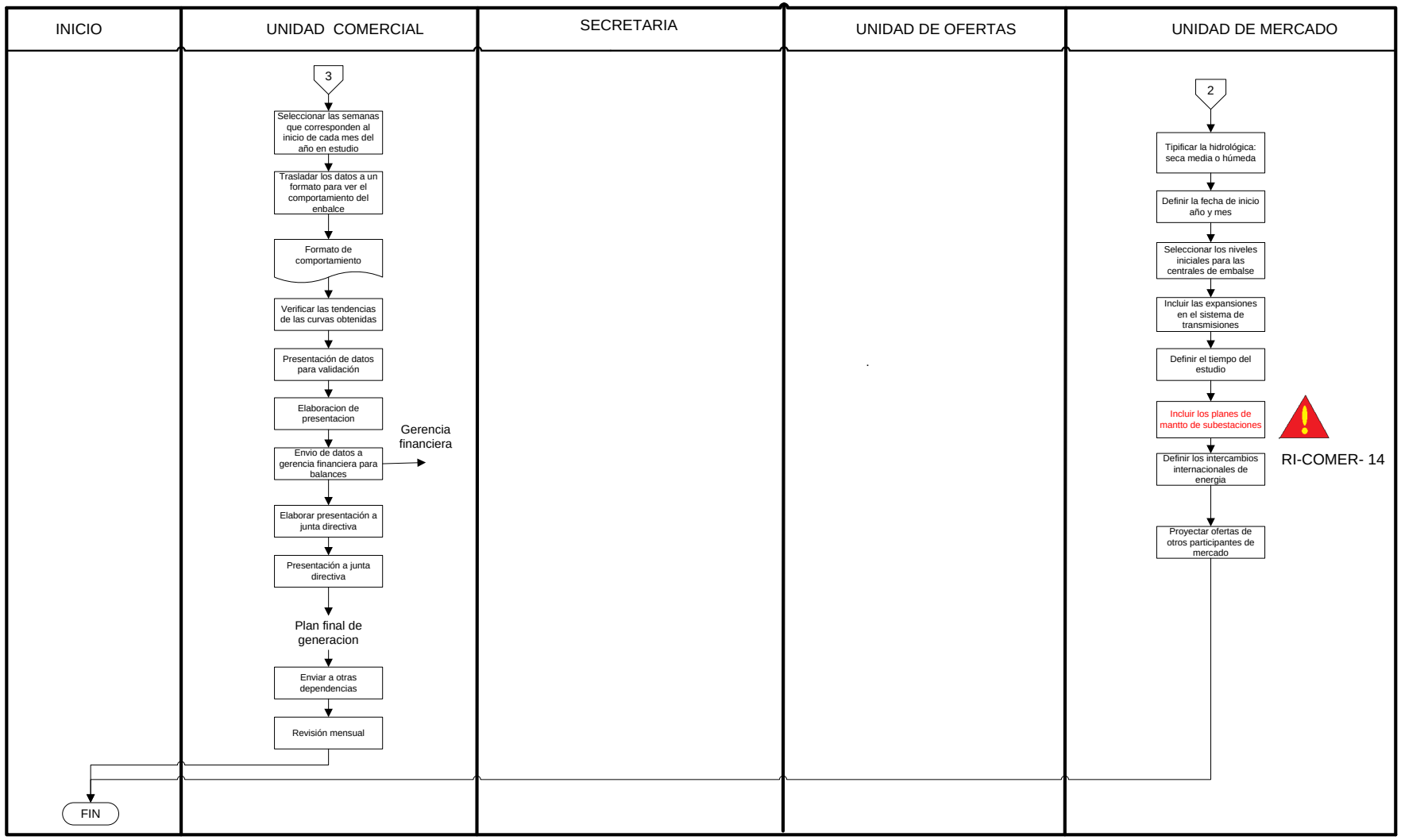
Desglose de proceso con Flujo de Datos: PROCESO GENERAL DE COMERCIALIZACIÓN



Desglose de proceso con Flujo de Datos: PROCESO GENERAL DE COMERCIALIZACIÓN



Desglose de proceso con Flujo de Datos: PROCESO GENERAL DE COMERCIALIZACIÓN



Desglose de proceso con Flujo de Datos: PROCESO GENERAL DE COMERCIALIZACIÓN

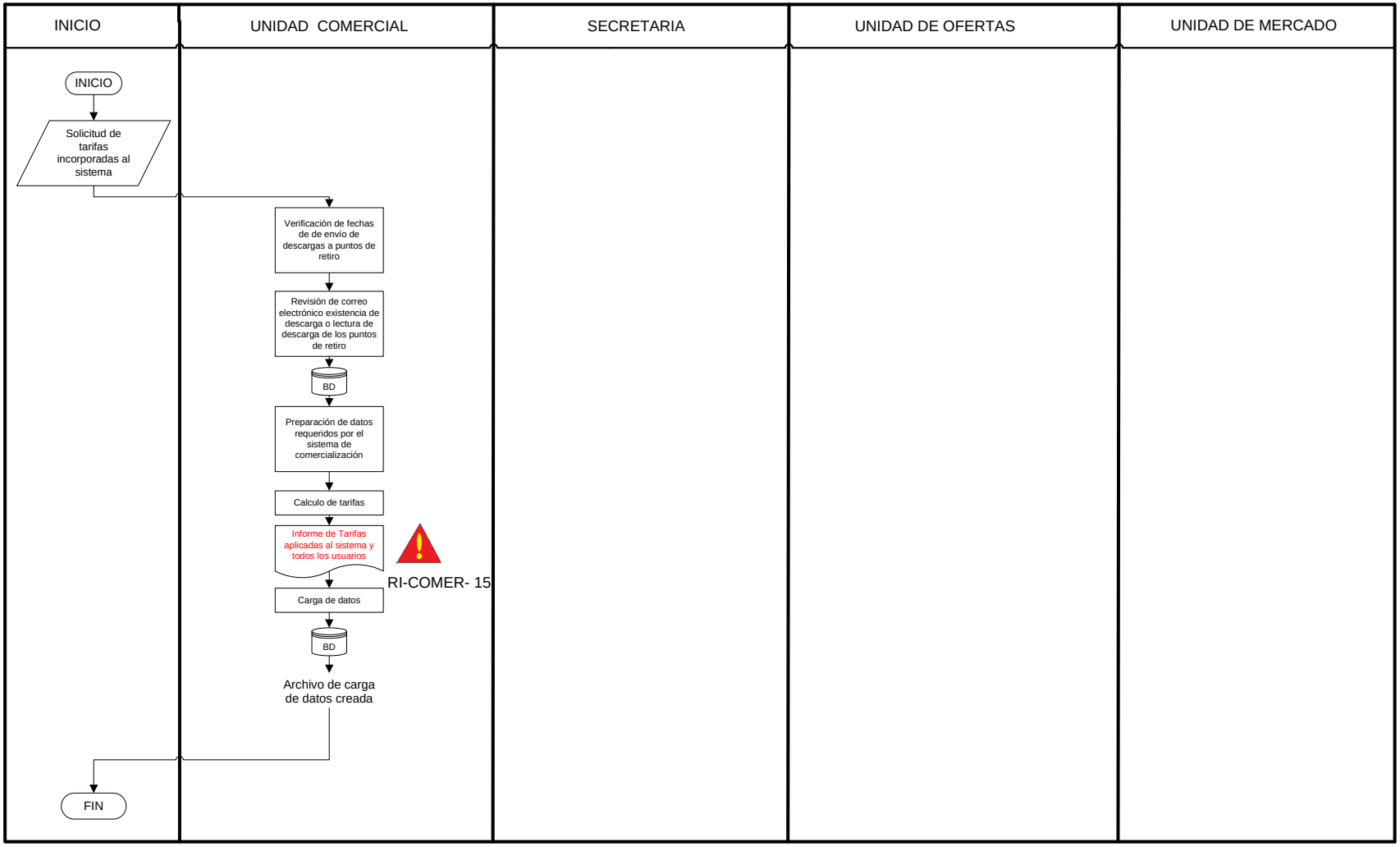


Figura 8: Flujo de proceso con flujo de datos del proceso de Comercialización

c. Proceso de Gestión de la Información

A continuación se presenta el listado de procedimientos involucrados en el Proceso de Gestión de la Información.

Dependencia	Código	Nombre del Procedimiento
Unidad Informática Institucional	PRA17-01	Procedimiento para el desarrollo y/o mantenimiento de sistemas informáticos con recurso interno.
	PRA17-02	Procedimiento para el control y seguimiento del análisis, diseño, desarrollo e implantación de sistemas informáticos creados por terceros.
	PRA17-03	Procedimiento para la detección de necesidades de hardware y software.
	PRA17-04	Ejecución de trabajos de servicios de mantenimiento correctivo a los equipos de computa de CEL. Y soporte técnico a los usuarios.
	PRA17-06	Procedimiento para la gestión del mantenimiento preventivo a los equipos de cómputo de CEL.
	PRA17-07	Procedimiento para alta, baja y cambio de rol de usuarios de servicios informáticos.
	PRA17-08	Procedimiento para el pago de planillas a los empleados de la Comisión en casos de contingencia.
	PRA17-09	Procedimiento para la preparación de energía eléctrica y recepción del pre-despacho en casos de contingencias.

Tabla 4: Procedimientos involucrados en el proceso de Gestión de la Información.

Medio Ambiente: Gestion para desechos y residuos PRA06-11 Seguridad Industrial (PRO41-123) Orden y limpieza (PRA21-01)				Proceso de apoyo: Gestion de Adquisiciones, Gestion Presupuestaria, Gestion Integrada		
PROCESO DE GESTION DE LA INFORMACION						
ENTRADAS	**REQUISITOS**	**PROVEEDOR**		**SALIDAS**	**REQUISITOS**	**CLIENTE**
Solicitud de infraestructura informatica incluyendo usuarios.	Tipo de equipos (computador personal o portatil, impresor, escaner, UPS). Funciones del personal que utilizara el equipo. Tiempo en que se requiere. Nivel de acceso a los sistemas de informacion	Todas las dependencias	Desarrollo de sistemas PRA 17-07	* Hardware instalado	* Cumplimiento a los requerimientos solicitados	Usuario solicitante
Llamada telefonica, correo electronico o Memorandum de solicitud de servicios de	Tipo de equipo Falla observable Prioridad (alta, media, baja)	Todas las dependencias	ADMINISTRACION DE REDES Y BASES DE DATOS PRA 17-07	* Sistema Funcionando	* Validad funcionalidad de acuerdo a los requerimientos	Usuario solicitante
Solicitud de desarrollo o modificacion de sistemas Mecanizados	Solicitud de desarrollo de sistemas Descripcion del procedimiento a mecanizar	Todas las dependencias usuarias de sistemas computarizados	MANTENIMIENTO Y SOPORTE TECNICO PRA 17-03, 04, 06	* Hardware funcionando	* Validar funcionamiento de acuerdo a los requerimientos	Usuario solicitante
solicitud de compra de software especializado	Cantidad tipo de Software, tiempo en que se requiere, hardware en que se instalara.	Todas las dependencias				
Recurso humano: 1 Jefe de Unidad, 1 secretaria, 1 Jefe de Area de Desarrollo de Sistemas, 6 Analista programador, 1 Analista Funcional, 1 jefe de Area de Administracion de Redes y Bases de Datos, 1 Jefe de Area de Mantenimiento y Soporte Tecnico, 2 Tecnic				Infraestructura: Edificaciones adecuadas y con los recursos necesarios para ejecutar el trabajo. (PRA25-01, 02,12,17 Y 18). Equipos y herramientas informaticas. (PARA 17-03)		

Objetivo del proceso: Proveer a las diferentes dependencias de una plataforma computacional, que combine en forma oportuna y eficiente la infraestructura y los sistemas informaticos que apoyan el que hacer de la comision

INDICE DE MEDICION	FRECUENCIA DE MEDICION	INDICE DE COMPARACION
1. % de Ordenes de Trabajo completadas, # de OT evacuadas/ # de OT asignadas x mes + OT pendientes del mes anterior. 2. Rendimiento del area sobre actividades	Manual Manual	90 % de OT por Area 90% de rendimiento
Mantenimiento y Soporte Tecnico No. de solicitudes evacuadas/Recibidas	Mensual	90 % de solicitudes evacuadas
Administracion de Redes y Bases de Datos No. de solicitudes evacuadas/recibidas No. de caidas de las bases de datos No. de caidas del correo electronico	Mensual	95 % de solicitudes evacuadas max. 2 caidas max. 2 caidas

OT: Ordenes de trabajo

Figura 8: Ficha de proceso PEPSU del proceso de Gestión de la información.

Nombre del Proceso: GESTIÓN DE LA INFORMACIÓN

Desglose de proceso con Flujo de Datos: GESTIÓN DE LA INFORMACIÓN

Procedimientos involucrados:

PRA17-01: "Procedimiento para el desarrollo y/o mantenimiento de sistemas informáticos con recurso interno"

PRA17-02: "Procedimiento para el control y seguimiento del análisis, diseño, desarrollo e implementación de sistemas informáticos creados por terceros"

PRA17-03: "Procedimiento para la detección de necesidades de hardware y software "

PRA17-04: "Ejecución de trabajos de servicios de mantenimiento correctivo a los equipos de computo de CEL y soporte técnico a usuarios"

PRA17-06: "Procedimiento para gestión del mantenimiento preventivo a los equipos de computo de CEL"

PRA17-07: "Procedimiento para alta, baja y cambio de rol de usuarios de servicios informáticos"

Listado de anexos involucrados:

PRA17-01:

Anexo No. 1: Formulario Solicitud de Servicio de TI

Anexo No. 2: Formulario Aprobación de Fase de Proyecto

PRA17-02:

No aplica

PRA17-03:

Anexo 1: Criterios para la Detección de Necesidades de Equipo de Cómputo y/o Software.

Anexo 2: Consolidación de necesidades de actualización y/o reasignación y/o adquisición de equipo de cómputo.

PRA17-04:

Anexo No. 1: Hoja de registro de trabajos de soporte técnico.

PRA17-06:

Anexo No. 1: Gama de recepción del mantenimiento preventivo.

Anexo No. 2: Gama de recepción del mantenimiento preventivo UPS.

Anexo No. 3: Gama de recepción del mantenimiento preventivo SWITCH.

Anexo No. 4: Registro de visitas aleatorias de supervisión de Mantenimiento.

Anexo No. 5: Lista de verificación del cumplimiento de la Normativa de Seguridad para Proteger la Información Electrónica y Equipos de Computación Personal.

Anexo No. 6: Informe sobre la gestión del mantenimiento preventivo a los equipos de cómputo.

Anexo No. 7: Lista de verificación del cumplimiento de la Normativa de Seguridad para Proteger la Información Electrónica y Equipos de Computación Personal – Equipos UPS.

Anexo No. 8: Gama de recepción del mantenimiento de servidores.

PRA17-07:

Anexo No. 1: RC17-003 "SOLICITUD DE ALTA, BAJA Y CAMBIO DE ROL DE USUARIOS"

Nombre del Proceso: GESTIÓN DE LA INFORMACIÓN

Desglose de proceso con Flujo de Datos: GESTIÓN DE LA INFORMACIÓN

Nomenclatura del Desglose de Procesos

A= Variable a evaluar

Ejemplos de Variables

- Solicitudes
- Requerimientos
- Formularios
- Memorándum
- Peticiones, etc.

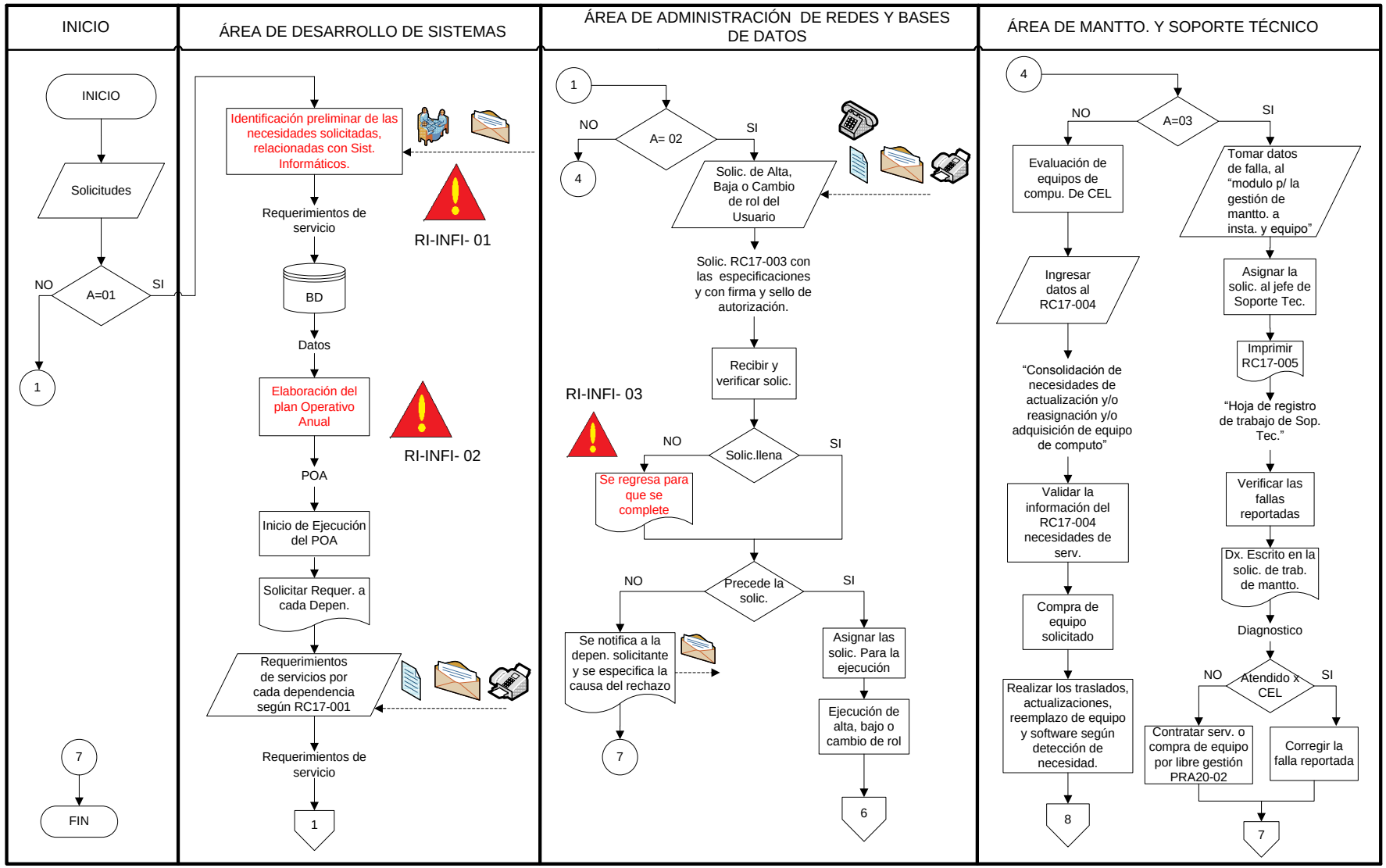
01= Entrada para el área de “DESARROLLO DE SISTEMAS” que utiliza el PRA17-01 y PRA17-02 como procedimientos de ejecución.

02= Entrada para el área de “ADMINISTRACIÓN DE REDES Y BASES DE DATOS” utiliza el PRA17-07 como procedimiento de ejecución.

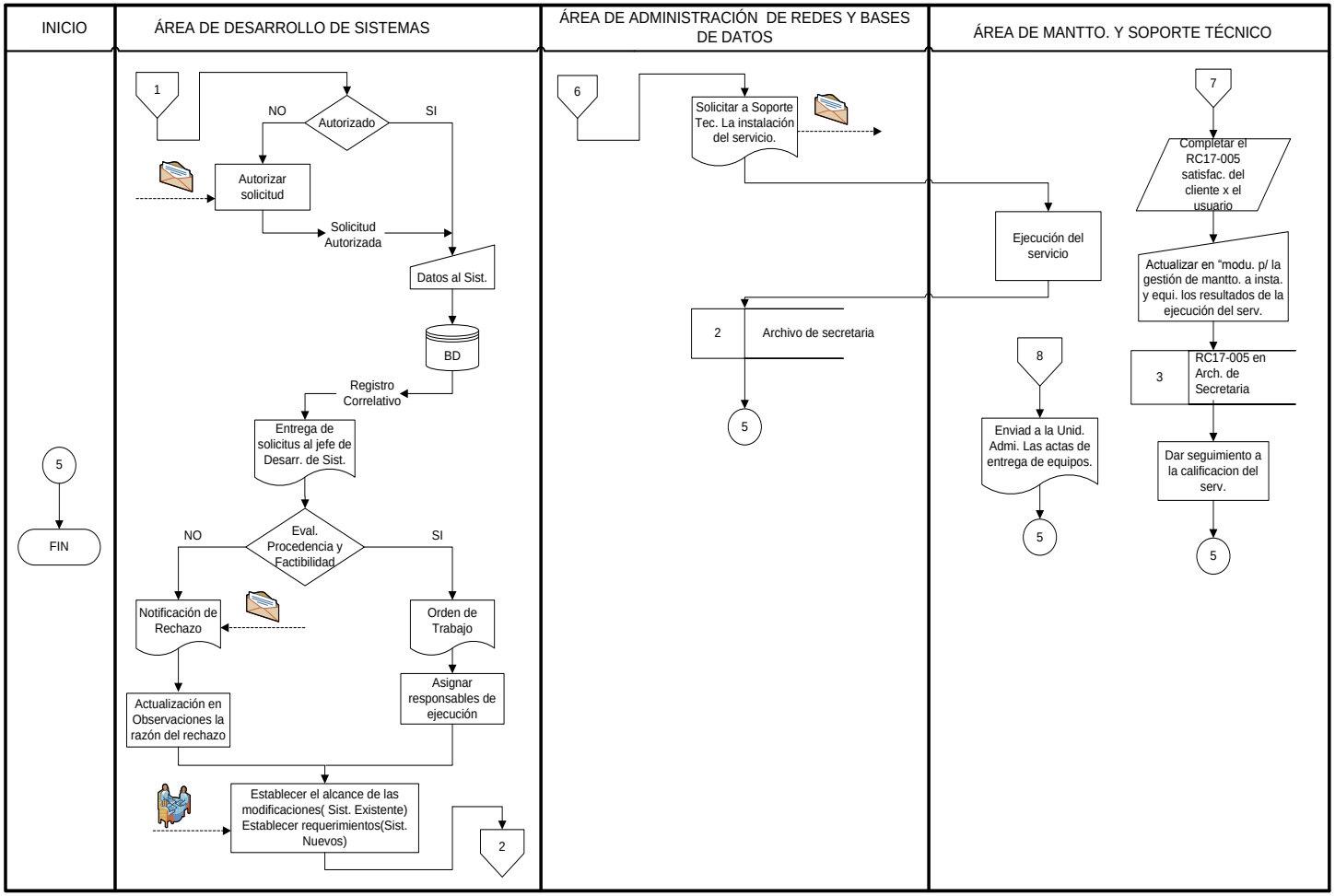
03= Entrada para el área de “MANTENIMIENTO Y SOPORTE TÉCNICO” utiliza el PRA17-03 como procedimiento de ejecución.

04= Entrada para el área de “MANTENIMIENTO Y SOPORTE TÉCNICO” utiliza el PRA17-04 como procedimiento de ejecución.

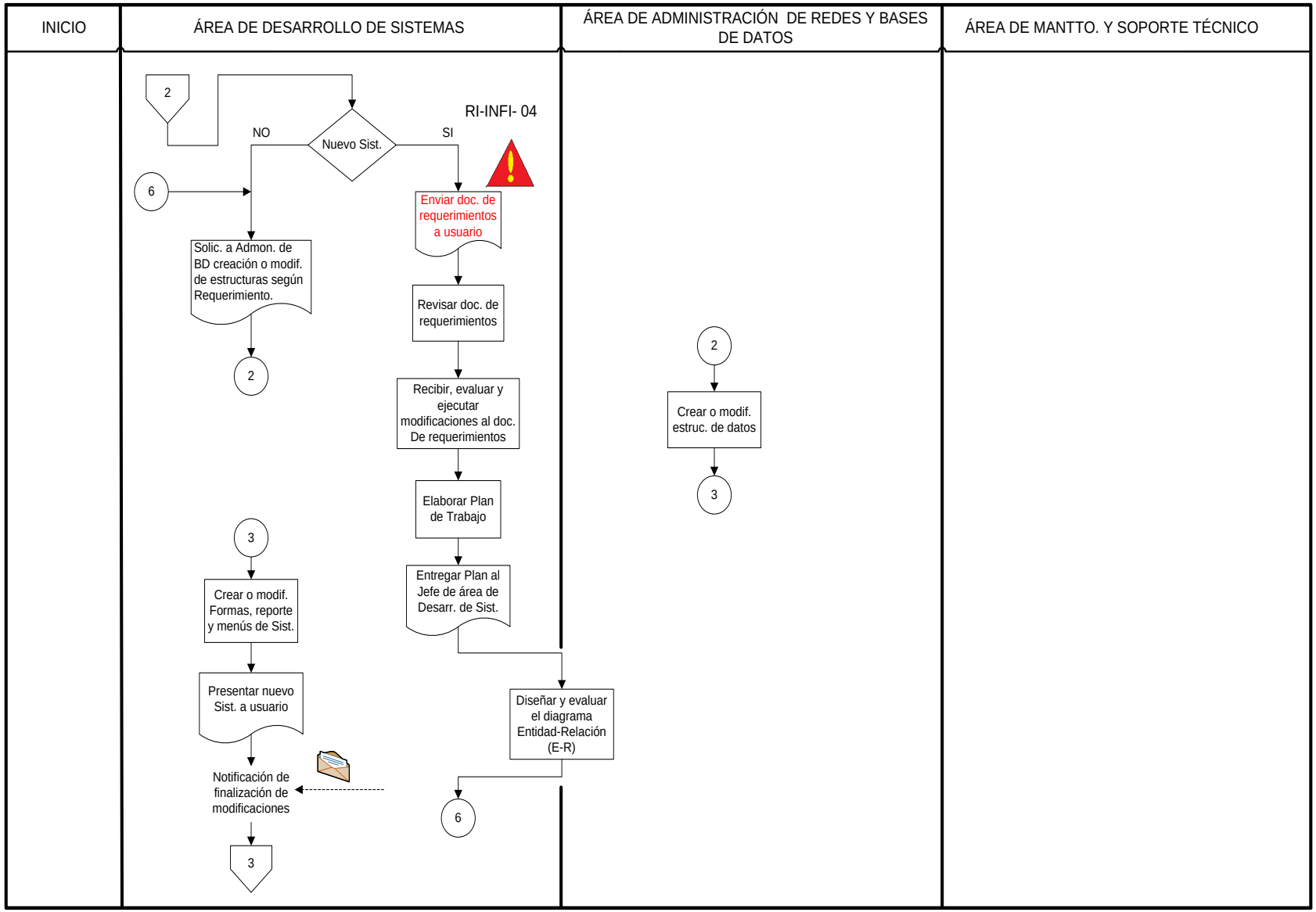
Desglose de proceso con Flujo de Datos: GESTIÓN DE LA INFORMACIÓN



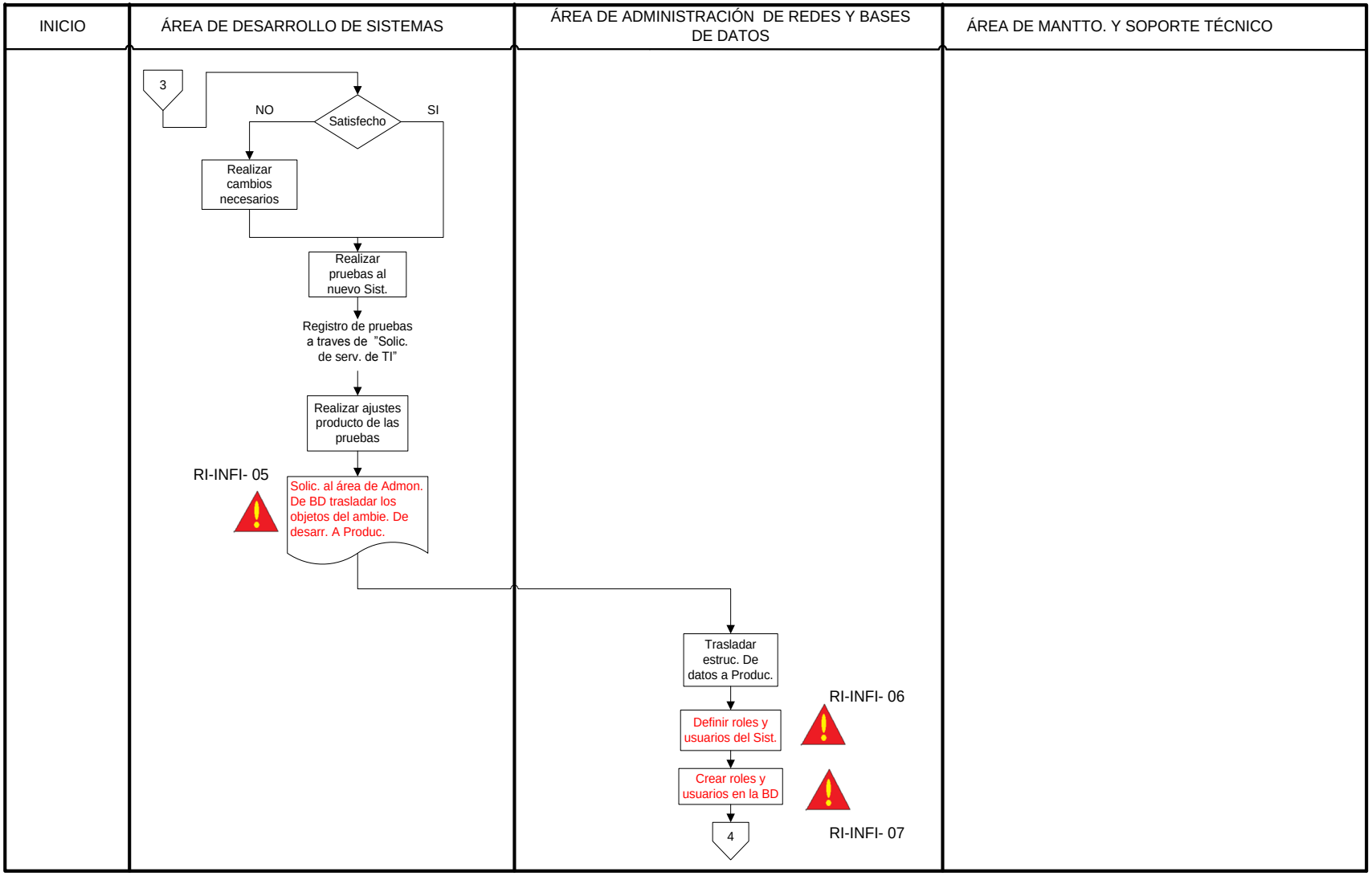
Desglose de proceso con Flujo de Datos: GESTIÓN DE LA INFORMACIÓN



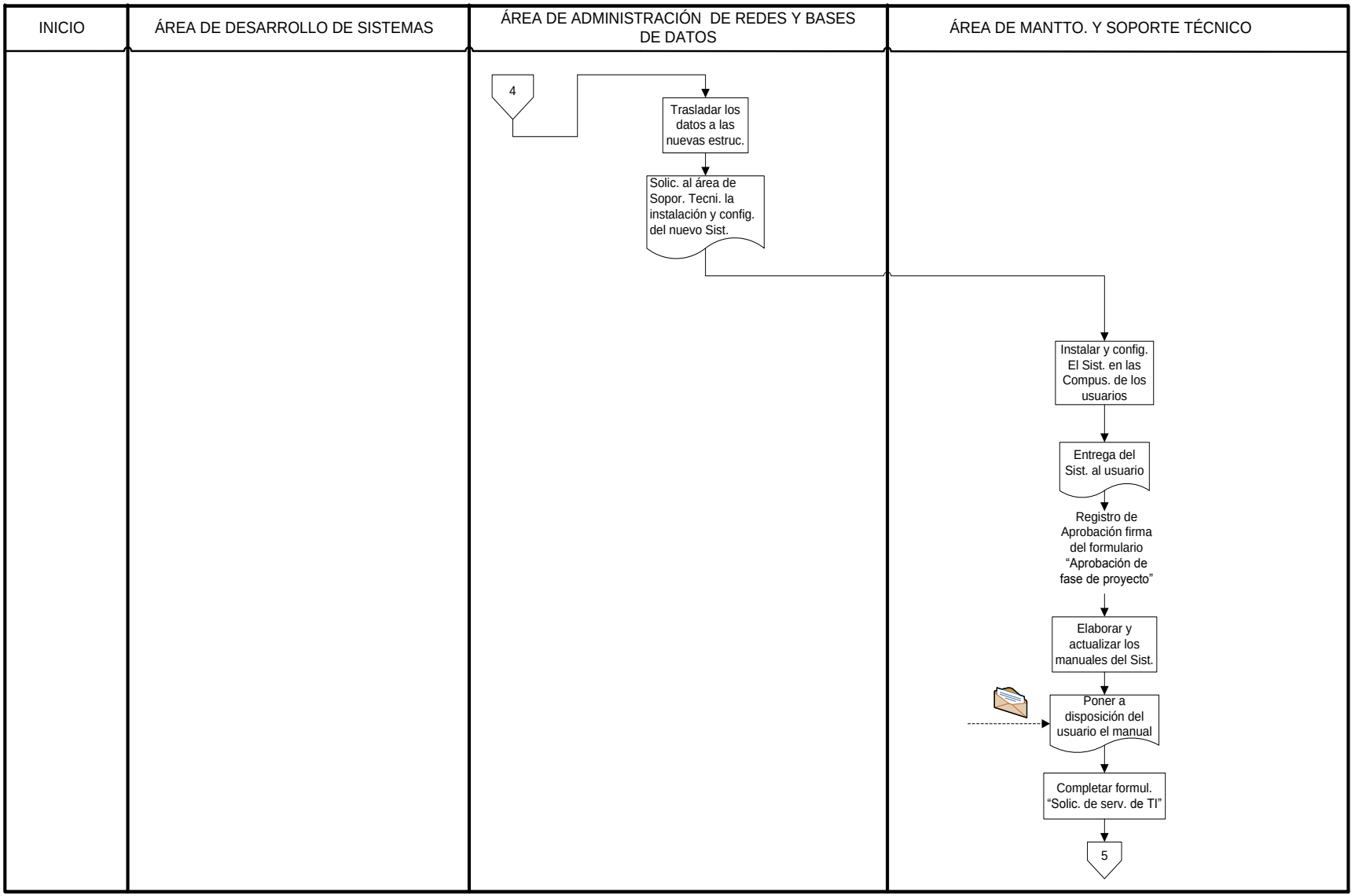
Desglose de proceso con Flujo de Datos: GESTIÓN DE LA INFORMACIÓN



Desglose de proceso con Flujo de Datos: GESTIÓN DE LA INFORMACIÓN



Desglose de proceso con Flujo de Datos: GESTIÓN DE LA INFORMACIÓN



Desglose de proceso con Flujo de Datos: GESTIÓN DE LA INFORMACIÓN

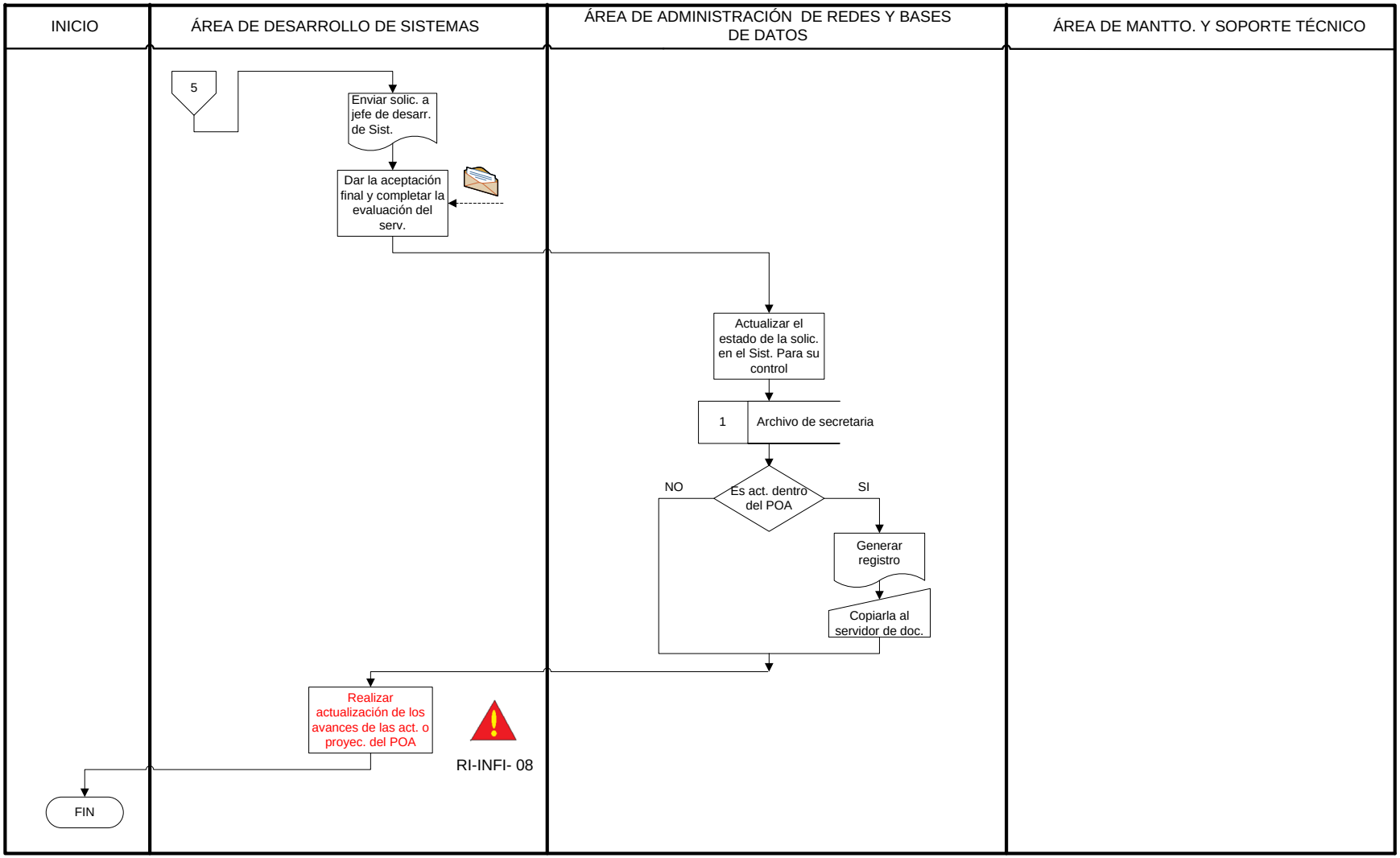


Figura 8: Flujo de proceso con flujo de datos del proceso de Informática.

d. Proceso de Recursos Humanos

A continuación se presenta el listado de procedimientos involucrados en el Proceso de Desarrollo Humano.

Dependencia	Código	Nombre del Procedimiento
Unidad de Desarrollo Humano	PRA22 -01	Procedimiento para la elaboración del plan general de capacitación.
	PRA22-02	Procedimiento para la elaboración del presupuesto del personal.
	PRA22-03	Procedimiento para reclutamiento y selección del personal.
	PRA22-04	Procedimiento para contratación e inducción del personal.
	PRA22-05	Procedimiento para la capacitación del personal.
	PRA22-06	Procedimiento para la elaboración de planillas.
	PRA22-07	Procedimiento para el otorgamiento de prestaciones.
	PRA22-08	Procedimiento para la elaboración del informe anual y constancias de retención de impuestos sobre la renta.
	PRA22-09	Procedimiento para tramitar indemnización del personal.
	PRA22-10	Procedimiento para la atención y seguimiento de enfermedades profesionales.
	PRA22-11	Procedimiento para el programa de medicina preventiva para los empleados de CEL.

Tabla 5: Procedimientos involucrados en el proceso de Desarrollo Humano.

Ambiente : Oficinas en buenas condiciones y en un ambiente de seguridad, orden y limpieza. PARA-17 y 18; PRO41 y PRA21-01

Prosesos de apoyo: Presupuestos, compras , licitaciones, riesgos, (PRA38-02, PRA19-01, PARA20-02, PRA16-01,02,03 Y 04)

ENTRADAS (INSUMOS)

PROCESO RECURSO HUMANO

SALIDAS (PRODUCTOS)

Entradas	Requisitos	Proveedor		SALIDAS	REQUISITOS	CLIENTES
Requerimientos de acciones de personal	Solicitados en forma escrita por las jefaturas de acuerdo a procedimientos y regalmentacion existente: Contrataciones de personal (permanentes, interinos o eventuales), incrementos de sueldo, coverturas de vacaciones con ascensos internos, trasalados, per	Todas las Jefaturas	**ACCIONES DE PERSONAL** PRA22-03 Procedimiento para el reclutamiento y selección del personal PRA22-04 Procedimiento para la contratacion e induccion de personal	* Personal contratado y con induccion recibida * Acciones de personal autorizadas, notificadas y ejecutadas (permisos con y sin goce de sueldo,incrementos salariales, terminaciones	* Candidatos propuestos con resultados satisfactorios en procesos de selección aprobados por la jefatura de la dependencia solicitante * Acciones de personal autorizadas por la direccion s	Dependencia solicitantes
Variables reportadas para elaboracion de planillas	Permisos con o sin goce de sueldo, vacaciones, ingresos, terminaciones de contrato, reportes de llegadas tardias, etc. Según el Reglamento interno de Trabajo	Todas las Jefaturas	**ADMINISTRACION DE PLANTILLAS** PRA22-06 Procedimiento para la elaboracion de planillas	Plantillas reportadas para su correspondiente pago	* Informacion presentada deacuerdo al calendario de pagos . * Informacion correcta	Deparatamento de tesoreria Todo el personal de la comision
Requerimientos de capacitacion del personal	Aprobadas por jefes inmediatos y que esten orientadas a reforzar o mejorara competencias	Todas las Jefaturas	**CAPACITACION** PRA22-01 Procedimiento para la elaboracion del plan anual de capacitacion, PRA22-05 Procedimiento para la capacitacion del personal	* Plan anual de capacitacionaprobado y ejecutado * Otras capacitaciones autorizadas y ejecutadas	* Ejecucion de las capacitaciones de acuerdo con plan de capacitacion o solicitudes adicionales recibidas y autorizadas	Dependemcias solicitantes
Solicitud de Prestaciones	Solicitadas por el personal de acuerdo a procedimientos y reglamentos existentes: Locaciones Costa CEL, controles de niño zano y embarazo, aros y lentes, etc. Coordinadas por la unidada de desarrollo Humano Previa autorizacion	Todo el personal de la comision	**PRESTACIONES** PRA22-07 Procedimiento para el otorgamiento de prestaciones	Aptos. Y glorietas de costa cel asignados, uniformes entregados, controles de embarazo y niño sano entregados, excurciones realizadas, tornros deportivos realizados	* Otorgamiento de acuerdo a los procedimientos y presupuestos autorizados * Satisfaccion del cliente	Todo el personal de la comision
Evaluaciones individuales del personal	Completadas y generadas en el sistema de evaluacion de desempeño empresarial, firmadas por los empleados y por los jefes inmediatos	Jefaturas de las dependenciasde la comisison	**MEDICION DEL DESEMPEÑO INDIVIDUAL** PRA06-02: Procedimiento parar la medicion del desempeño del personal.	* personal con resultados obtenidos en la evaluacion del desempeño individual	* 70% resultados obtenidos en el cumplimiento de objetivos de dependencia y 30% en el cumplimiento de competencias	Todo el personal de la comision

RECURSO HUMANO: 1 jefe de unidad, 3 colaboradores administrativos, 5 analistas de desarrollo humano, un encargado de capacitacion, 1 colaborador de prestaciones, 1 ingeniero de sistemas, 1 jefe de area, 1enfermera y 2 medicos internistas . Total 19 empleados.

Infraeastructura: Edificaciones adecuadas y con los recursos necesarios para ejecutar el trabajo. (PRA25-01,02,12,17 y 18)

Figura 9: Ficha de proceso PEPSU del proceso de Desarrollo Humano

Nombre del proceso: PROCESO DE RECURSO HUMANO

Desglose de proceso con Flujo de Datos: PROCESO DE RECURSO HUMANO

Procedimientos involucrados:

PRA22-01: “Procedimiento para la elaboración del plan anual de capacitación”
PRA22-03: “Procedimiento para el reclutamiento y selección de personal”
PRA22-04: “Procedimiento para la contratación e inducción de personal”
PRA22-05: “Procedimiento para la capacitación del personal”
PRA22-06: “Procedimiento para la elaboración de planillas”
PRA22-07: “Procedimiento para el otorgamiento de prestaciones”
PRA22-09: “Procedimiento para tramitar indemnizaciones del personal”
PRA06-02: “Procedimiento para la medición del desempeño empresarial”

Listado de anexos involucrados:

PRA22-01:

Anexo No. 1: Políticas y Normas de Capacitación
Anexo No. 2: Detección de Necesidades de Capacitación (DNC)
Anexo No. 3: Formulario para la detección de necesidades de capacitación
Anexo No. 4: Instructivo para la elaboración del plan general de capacitación
Anexo No. 5: Formulario de cédula didáctica

PRA22-03:

Anexo No. 1: Evaluación de factibilidad de cobertura de una plaza vacante
Anexo No. 2: Manejo y actualización del manual de descripción de puestos
Anexo No. 3: Instructivo para gestionar concurso interno
Anexo No. 4: Formulario para investigación de referencias de trabajo
Anexo No. 5: Formulario para la investigación de referencias personales
Anexo No. 6: Instructivo para aplicación y procesamiento de pruebas a los aspirantes que participan en el proceso de selección
Anexo No. 7: Formulario de oferta de servicios
Anexo No. 8: Entrevista para proceso de selección
Anexo No. 9: Descripción de puesto
Anexo No. 10: Cuadro comparativo de resultados
Anexo No. 11: Formulario para investigación de referencias laborales para concurso interno

PRA22-04:

Anexo No. 1: “Requisitos de candidatos propuestos para contratación”
Anexo No. 2: “Tareas relacionadas con trámites de Contratación”
Anexo No. 3: “Desarrollo del programa de inducción a trabajadores de nuevo ingreso”
Anexo No. 4: "Evaluación de desempeño del personal en período de prueba”
Anexo No. 5: “Hoja de Confirmación de Datos”
Anexo No. 6: “Propuesta de Acción de Personal”
Anexo No. 7: “Notificación de Acción de Personal”
Anexo No. 8: “Inscripción de beneficiarios de su grupo familiar”.
Anexo No. 9: “Contrato individual de trabajo”
Anexo No. 10: “Formulario, para evaluación del desempeño de período de prueba”.
Anexo No. 11: “Control de Inducción Impartida por el Departamento de Personal, a personal de nuevo ingreso”
Anexo No 12: “Control de inducción de Sistema de Gestión Integrada impartida a personal de nuevo ingreso”
Anexo No. 13: “Reforma de contrato individual de trabajo”

PRA22-05:

Anexo 1: Gestión de capacitaciones cubiertas en su totalidad con fondos propios de CEL.
Anexo 2: Formulario cuadro comparativo de ofertas de servicios de capacitación
Anexo 3: Evaluación de Seminarios
Anexo 4: Registro de capacitaciones impartidas
Anexo 5: Encuesta para el seguimiento de la capacitación
Anexo 6: Listado de asistencia
Anexo 7: Formulario informe de resultados de la efectividad de la capacitación

PRA22-06:

ANEXO No. 1: “Instructivo para registro de ingreso y salida del personal”
ANEXO No. 2: “Instructivo para registro y control de permisos e incapacidades “
ANEXO No. 3: RC22-012 “Formulario de horas extras”
ANEXO No. 4: RC22-013 “Formulario de reporte para cobro de viáticos”
ANEXO No. 5: RC22-038 “Formulario de reporte de trabajo del personal jornal”
ANEXO No. 6: “Instructivo para elaborar planillas de salarios del personal jornal”
ANEXO No. 7: “Instructivo para elaborar planillas de salarios del personal mensual”
ANEXO No. No. 8: “Instructivo para elaborar planillas de vacaciones del personal jornal, mensual y ejecutivo”
ANEXO No. 9: “Instructivo para elaborar planillas de bonificación”
ANEXO No. 10: “Instructivo para elaborar planillas de aguinaldo”
ANEXO No. 11: “Instructivo para la elaboración planilla del IPSFA”
ANEXO No. 12: “Instructivo para la elaboración planilla del ISSS, AFP e INPEP”
ANEXO No. 13: “Instructivo para la elaboración planilla del INSAFORP”
ANEXO No. 14: “Instructivo para completar la declaración del impuesto sobre la renta”
ANEXO No. 15: RC22-014 “Cuadro de Liquidación de planillas de INSAFORP”
ANEXO No. 16: RC22-015 “Formato de constancia de pago de cotización“
ANEXO No. 17: RC22-016 LIQUIDACIÓN DE COTIZACIONES AL (IPSFA, INPEP, ISSS) PERSONAL (MENSUAL) (MES Y AÑO)
ANEXO No. 18: RC22-017 LIQUIDACIÓN DE RENTA MENSUAL
ANEXO No. 19: “Instructivo para cargar los salarios a través del sistema Pc_BAC del Banco Agrícola”
ANEXO No. 20: “Instructivo para cargar el salario a través del sistema NETBANKING del Banco Cuscatlán”
ANEXO No. 21: “Instructivo de generación del disquete y la planilla de pago para el Fondo Social para la Vivienda”
ANEXO No. 22: RC22-039 “Reporte de clasificación de días laborados, horas extras y viáticos del personal jornal”
ANEXO No. 23: RC22-040 “Resumen de datos básicos de los días laborados, horas extras y viáticos del personal jornal”

PRA22-07:

ANEXO No. 1: “Instructivo para la adquisición y asignación de uniformes al personal femenino y masculino”
ANEXO No. 2: “Instructivo para la asignación de capas y paraguas”
ANEXO No. 3: “Instructivo para la asignación de calzado de seguridad”
ANEXO No. 4: “Instructivo para la adquisición y entrega de café y azúcar a las dependencias“
ANEXO No. 5: “Instructivo para el otorgamiento de Becas para hijos de trabajadores”
ANEXO No. 6: “Instructivo para la asignación de apartamentos y glorietas del centro social costa CEL”
ANEXO No. 7: “Instructivo para realización de excursiones”
ANEXO No. 8: “Instructivo para ayudas por defunción de trabajador o familiar”
ANEXO No. 9: “Instructivo para tramitar autorización de la prestación económica para la adquisición de aros y lentes”
ANEXO No. 10: “Instructivo para registro y autorización de órdenes para control de niño sano”
ANEXO No. 11: “Instructivo para registro y autorización de órdenes para control de embarazo”
ANEXO No. 12: “Instructivo para realizar intramuros deportivos”
ANEXO No. 13: “Instructivo para el otorgamiento de permisos”
ANEXO No. 14: “Formulario de solicitud para aspirante a becas”
ANEXO No. 15: “Solicitud de ayuda por gastos funerarios”
ANEXO No. 16: “Informe de ayuda por defunción de familiares.”
ANEXO No. 17: “Formulario de solicitud permiso por estudios”
ANEXO No. 18: “Formulario de solicitud de permiso”
ANEXO No. 19: “Formulario de solicitud Costa CEL”
ANEXO No. 20: “Formulario Orden de Descuento Centro Social Costa CEL”
ANEXO No. 21: “Recibo de pago por entrega de subsidio para uniformes y entrega prestación de calzado”
ANEXO No. 22: RC22-025 “formulario de carta compromiso entrega subsidio uniformes masculinos”
ANEXO No. 23: RC22-032

Nombre del proceso: PROCESO DE RECURSO HUMANO
Desglose de proceso con Flujo de Datos: PROCESO DE RECURSO HUMANO

PRA22-09:

Anexo No. 1: Instructivo para el cálculo de indemnización del personal
Anexo No. 2: Cálculo de indemnización
Anexo No. 3: Formato de recibo de indemnización
Anexo No. 4: Hoja de aplicación del Impuesto sobre la Renta en Indemnización
Anexo No. 5: Formato de Finiquito 1
Anexo No. 6: Formato de Finiquito por recibir pasivo laboral

PRA06-02:

Anexo No. 1: Ciclo del SIMEDE.
Anexo No. 2: Etapa de Planificación
Anexo No. 3: Etapa de Seguimiento
Anexo No. 4: Etapa de Evaluación

Nomenclatura del Desglose de Procesos

A= Variable a evaluar

Ejemplos de Variables

- Solicitudes
- Requerimientos
- Formularios
- Memorándum
- Peticiones, etc.

01= Entrada para el área de "ACCIONES DE PERSONAL"

011= ACCIÓN DE PERSONAL que utiliza el PRA22-03 y PRA22-04 como procedimiento de ejecución.

012= ACCIÓN DE PERSONAL que utiliza el PRA22-09 como procedimiento de ejecución.

02= Entrada para el área de "ADMINISTRACIÓN DE PLANILLA" utiliza el PRA22-06 como procedimiento de ejecución.

03= Entrada para el área de "CAPACITACIÓN"

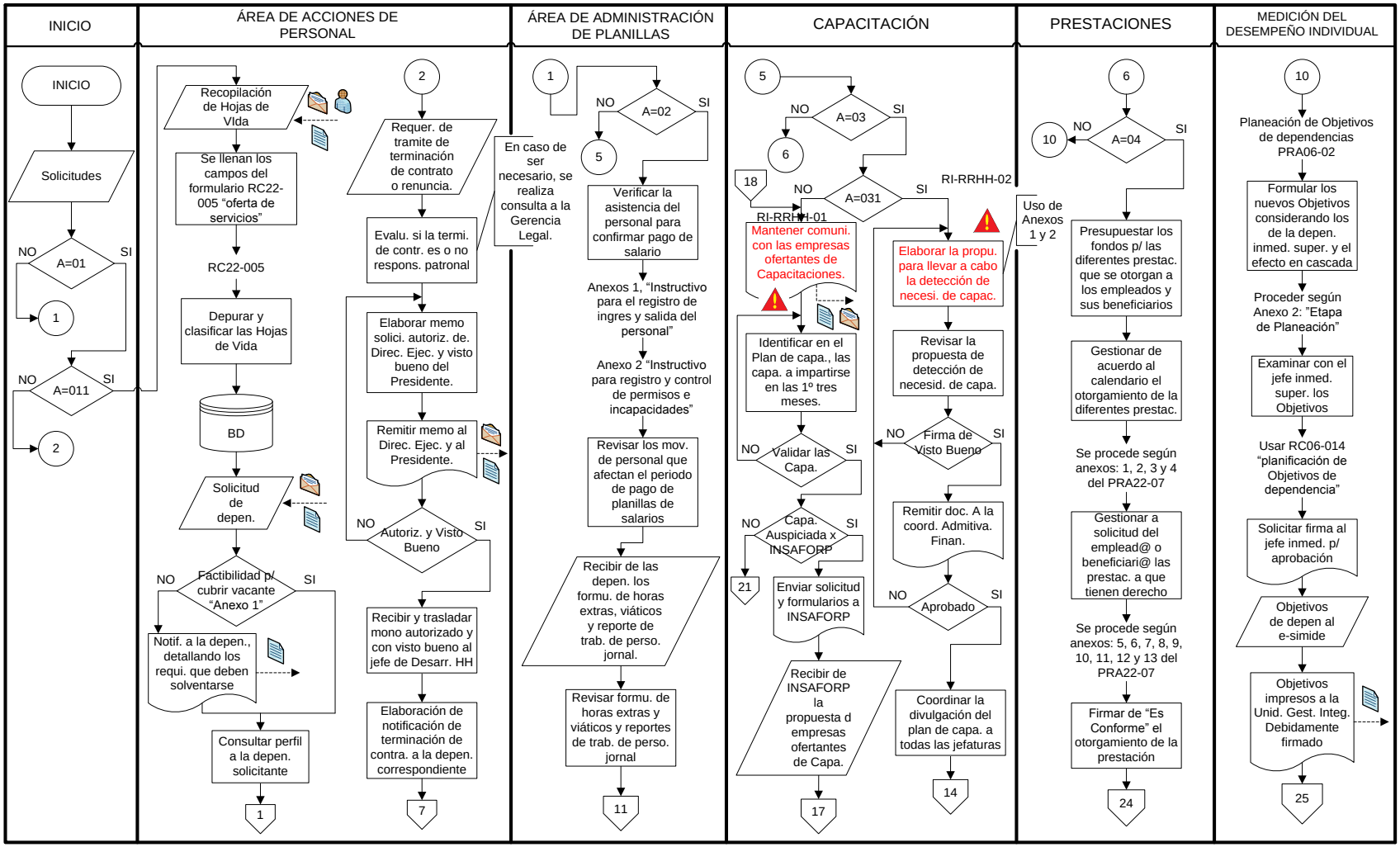
031= REQUERIMIENTO que utiliza el PRA22-01 como procedimiento de ejecución.

032= REQUERIMIENTO que utiliza el PRA22-05 como procedimiento de ejecución.

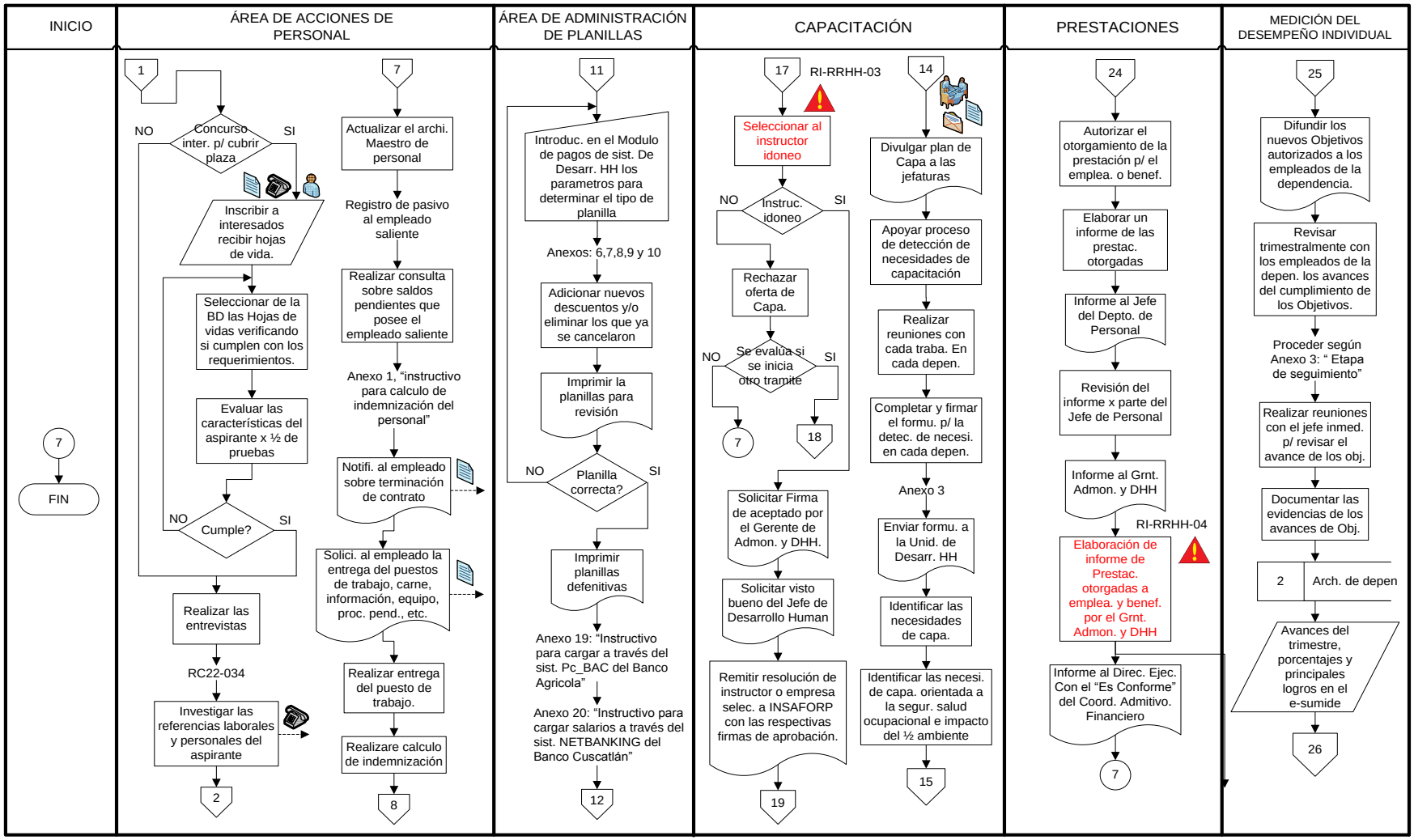
04= Entrada para el área de "PRESTACIONES" utiliza el PRA22-07 como procedimiento de ejecución.

05= Entrada para el área de "MEDICIÓN DE DESEMPEÑO INDIVIDUAL" utiliza el PRA22-06 como procedimiento de ejecución.

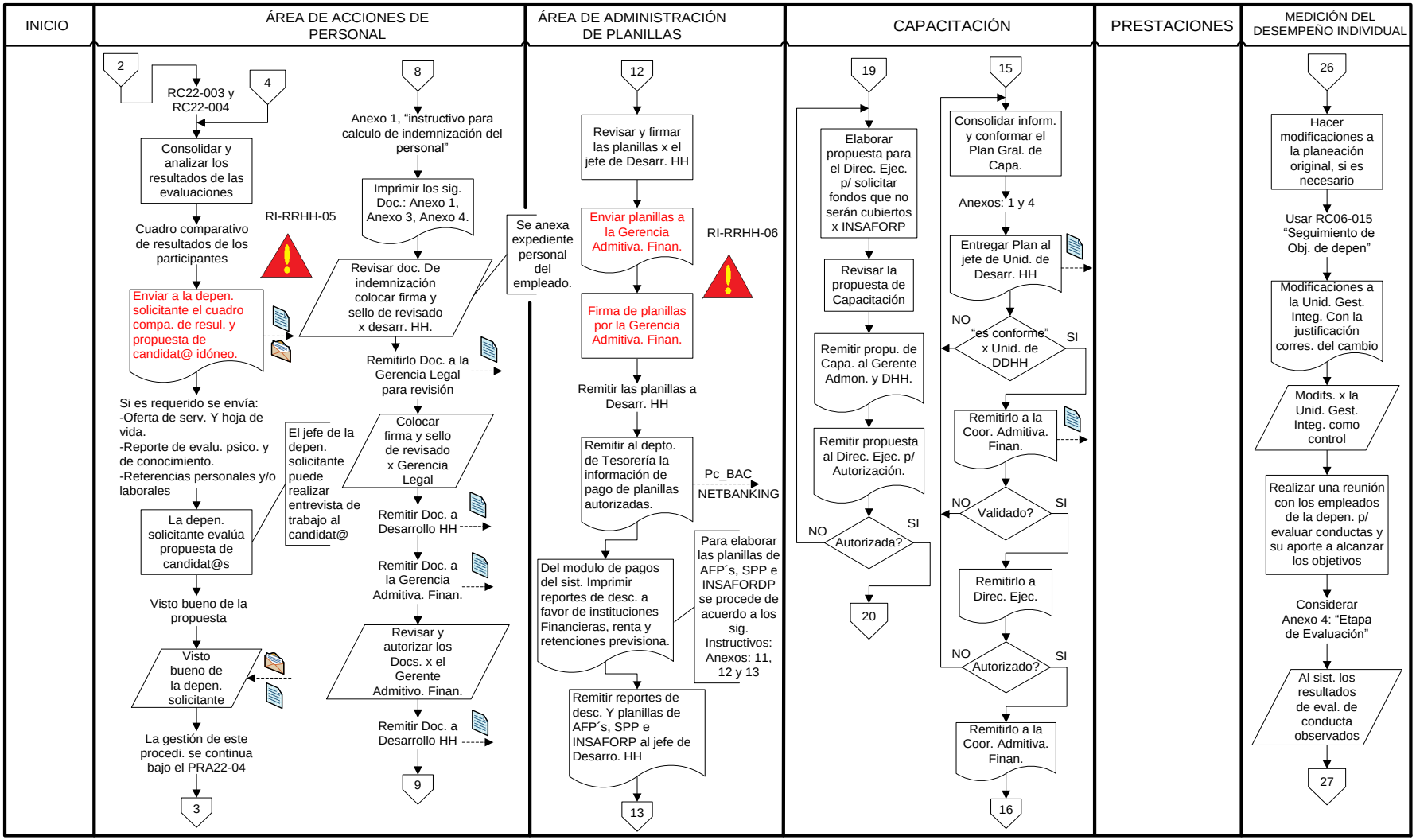
Desglose de proceso con Flujo de Datos: PROCESO DE RECURSO HUMANO



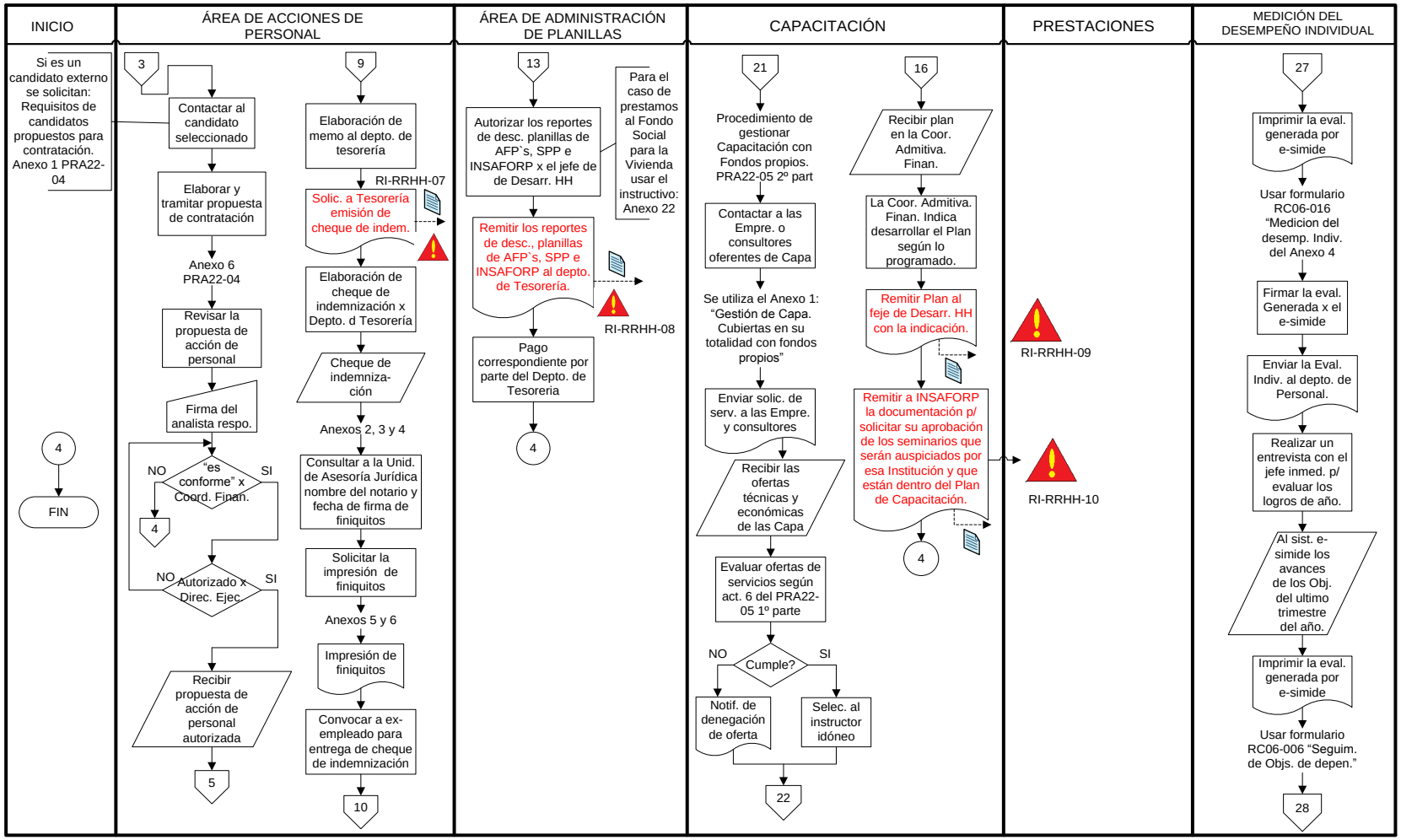
Desglose de proceso con Flujo de Datos: PROCESO DE RECURSO HUMANO



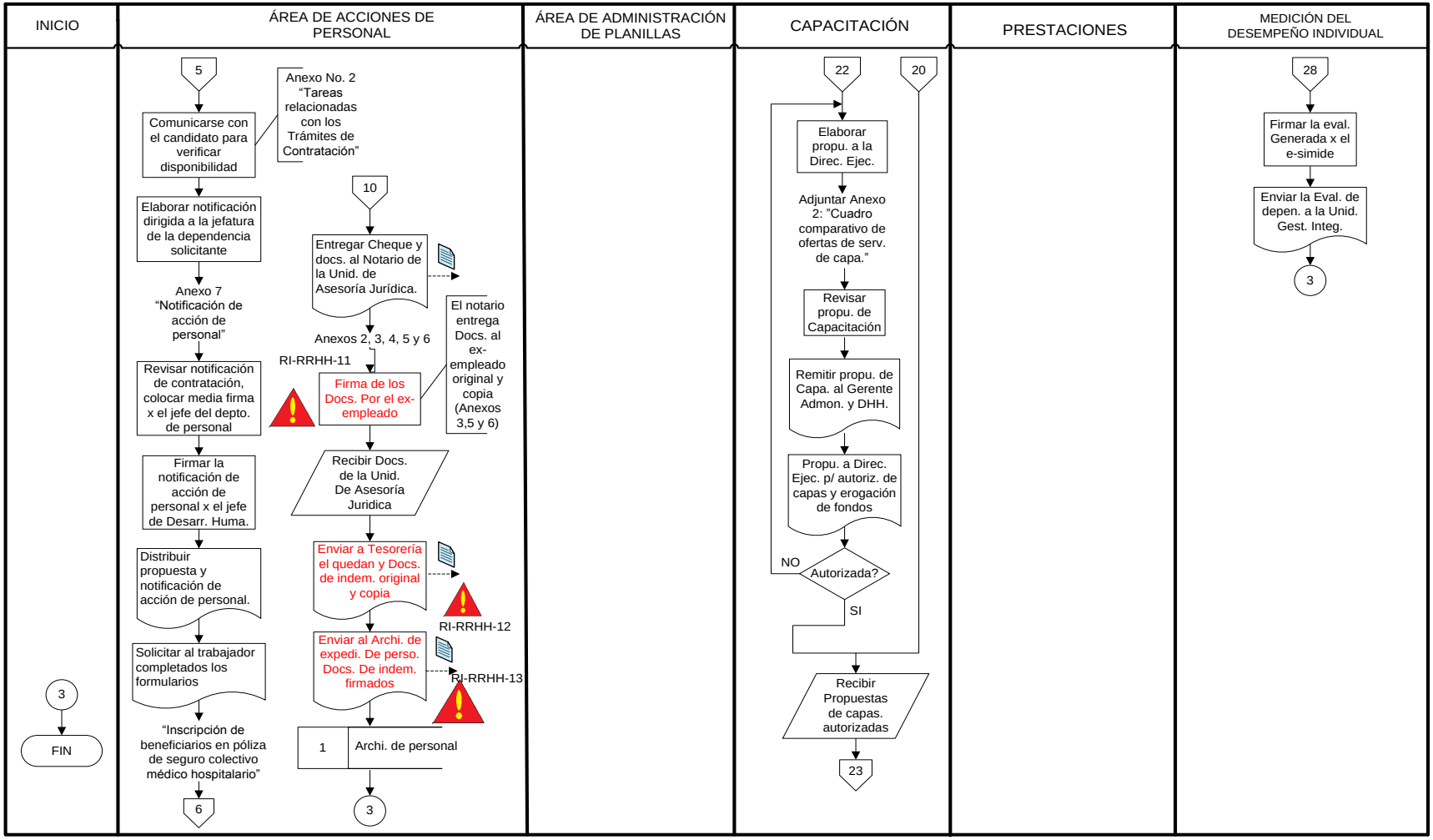
Desglose de proceso con Flujo de Datos: PROCESO DE RECURSO HUMANO



Desglose de proceso con Flujo de Datos: PROCESO DE RECURSO HUMANO



Desglose de proceso con Flujo de Datos: PROCESO DE RECURSO HUMANO



Desglose de proceso con Flujo de Datos: PROCESO DE RECURSO HUMANO

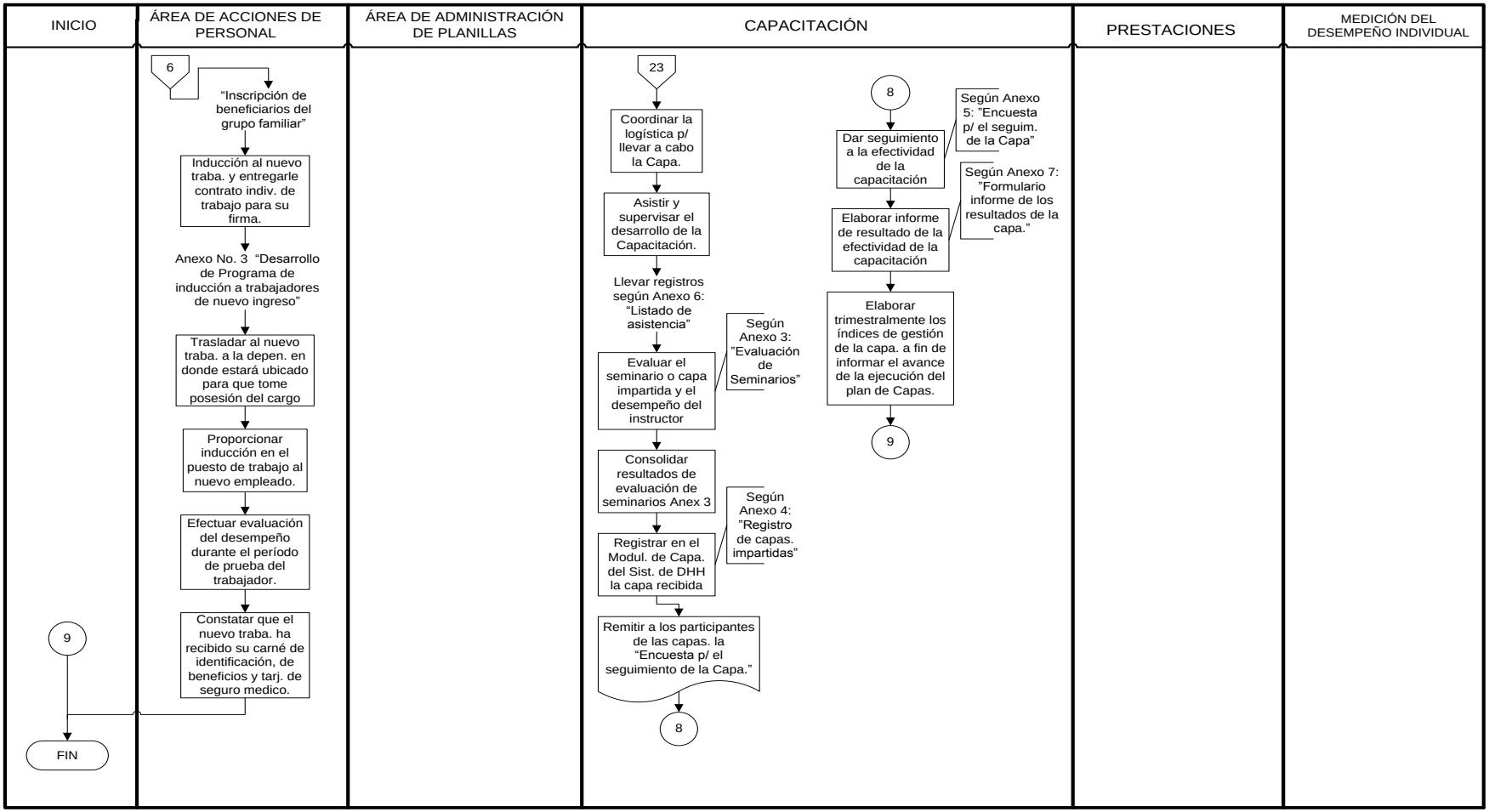


Figura 10: Flujo de proceso y flujo de datos del proceso de Desarrollo Humano.

C. MAPA DE PROCESOS

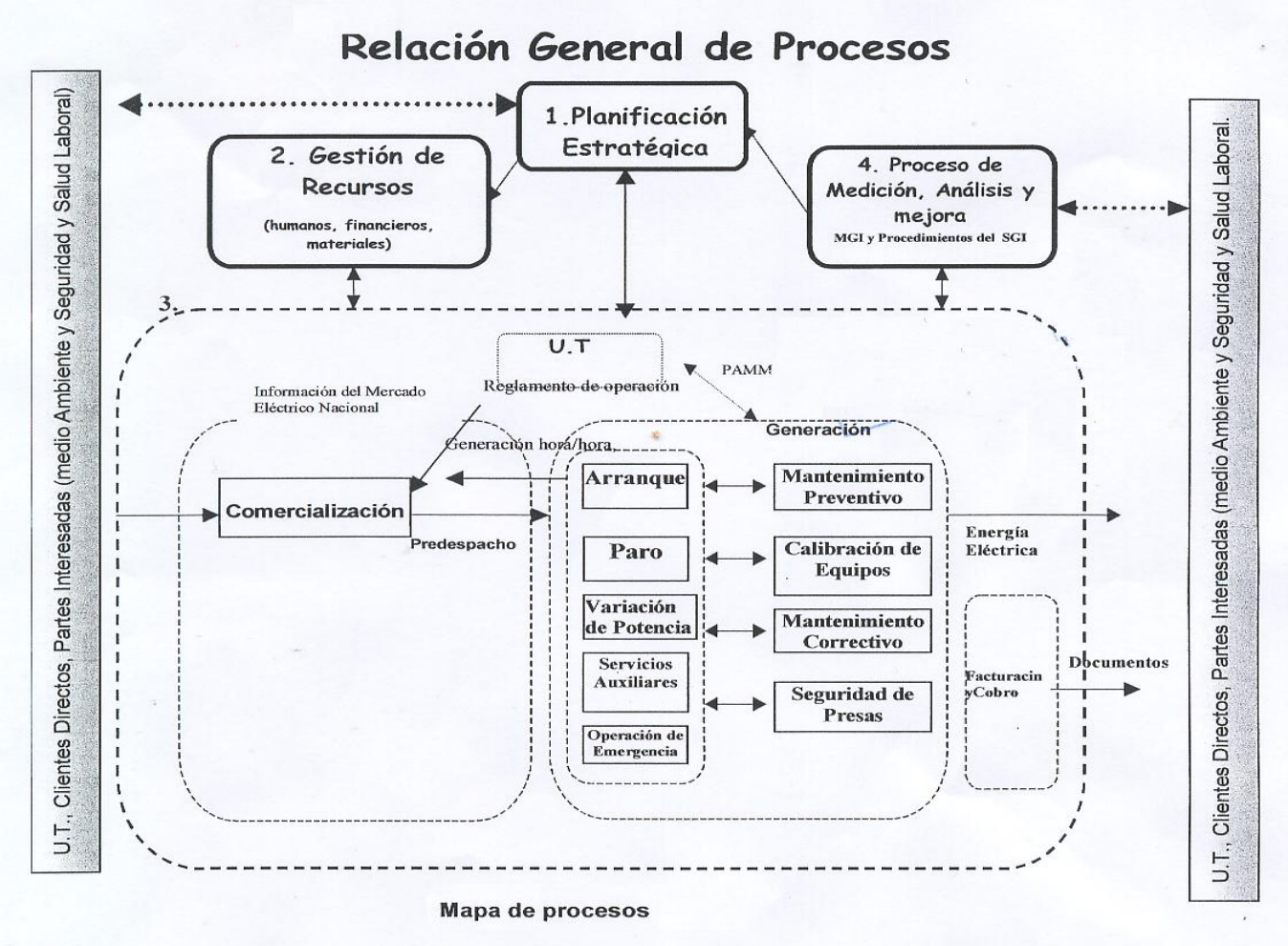


Figura 11: Mapa de procesos de CEL.

D. DISPOSICIONES LEGALES

El presente documento se emite de conformidad a lo establecido en las NTCI de CEL y en sus objetivos que establecen lo siguiente:

Objetivos Generales del Sistema de Control Interno

Art. 3.- El Sistema de Control Interno tendrá como finalidad coadyuvar al cumplimiento del siguiente objetivo:

> *Promover operaciones económicas, eficientes y eficaces en el manejo de los recursos naturales, humanos, materiales, financieros y tecnológicos relacionados con la generación y comercialización de energía eléctrica*.

Dicho objetivo plantea promover operaciones eficientes y eficaces en el manejo de los recursos de todo tipo, este objetivo es clave para echar a andar un SGSI ya que ayudara en gran manera a cumplirlo.

De igual forma se establece lo siguiente:

Componentes Orgánicos del Control Interno

Art. 4.- Los procedimientos de control interno establecidos por la Junta Directiva, deberá asegurar el cumplimiento de las directrices administrativas en el quehacer de la Institución y serán aplicadas por todo el personal que la integra, siendo sus componentes: ambiente de control, valoración de riesgos, actividades de control, monitoreo, información y comunicación.

Art. 6.- La valoración de riesgos comprenderá: la identificación, análisis y administración de riesgos relevantes para la consecución de los objetivos estratégicos.

Art. 7.- Las actividades de control incluirá: aprobaciones, autorizaciones, verificaciones, conciliaciones, revisión, seguridad, segregación de responsabilidades y auditorías.

Art. 8.- La información y la comunicación comprenderá: relaciones públicas, manejo de información interna con medios de comunicación social e instituciones públicas y privadas, administración de archivo institucional y de documentos.

Art. 9.- El monitoreo comprenderá: evaluaciones en la marcha, mediante autoevaluaciones y auditorías.

E. COMPROMISO DE LA GERENCIA

El compromiso surgió desde el momento en que el la Dirección Ejecutiva aprobó el desarrollo del proyecto del SGSI, los principales compromisos que la gerencia adopta son los siguientes:
La gerencia debe desempeñar un papel protagónico en el manejo de un SGSI. La gerencia deberá apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.
La gerencia deberá:

a) Asegurar que los objetivos de seguridad de la información estén identificados, cumplan con los requerimientos organizacionales y estén integrados en los procesos relevantes;
b) Formular, revisar y aprobar la política de seguridad de la información;
c) Revisar la efectividad de la implementación de la política de seguridad de la información;
d) Proporcionar una dirección clara y un apoyo gerencial visible para las iniciativas de seguridad;
e) Proporcionar los recursos necesarios para la seguridad de la información;
f) Aprobar la asignación de roles y responsabilidades específicas para la seguridad de la información a lo largo de toda la organización;
g) Iniciar planes y programas para mantener la conciencia de seguridad de la información;
h) Asegurar que la implementación de los controles de seguridad de la información sea coordinado en toda la organización.

La gerencia debiera identificar las necesidades de consultoría especializada interna o externa para la seguridad de la información, y revisar y coordinar los resultados de la consultoría a través de toda la organización. Para lograr una adecuada integración de todas las personas relacionadas con la seguridad de la información, una buena práctica es tener sus descripciones de puestos y sus responsabilidades frente a la seguridad de la información.
La gerencia es la responsable de que en la organización se divulguen los objetivos y políticas de seguridad y se comunique la importancia de alcanzar los objetivos y cumplir con las políticas establecidas, las responsabilidades que como organización se deben cumplir bajo la ley y el compromiso de ferviente sentido de mejora continua. Así mismo la gerencia debe proporcionar los recursos suficientes para desarrollar, implementar, operar y mantener el SGSI.
Tiene la tarea de establecer el criterio para la aceptación del riesgo y los niveles permisibles, es decir debe de especificar las opciones más apropiadas para el tratamiento del riesgo de una manera clara y documentada.
Otro de los aspectos que como gerencia debe realizarse es asegurar que se realicen las auditorías internas al SGSI, así como realizar revisiones gerenciales. Esto con el fin de legitimar que todos y cada uno de los factores involucrados en el desarrollo, implementación, operación y mantenimiento del SGSI estén debidamente interrelacionados y focalizados al cumplimiento de los objetivos del mismo, garantizando así el buen manejo y la seguridad de la información, activo vital de las organizaciones.

CAPITULO II: MARCO TEORICO SOBRE LA ISO 27000

A. DEFINICIONES

- INFORMACIÓN

Información es un conjunto organizado de datos **procesados**, que constituyen un mensaje sobre un determinado ente o fenómeno. Según su naturaleza esta adquiere valor para quien la posee.

- MANEJO DE LA INFORMACIÓN

El manejo de información, es el desarrollo de un conjunto de habilidades técnicas y tecnológicas que permiten definir la información necesaria, obtenerla y aprovecharla; para lograr rapidez, reducir el esfuerzo, representar y comunicar la información.

- SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información es el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, con el fin de minimizar las amenazas y riesgos continuos a los que está expuesta, a efectos de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de inversiones y las oportunidades del negocio. Y en el caso de cada individuo de proteger la identidad y la privacidad.

- GESTIÓN DE LA SEGURIDAD

La gestión de la seguridad consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización.

- SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de la Seguridad de la Información (SGSI): Es el sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.

B. ANTECEDENTES NORMA ISO 27000

Antecedentes de la Norma ISO 27000

La norma ***BS 7799 de BSI*** (British Standards Institution, "Instituto de Normalización Británico" la organización británica equivalente a AENOR en España) aparece por primera vez en 1995, con el objeto de proporcionar a cualquier empresa –británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación.

Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, es la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.
En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó la ISO 17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

ESQUEMA DE EVOLUCIÓN DE ISO 27000

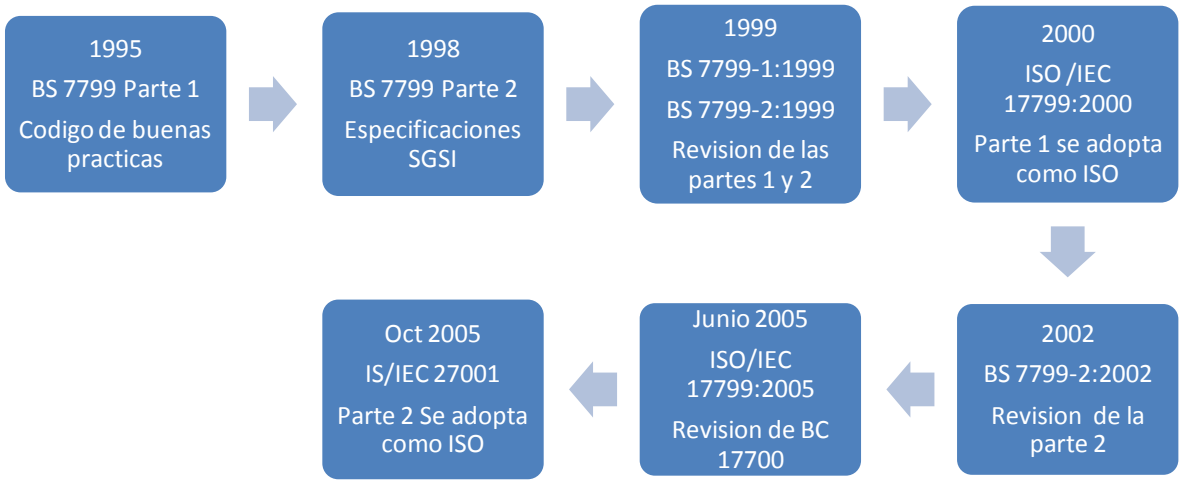


Figura 12: Esquema de evolución de la ISO 27000.

En Marzo de 2006, posteriormente a la publicación de la ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

C. PRINCIPIOS DE LA GESTIÓN DEL MANEJO Y SEGURIDAD DE LA INFORMACIÓN

A continuación se presentan los ocho principios de la Gestión de Calidad, en los cuales se basan las normas para la creación de Sistemas de Gestión de Calidad bajo la serie ISO 9000:2000; estos principios descritos de manera general proporcionan la base primordial de donde se desagregan los principios fundamentales de la Gestión del Manejo y Seguridad de la Información de la serie ISO 27000.

№	PRINCIPIO	DESCRIPCIÓN
1	Enfoque al cliente	Las organizaciones dependen de sus clientes y por lo tanto deberían comprender las necesidades actuales y futuras de los clientes, satisfacer los requisitos de los clientes y esforzarse en exceder las expectativas de los clientes.
2	Liderazgo	Los líderes establecen unidad de propósito y dirección en una organización. Ellos deben crear y mantener el clima interno en el cual las personas puedan sentirse totalmente involucradas con el logro de los objetivos organizacionales.
3	Participación/Involucramiento del Personal	El personal, en todos sus niveles, es la esencia de la organización y su total involucramiento posibilita el uso de sus habilidades en beneficio de la organización.
4	Gestión por Procesos/Enfoque basado en Procesos	El resultado deseado es alcanzado con mayor eficiencia gestionando los recursos y actividades relacionadas como un proceso.
5	Gestión a través de Sistemas /Enfoque de Sistemas para la Gestión.	Identificar, comprender y gestionar un sistema de procesos interrelacionados para un objetivo dado mejora la eficacia y la eficiencia de una organización.
6	Mejora Continua	La mejora continua debe ser un objetivo permanente en la empresa.
7	Enfoque basado en hechos para la toma de decisión	Las decisiones efectivas están basadas en el análisis de datos e información.
8	Relaciones con los Proveedores Mutuamente Beneficiosas	Una organización y sus proveedores son interdependientes y una relación mutuamente beneficiosa aumenta la capacidad de ambos para crear valor.

Tabla 6: Principios de Gestión de la Calidad

El estándar para la seguridad de la información **ISO/IEC 27001** especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming"; el cual es una estrategia de mejora continua de la calidad en cuatro pasos.
También se denomina espiral de mejora continua, esta mejora continua proporciona una herramienta que ayuda al incremento de la productividad, favoreciendo el desarrollo estable y consistente en todos los segmentos de los proceso.

Partiendo de lo anterior se establece una continuidad en el desarrollo y aplicación de los principios de la Gestión de Calidad, (Principio 6) como extensión integral de un sistema de Gestión Global coherente, funcional, dinámico y capaz de integrarse con otros sistemas de gestión.

Por tanto estos principios de Gestión de Calidad sirven de marco de referencia, en los cuales se establecen los ejes básicos sobre los que descansa la estructura de la serie de normas ISO 27000.
La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información: Se presentan los principios básicos del Sistema de Gestión de Manejo y Seguridad de la Información así:

PRINCIPIO	NOMBRE
Principio 1	Control
Principio 2	Integridad
Principio 3	Autenticidad
Principio 4	Disponibilidad
Principio 5	Utilidad
Principio 6	Confidencialidad

Tabla 7: Principios de Seguridad de la Información.

La descripción de estos principios se muestra a continuación:

Principio 1: CONTROL
La información como un activo valioso para la organización debe ser periódicamente controlada, tomando en cuenta las implicaciones en las que se incurre el no hacerlo; es decir dentro de las organizaciones debe existir un mecanismo que sea capaz de auditar los niveles de seguridad a los que se expone la información.

BENEFICIOS CLAVES:

- Se alcanza un nivel de confiabilidad en la información procesada.
- Se detentan con antelación cualquier anomalía con respecto al manejo de la información.
- Los usuarios obtienen la información necesaria y suficiente para realizar sus tareas.
- Permite tomar las acciones preventivas y correctivas oportunamente.
- Garantiza la integridad y autenticidad de la información.
- Permite depurar la información con calificativo de “no conforme”, proporcionando la información útil y necesaria.
- La auditoria permite determinar si los sistemas y procedimientos establecidos son efectivos.
- Hace recomendaciones para el mejoramiento de las políticas, procedimientos, sistemas, etc.
- Permite verificar continuamente la efectividad de los controles establecidos.

Principio 2: INTEGRIDAD

Permite garantizar que la información no ha sido alterada en su contenido, por tanto, es íntegra. Una información íntegra es una información que no ha sido alterada de forma indebida o no autorizada.
Para que la información se pueda utilizar, deberá estar íntegra. Cuando ocurre una alteración no autorizada de la información en un documento, quiere decir que el documento ha perdido su integridad.
Manteniendo la exactitud y el contenido completo de la información y sus métodos de proceso.
Garantizar que la información no ha sido alterada en su contenido.
La modificación no autorizada de los datos puede ocurrir tanto durante su almacenamiento como durante el transporte o en el procesamiento.

BENEFICIOS CLAVES:

- El receptor de la información deberá tener la seguridad de que la información obtenida, leída u oída es exactamente la misma que fue colocada a su disposición para una debida finalidad.
- Estar íntegra quiere decir estar en su estado original, por lo que al llegar a su receptor se minimizan las posibilidades de ocasionar errores, fraudes y de perjudicar la comunicación y la toma de decisiones.
- Se disminuye el riesgo de que la información se corrompa, falsifique o burle.
- Se protege la información misma tanto como el ambiente que la soporta, es decir, el proceso que la genera y los medios que la manipulan.

Principio 3: AUTENTICIDAD

Garantiza que la información proporcionada cumpla con los niveles de veracidad exigibles por la organización.
Toda información dispuesta para los usuarios, ya sean internos como externos, debe estar soportada por una base que respalde y verifique la información suministrada.

BENEFICIOS CLAVES:

- Se garantiza que la información suministrada o requerida sea real y veras.
- Toda la información cuenta con un respaldo que permite su verificación, a petición de los usuarios o como parte del proceso de emisión y divulgación de la información.
- Se maneja información actualizada y depurada esencial para la toma de decisiones.
- Se establecen niveles de control que revisan, registran y filtran la información según la naturaleza de la misma.
- Se normaliza el manejo y contenido de la información, garantizando que todos los usuarios manipulen una información fiel y adecuada.

- También se garantiza la autenticidad y fiel cumplimiento de los procesos responsables de generar, editar, revisar y reproducir la información hacia los diferentes usuarios.

Principio 4: DISPONIBILIDAD

Intenta garantizar que la información permanezca accesible cuando se requiera y durante el tiempo que sea necesario.
Los usuarios autorizados tienen acceso a la información y a los recursos relacionados cuando lo requieran.
Los ataques más habituales a la disponibilidad son los de denegación de servicio y la destrucción de archivos.

BENEFICIOS CLAVES:

- Se garantiza que la información requerida por los usuarios llegue en el momento preciso y oportuno.
- Se agiliza la toma de decisiones ya que se cuenta con la información necesaria en el momento adecuado.
- Se asegura la disponibilidad de la información, tanto en su estructura física como en los medios tecnológicos que permiten el acceso, transito y almacenamiento.
- Permite que la información esté al alcance de los usuarios y destinatarios.
- Se minimiza el ataque de denegación de servicio, que consisten en consumir todos los recursos de un sistema de tal manera que éste no pueda dar servicio a los usuarios.
- Se minimiza el ataque de destrucción de archivo, el cual es frecuentemente por causas tecnológicas (espías, jakers, virus, etc.) y por el manejo físico de los usuarios.

Principio 5: UTILIDAD

Se entiende por aptitudes para la utilidad y uso de la información como un conjunto de habilidades que exigen a los individuos “reconocer cuándo se necesita información y poseer la capacidad de localizar, evaluar y utilizar eficazmente la información requerida”. Las aptitudes para la utilidad y uso de la información resultan cada vez más importantes en el entorno actual de rápidos cambios tecnológicos y de proliferación de los recursos de información.

BENEFICIOS CLAVES:

- Se determinar la naturaleza y nivel de la información que se necesita.
- Se determinar el alcance de la información requerida
- Acceder a ella con eficacia y eficiencia
- Evaluar de forma crítica la información y sus fuentes
- Incorporar la información seleccionada a una base de conocimientos propia de cada individuo.
- Se utilizar la información de manera eficaz para acometer tareas específicas.

- Se comprender la problemática económica, legal y social que rodea al uso de la información, y acceder a ella y utilizarla de forma ética y legal.

Principio 6: CONFIDENCIALIDAD
El principio de la confidencialidad de la información tiene como propósito el asegurar que sólo la persona correcta acceda a la información que queremos distribuir. La información que se intercambian entre individuos y empresas no siempre deberá ser conocida por todo el mundo. Mucha de la información generada por las personas se destina a un grupo específico de individuos, y muchas veces a una única persona. Eso significa que estos datos deberán ser conocidos sólo por un grupo controlado de personas, definido por el responsable de la información.

BENEFICIOS CLAVES:

- Tener confidencialidad en la comunicación, es la seguridad de que lo que se dijo a alguien o escribió en algún lugar será escuchado o leído sólo por quien tenga ese derecho.
- Se asegura que todos los elementos involucrados en el manejo de la información, desde el emisor, el camino que recorre hasta el receptor cuenten con el nivel de confidencialidad requerido.
- Cuanto más valiosa es una información, mayor debe ser su grado de confidencialidad establecido.
- Cuanto mayor sea el grado de confidencialidad, mayor será el nivel de seguridad necesario de la estructura tecnológica y humana que participa de este proceso: del uso, acceso, tránsito y almacenamiento de las informaciones.

A continuación se presenta la descripción de de la familia de normas ISO 27000-2005, la cual contiene el detalle de su contenido, requisitos y sus elementos de apoyo.

D. DESCRIPCIÓN DE LAS NORMAS ISO 27000

1. ¿Qué es ISO 27000 y en qué consiste?

ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) han establecido un comité técnico conjunto específico para las Tecnologías de la Información denominado JTC1 (Joint Technical Committee).
Dentro de dicho comité, el subcomité SC27 es el encargado del desarrollo de proyectos en técnicas de seguridad, labor que realiza a través de cinco grupos de trabajo (WG1, WG2, WG3, WG4 y WG5).
Es de este Comité Técnico Conjunto JTC1, en conjunto con el sub-comité SC27 y los grupos de trabajo WG1, 2, 3, 4 y 5 de donde nace la Norma ISO/IEC 27000.

ISO/IEC 27000 es un conjunto de estándares desarrollados –o en fase de desarrollo- por ISO (International Organization for Standardization), (Organización Internacional para la Estandarización) e IEC (International Electrotechnical Commission), (Comisión Electrotécnica Internacional) que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
De ahora en adelante a lo largo de este documento se invocara a la Norma ISO/IEC 27000 como ISO 27000 solamente.

a) El Sistema de Gestión de Seguridad de la Información

El concepto central sobre el que se construye ISO 27000 es el SGSI; SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de *Information Security Management System*.
El Sistema de Gestión de la Seguridad de la Información (SGSI); comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.
La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.
Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

b) El propósito del Sistema de Gestión de la Seguridad de la Información

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

c) Estructura del SGSI

La norma ISO 27000, a través del SGSI establece once dominios estructurales[7] que cubren por completo la Gestión de la Seguridad de la Información:
Todo inicia con la ***elaboración de una estrategia de la organización*** en conjunto que implique a la dirección.
Luego se determinan:

[7] Estos dominios se ilustran en el *ciclo PHVA* correspondiente a la aplicación del SGSI, y se especifica la elaboración de los mismos.

- El alcance del SGSI;
- Política y objetivo de seguridad;
- Manual de seguridad;
- Procedimientos y mecanismos de control que soportan el SGSI; Es de gran utilidad en este punto la aplicación de la Normativa ISO 27002 "Código de buenas prácticas para la gestión de la Seguridad de la Información" con 10 secciones, 39 objetivos y 133 controles.
- Metodología de evaluación de riesgos;
- Informe de evaluación de riesgos;
- Plan de tratamiento del riesgo;
- Procedimientos documentados;
- Registros requeridos por este Estándar Internacional;
- La declaración de aplicabilidad.
- Instructivos, checklists y formularios.

A continuación se comentan los detalles de cada componente de la estructura:

Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.
Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.
Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables .
Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como *output* que demuestra que se ha cumplido lo indicado en los mismos.
Declaración de aplicabilidad: (SOA –*Statement of Applicability*-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.
Instrucciones, *checklists* y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

d) Modelo de Seguridad de la Información

Figura 13: Pirámide de Productos de la ISO 27000.

e) Tipos de activos que considera ISO 27000

Un activo es todo aquel elemento que compone el proceso de la comunicación, partiendo desde la información, su emisor, el medio por el cual se transmite, hasta su receptor.

- Información
- Equipos que la soportan:
    - Software
    - Hardware
    - Organización

- Personas que los utilizan o usuarios

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se **guarde o transmita** (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), **de su origen** (de la propia organización o de fuentes externas) o **de la fecha de elaboración**.

f) Elementos que busca proteger el SGSI

Por tanto, los componentes a los cuales se les busca proteger con la aplicación del SGSI son los siguientes:

- La información misma.
- Los equipos que la soportan.
- Las personas que la utilizan.

Figura 14: Elementos que busca proteger el SGSI.

Es importante definir claramente de que o quienes se van a proteger los activos de la organización, como respuesta a esto ISO 27000, por medio de la aplicación del SGSI plantea defender los activos de la organización de los siguientes aspectos:

- Amenazas y
- Vulnerabilidades.

g) Tipos de Amenazas

Las amenazas son **agentes capaces de explotar los "fallos de seguridad"**, que se denominan puntos débiles y, como consecuencia de ello, **causar pérdidas o daños a los activos** de una empresa, afectando el ejercicio de su negocio.

Figura 15: Tipos de amenazas.

- **Amenazas naturales** – condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos,
- **Intencionales** – son amenazas deliberadas, fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información, entre otras.
- **Involuntarias** – son amenazas resultantes de acciones inconscientes de usuarios, por virus electrónicos, muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores, perdidas y accidentes.

Puntos débiles o fallos de seguridad:
Los puntos débiles son los elementos que, al ser explotados por amenazas, afectan el control, la integridad, autenticidad, disponibilidad, utilidad y confidencialidad de la información de un individuo o empresa.

h) Tipos de Vulnerabilidades

La vulnerabilidad, en seguridad de la información se refiere a la existencia de una debilidad en un sistema permitiendo a un atacante violentar **el control, la integridad, autenticidad, disponibilidad, utilidad y confidencialidad de la información** de sus datos y aplicaciones.

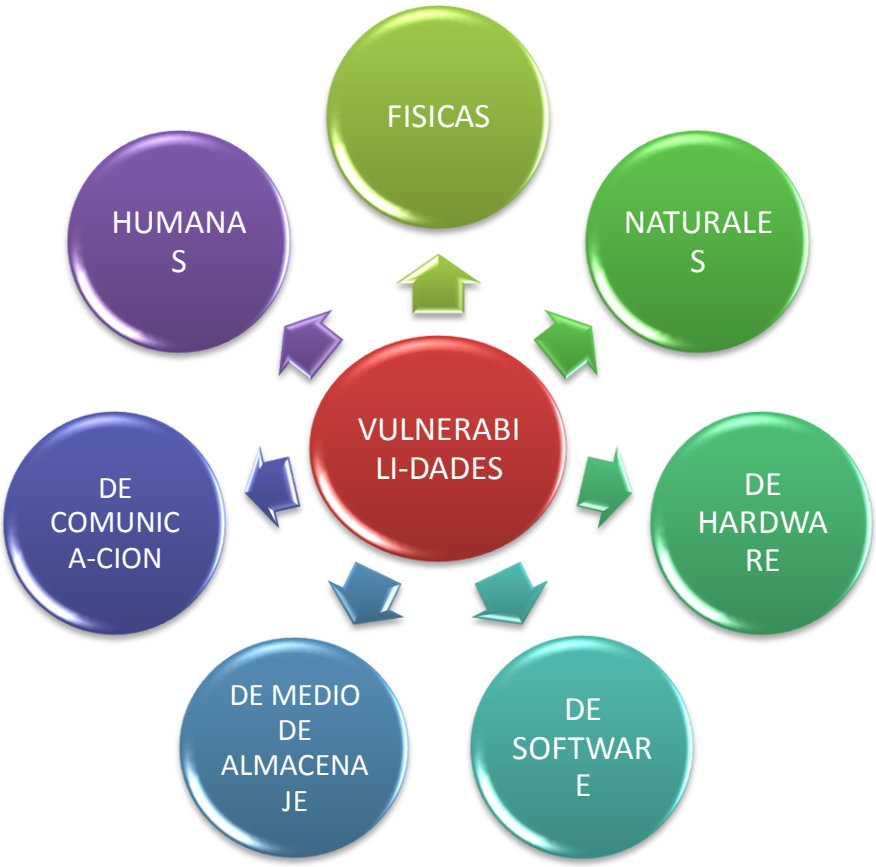


Figura 16: Tipos de vulnerabilidades.

- **Vulnerabilidades físicas:** Los puntos débiles de orden físico son aquellos presentes en los ambientes en los cuales la información se está almacenando o manejando.
- **Vulnerabilidades naturales:** Los puntos débiles naturales son aquellos relacionados con las condiciones de la naturaleza que puedan colocar en riesgo la información.
- **Vulnerabilidades de hardware:** Los posibles **defectos en la fabricación o configuración** de los equipos de la empresa que pudieran permitir el ataque o alteración de los mismos.
- **Vulnerabilidades de software**: Los puntos débiles de aplicaciones **permiten que ocurran accesos indebidos a sistemas informáticos** incluso sin el conocimiento de un usuario o administrador de red.
- **Vulnerabilidades de medios de almacenaje**: Los medios de almacenamiento son los **soportes físicos o magnéticos** que se utilizan para almacenar la información.
- **Vulnerabilidades de comunicación:** Este tipo de punto débil abarca todo el tránsito de la información
- **Vulnerabilidades humanas:** Esta categoría de vulnerabilidad está relacionada con los daños que las personas pueden causar a la información y al ambiente tecnológico que la soporta.

i) Gestión del Riesgo y Medidas a realizar según ISO 27000

El **riesgo** es la probabilidad de que las amenazas **exploten los puntos débiles,** causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando: Los principios básicos de Gestión del manejo y Seguridad de la Información.
Uno de los primeros pasos para la implementación de la seguridad es rastrear y eliminar los puntos débiles en el medio ambiente donde se manipula la información.
Al ser identificados los puntos débiles, será posible dimensionar los riesgos a los cuales el ambiente está expuesto y definir las medidas de seguridad apropiadas para su corrección.
Es por eso que una de los aspectos novedosos que aporta la Norma ISO 27000, es la elaboración de un análisis y evaluación de los riesgos reales y potenciales a los que se están expuestos los acticos de la organización.

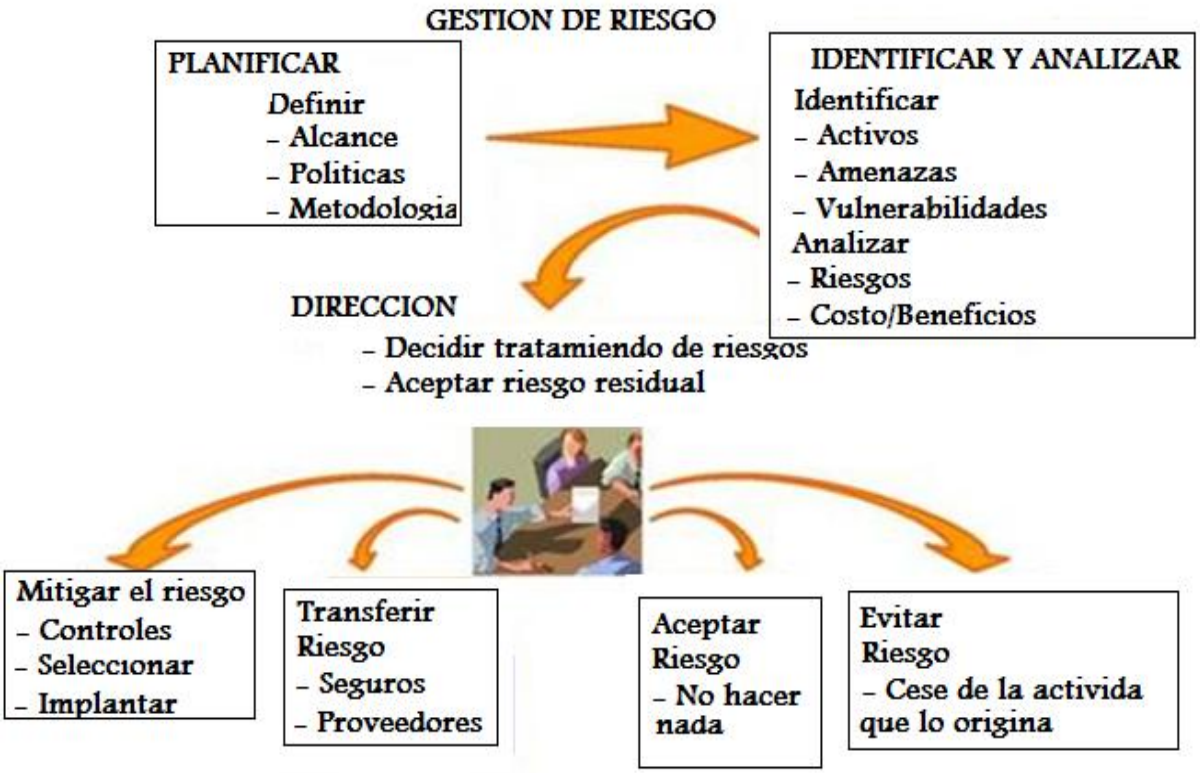


Figura 17: Gestión de Riesgos.

Las medidas de seguridad son **acciones orientadas hacia la eliminación de vulnerabilidades**, teniendo en mira evitar que una amenaza se vuelva realidad.
Estas medidas son el paso inicial para el aumento de la seguridad de la información, en el ambiente donde ésta se manipule.
Medidas a tomar:

- **Preventivo:** buscando evitar el surgimiento de nuevos puntos débiles y amenazas;
- **Perceptivo:** orientado hacia la revelación de actos que pongan en riesgo la información o

- **Correctivo:** orientado hacia la corrección de los problemas de seguridad conforme su ocurrencia.

j) Ciclo de Seguridad

Otro de los aspectos importantes que contempla la Norma ISO 27000, es el desarrollo e implementación del Ciclo de Seguridad.
El ciclo de seguridad se inicia con la identificación de las amenazas a las cuales están sometidas las empresas. La **identificación de las amenazas** permitirá la visualización de los puntos débiles que se podrán explotar, exponiendo los activos a riesgos de seguridad.
Esta exposición lleva a la pérdida de uno o más principios básicos de la seguridad de la información, **causando impactos en el negocio de la organización**, aumentando aún más los riesgos a que están expuestas las informaciones.
Para que el impacto de estas amenazas al negocio se pueda reducir, se toman medidas de seguridad para impedir la ocurrencia de puntos débiles.

Figura 18: Ciclo de seguridad.

Como se puede ver en el diagrama anterior, los riesgos en la seguridad de la empresa aumentan en la medida que las amenazas pueden explotar las vulnerabilidades, y por tanto causar daño en los activos. Estos daños pueden causar que el control, la integridad, autenticidad, disponibilidad, utilidad y confidencialidad de la información se pierda, causando impactos en el negocio de la organización.

Las medidas de seguridad permiten disminuir los riesgos, y con esto, permitir que el ciclo sea de mucho menor impacto para los activos, y por tanto, para la organización.

k) Niveles de Seguridad

- **Lógico:** Control, Integridad, Autenticidad, Confidencialidad, Utilidad y Disponibilidad de la Información, los Equipos que la soportan y los Usuarios que la utilizan.
- **Organizativo:** Relativa a la prevención, detección y corrección de riesgos;
- **Físico:** Protección de elementos físicos de las instalaciones: bodegas, archivos, servidores, PCs.;
- **Legal:** Cumplimiento de la legislación vigente.

l) Áreas que se deben cubrir con ISO 27000

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.
9. Gestión de continuidad del negocio.
10. Conformidad con la legislación.

A continuación se comentan los detalles de cada dominio:

1. Política de seguridad.

Su objetivo principal es dirigir y dar soporte a la gestión de la seguridad de la información. La alta dirección debe definir una **política** que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.
La política se constituye en la base de todo el sistema de seguridad de la información.
La alta dirección debe **apoyar visiblemente** la seguridad de la información en la organización.

2. Aspectos organizativos para la seguridad.

Gestionan la seguridad de la información dentro de la organización. Mantienen la seguridad de los equipos que soportan la información de la organización que son accedidos por terceros. Mantienen

también la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.
Debe diseñarse una estructura organizativa dentro de la compañía que defina las **responsabilidades** que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma. Dicha estructura debe poseer un enfoque **multidisciplinar**: los problemas de seguridad no son exclusivamente técnicos.

3. Clasificación y control de activos.

Mantener una protección adecuada sobre los activos de la organización. Asegurar un nivel de protección adecuado a los activos de información. Debe definirse una **clasificación** de los activos relacionados con los sistemas de información, manteniendo un **inventario** actualizado que registre estos datos, y proporcionando a cada activo el nivel de **protección** adecuado a su valor en la organización.

4. Seguridad ligada al personal.

Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios. Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo. Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.
Las implicaciones del **factor humano** en la seguridad de la información son muy elevadas, todo el personal, tanto **interno** como **externo** a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.
Debe haber diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc., y procesos de **notificación de incidencias** claros, ágiles y conocidos por todos.

5. Seguridad física y del entorno.

Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización. Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización. Prevenir las exposiciones a riesgo o robos de información y de los equipos que la soportan.
Las áreas de trabajo de la organización y sus activos deben ser clasificadas y **protegidas** en función de su nivel de riesgo, siempre de una **forma adecuada** y frente a cualquier **amenaza factible** de índole física (robo, inundación, incendio...).

6. Gestión de comunicaciones y operaciones.

Asegurar la operación correcta y segura de los recursos de tratamiento de información, (equipo de soporte). Minimizar el riesgo de fallos en los sistemas. Proteger la integridad del software y de la información. Mantener la integridad y la disponibilidad de los servicios de tratamiento de información

y comunicación. Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.
Evitar daños a los activos e interrupciones de actividades de la organización. Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.
Se debe garantizar la seguridad de las **comunicaciones** y de la **operación** de los sistemas críticos para el negocio.

7. Control de accesos.

Controlar los accesos a la información, evitar accesos no autorizados a los sistemas de información. Evitar accesos no autorizados a ordenadores y sus sistemas. Detectar actividades no autorizadas. Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y tele-trabajo.
Se debe garantizar que cada usuario tenga única y exclusivamente acceso a la información tanto física como digital que necesita para desempeñar sus funciones.
Se deben establecer los **controles de acceso adecuados** para proteger los sistemas de información críticos para el negocio, a diferentes niveles: sistema operativo, aplicaciones, redes, etc.

8. Desarrollo y mantenimiento de sistemas.

Asegurar que la seguridad está incluida dentro de los sistemas de información. Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones. Proteger la confidencialidad, autenticidad e integridad de la información. Asegurar que los proyectos de Tecnología de la Información y las actividades complementarias son llevadas a cabo de una forma segura. Mantener la seguridad del software y la información de la aplicación del sistema.

9. Gestión de continuidad del negocio.

Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos (claves) frente grandes fallos o desastres. Todas las situaciones que puedan provocar la **interrupción** de las actividades del negocio deben ser **prevenidas** y **contrarrestadas** mediante los planes de contingencia adecuados.
Los **planes de contingencia** deben ser probados y revisados periódicamente. Se deben definir **equipos de recuperación** ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

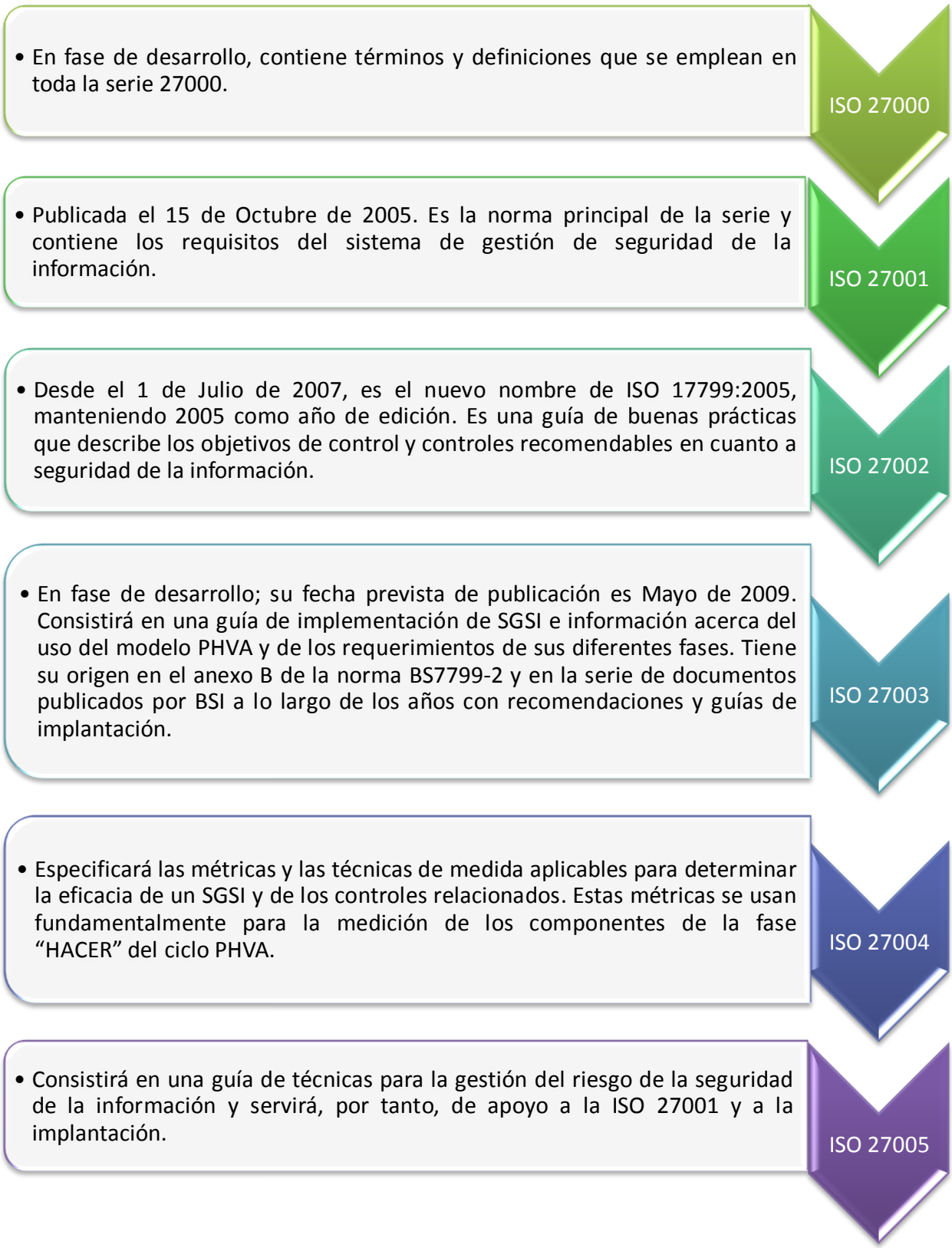
10. Conformidad con la legislación.

Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad. Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma. Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas.
Se debe identificar convenientemente la **legislación aplicable** a los sistemas de información corporativos, integrándola en el sistema de seguridad de la información de la organización y garantizando su cumplimiento.

Se debe definir un plan de **auditoría interna** y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.
Dentro de la familia de normas de la ISO 27000, una de las normas que aporta elementos funcionales para la misma es la Norma ISO 27002:2005, antes ISO/IEC 17799:2005, la cual es compendio de buenas practicar en el manejo y seguridad de la Información así como también posee 133 controles aplicables a las organizaciones que deseen implementar un SGSI.
Por lo tanto, la seguridad de la información es una actividad cuyo propósito es: proteger a los activos contra accesos no autorizados, evitar alteraciones indebidas que pongan en peligro su integridad y garantizar la disponibilidad de la información; ésta seguridad de la información es instrumentada por medio de políticas y procedimientos de seguridad que permiten: la identificación y control de amenazas y puntos débiles, tomando en cuenta la preservación de el control, la integridad, autenticidad, disponibilidad, utilidad y confidencialidad de la información.

2. La serie ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).
La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).
La familia de normas ISO 27000-2005 ha sido elaborada para auxiliar a las organizaciones en la implementación y operación de Sistemas de Gestión de manejo y Seguridad de la Información.
A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.
La familia de normas ISO 27000-2005 está compuesta por el siguiente listado de normas:


• En fase de desarrollo, contiene términos y definiciones que se emplean en toda la serie 27000.
ISO 27000
• Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.
ISO 27001
• Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
ISO 27002
• En fase de desarrollo; su fecha prevista de publicación es Mayo de 2009. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PHVA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
ISO 27003
• Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "HACER" del ciclo PHVA.
ISO 27004
• Consistirá en una guía de técnicas para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO 27001 y a la implantación.
ISO 27005

ISO 27006

- Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs.
- Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

ISO 27007

- En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.

ISO 27011

- En fase de desarrollo; su fecha prevista de publicación es Enero de Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

ISO 27031

- En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

ISO 27032

- En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía relativa a la ciberseguridad.

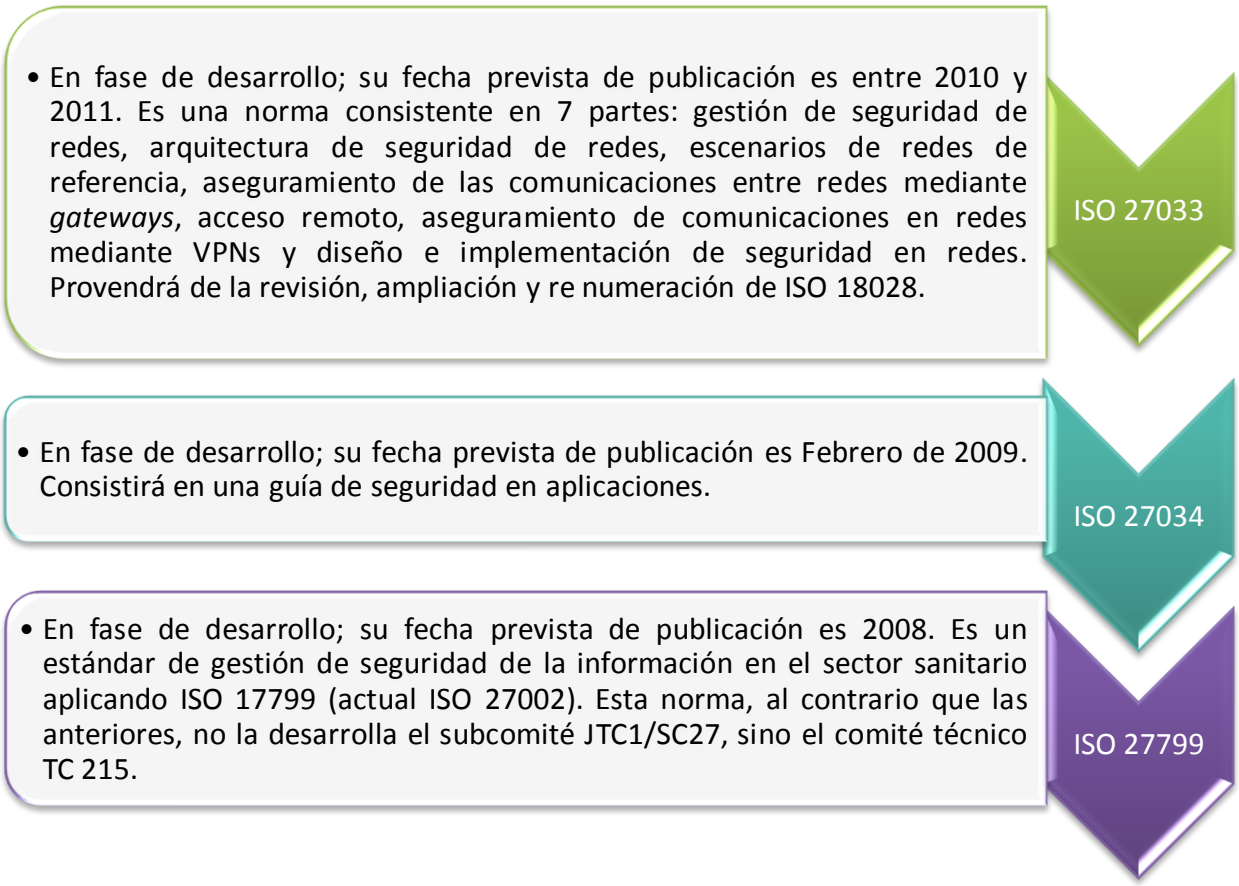


Figura 19: La familia de la ISO 27000.

3. Selección y Uso de la familia de Normas ISO 27000

De la gran familia de normas ISO 27000 la primera que se desprende es estas es la norma "ISO 27000", en esta se especifican los términos y definiciones básicas que se emplearan a lo largo de la serie de normas ISO 27000.

El éxito en la aplicación de cualquier estándar pasa por la elaboración de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión, es por eso que ISO 27000 ofrece una punto de partida o base para entender e interpretar adecuadamente y al mismo nivel los distintos términos y conceptos utilizados a los largo de la familia de normas ISO 27000.

Adoptar la norma ISO 27000, garantizara que los diferentes actores responsables de echar a andar el SGSI manejen el mismo lenguaje e interpretaciones y así con esto eficientizar las operación encaminadas al desarrollo e implementación del mismo, así como los resultados de éste de cara a satisfacer las necesidades de los usuario o clientes del Sistema.

La norma ISO 27001:2005, llamada así por el año de su publicación, (15 de Octubre de 2005). Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

Esta norma muestra cómo aplicar los controles propuestos en la ISO 17799 ahora ISO 27002, estableciendo los requisitos para construir un SGSI, "auditable" y "certificable".

La norma ISO 27001:2005 se utiliza para establecer un Sistema de Gestión de Seguridad de la Información que cumpla con eficientes niveles de confiabilidad y funcionabilidad que esa capaz de satisfacer las necesidades de demandas de los clientes.

Dentro del contenido de la norma ISO 27001:2005 sobresalen cinco apartados esenciales, (4. Sistema de Gestión de Seguridad de la Información, 5. Responsabilidad de la Gerencia 6. Auditorías Internas del SGSI 7. Revisión por la Gerencias del SGSI 8. Mejoramiento del SGSI), en los cuales se concentran los requisitos fundamentales para la elaboración e implementación de un Sistema de Gestión de Seguridad de la Información, por la naturaleza del contenido de cada uno de los cinco capítulos, los requisitos de los cinco capítulos son totalmente aplicables a cualquier tipo organización que esté dispuesta a asegurar su información como un activo valioso.

La norma ISO 27001:2005 posee en su Anexo A, un listado que enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Los cinco capítulos de la norma ISO 27001:2005 se utilizan para cumplir con los requisitos de tipo: **Lógicos, Organizativos, Físicos y Legales,** requisitos que al cumplirlos de manera integral garantizan un nivel se seguridad confiable y eficiente, capaz de satisfacer las necesidades de los usuarios frente a cualquier requerimiento o contingencia.

La norma ISO 27002:2005, llamada así porque mantiene el año de su edición por ISO; contiene una guía de buenas practicar para el manejo y seguridad de la información, así mismo

Consta de 39 objetivos de control y 133 controles agrupados en 11 dominios aplicables a las organizaciones, esta norma sirve de apoyo al SGSI planteado en la norma ISO 27001:2005.
Los 133 controles que contiene la norma ISO 27002:2005 son aplicables en las organizaciones en relación a la gestión de la continuidad de negocio, la gestión de incidentes de seguridad, control de accesos o regulación de las actividades del personal interno o externo, entre otros, estos controles ayudarán a la organización a implantar medidas que reduzcan sus riesgos en cuanto a seguridad de la información.
Como se dijo anteriormente, ISO 27001:2005 contiene un anexo A, que considera los controles de la norma ISO 27002 para su posible aplicación en el SGSI que implante cada organización (justificando, en el documento denominado "Declaración de Aplicabilidad", los motivos de exclusión de aquellos que finalmente no sean necesarios).
ISO 27002:2005 es para ISO 27001:2005, por tanto, una relación de controles necesarios para garantizar la seguridad de la información.
Es de aclarar que esta norma, ISO 27002:2005, NO es certificable y la aplicación total o parcial en cada organización se realiza de forma totalmente libre y sin necesidad de una supervisión regular externa.
La norma que sí es certificable es ISO 27001:2005.
La norma ISO 27002:2005, se utiliza como complemento de la norma ISO 27001:2005, sirviendo de apoyo en la medida que ofrece toda una gama de controles que operan la ejecución particular de las actividades propias de cada organización en la implementación del SGSI.

Es decir, para la implantación del SGSI se necesitaran de una seria de controles que respalden al Sistema, controles que se encuentran especificados en el código de buenas practica (ISO 27002:2005), es de esa manera que se establece la relación fundamental entre las dos normas.
En términos culinarios se puede definir la relación entre ambas normas así: ISO 27001:2005 tiene la receta e ISO 27002:2005 tiene los ingredientes.

4. Otras normas de apoyo a ISO 27000[8]

NORMA	PROPÓSITO
ESTÁNDARES ELABORADOS POR EL COMITÉ TÉCNICO CONJUNTO Y SU SUB-COMITÉ ISO JTC1 / SC27	
ISO/IEC 7064:2003	Tecnología de la Información – Técnicas de seguridad – Verificación de tipos de Sistemas.
ISO/IEC 9796-2:2002	Tecnología de la Información – Técnicas de seguridad – Firma Digital de Proyectos dando un mensaje de recuperación – Parte 2: Mecanismos basados en Factorización de números enteros.
ISO/IEC 9796-3:2006	Tecnología de la Información – Técnicas de seguridad – Firma Digital de Proyectos dando un mensaje de recuperación – Parte 3: Mecanismos basados en Logaritmos discretos.
ISO/IEC 9797-1:1999	Tecnología de la Información – Técnicas de seguridad – Códigos y Mensajes de Autenticación (MACs) – Parte 1: Mecanismos usando un bloque de cifras.
ISO/IEC 9797-2:2002	Tecnología de la Información – Técnicas de seguridad – Códigos y Mensajes de Autenticación (MACs) – Parte 2: Mecanismos usando una función para generar claves delicadas, o para identificar un conjunto de información.
ISO/IEC 20000	Es el primer estándar internacional certificable para la gestión de servicios de Tecnologías de la Información (TI).
ISO 20000-1:	Especificaciones en las cuales se describe la adopción de un proceso de mejora integrado para el desempeño y gestión de los servicios acorde a los requisitos del negocio y del cliente.
ISO 20000-2:	Código de prácticas donde se describen las mejores prácticas para la gestión de los servicios de Tecnologías de la Información y dentro del ámbito indicado por la norma ISO 20000-1.

Tabla 8: Normas de apoyo de la ISO 27000

5. Descripción del contenido de las normas ISO 27000

A continuación se presenta un cuadro resumen de los apartados más importantes que se establecen en la Norma ISO 27001:2005

[8] Ver Anexo 5. listados completo de los estándares vigentes hasta septiembre 2008, desarrollados y publicados por el comité técnico conjunto y su sub-comité ISO JTC1 / SC27

ISO 27001:2005	
APARTADO	DESCRIPCIÓN
0. Introducción:	Generalidades e introducción al método PHVA.
1. Objeto y campo de aplicación:	Se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
2. Normas para consulta:	Otras normas que sirven de referencia.
3. Términos y definiciones:	Breve descripción de los términos más usados en la norma.
4. Sistema de gestión de seguridad de la información.	
4.1. Requisitos Generales	Cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.
4.2. Establecer y Gestionar el SGSI	
4.2.1. Establecer el SGSI	Definir el alcance, limitaciones, política, gestión de riesgos (identificación, análisis, evaluación, tratamiento y control), autorización de la gerencia y declaración de aplicabilidad.
4.2.2. Implementar y operar el SGSI	**Formular e implementar plan de tratamiento de riesgos, implementar controles y medir eficacia de los mismos, plan de capacitación, gestión de operación y recursos del SGSI, procedimientos de contingencia.**
4.2.3. Monitorear y revisar el SGSI	Procedimientos, controles, políticas y objetivos del SGSI, eficacia de controles y valoración del riesgo, auditorías internas, revisión gerencial, planes de seguridad y registro de acciones y eventos.
4.2.4. Mantener y mejorar el SGSI	Implementar mejoras identificadas, acciones correctivas y preventivas, socialización de acciones a tomar y alcance de objetivos según las mejoras.
4.3. Requisitos de la documentación	
4.3.1. Generales	Requisitos de la documentación y control de la misma. (alcance, política, procedimientos, controles y gestión de riesgos)
4.3.2. Control de documentos	Aprobar, revisar y actualizar los documentos, garantizar su disponibilidad, autenticidad, integridad, utilidad y confidencialidad.
4.3.3. Control de registros	Son almacenados (legibles, identificables y recuperables) como evidencia de operación y conformidad del SGSI, mantienen requisitos legales,
5. Responsabilidad de la gerencia/dirección	
5.1. Compromiso de la gerencia	La dirección establece un compromiso formal y directo a todos los niveles con el desarrollo del SGSI.

5.2. Gestión de recursos	
5.2.1. Provisión de recursos	Se asignan los recursos necesarios para el desarrollo del SGSI.
5.2.2. Capacitación, conocimiento y competencia	Garantizar el adecuado personal que sea responsable del SGSI.
6. Auditorías internas al SGSI	Cómo realizar las auditorías internas de control y cumplimiento.
7. Revisión del SGSI por la gerencia	
7.1. Generalidades	Cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.
7.2. Insumos para la revisión	Elementos a considerar para la revisión.
7.3. Resultados de la revisión	Decisiones y acciones concretas para ser aplicadas en todas las áreas y niveles del SGSI.
8. Mejoramiento del SGSI	
8.1. Mejora continua	Mejorar la eficacia del SGSI.
8.2. Acción correctiva	Acciones para eliminar las causas de no conformidades reales.
8.3. Acción preventiva	Acciones para eliminar las causas de no conformidades potenciales.
Anexo A: Objetivos de control y controles:	Anexo A, normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.
Anexo B: Relación con los Principios de la OCDE:	Anexo B, informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.
Anexo C: Correspondencia con otras normas:	Anexo C, informativo con una tabla de correspondencia de cláusulas con ISO 9001 e ISO 14001.
Bibliografía:	Normas y publicaciones de referencia.

Tabla 9: Contenido de la norma ISO 27000.

CAPITULO III: DIAGNOSTICO DEL MANEJO Y SEGURIDAD DE LA INFORMACION EN CEL.

A. DESARROLLO DE LA METODOLOGÍA DE LA INVESTIGACIÓN.[9]

1. Diagrama de la Metodología de Investigación

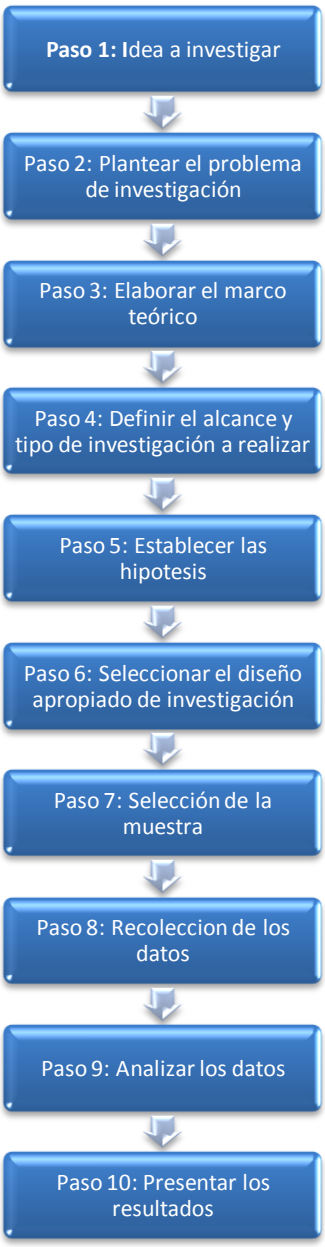


Figura 20: Pasos de la metodología de Investigación.

[9] Ver Anexo 6 : Metodología de investigación

2. Aplicación de las etapas de la metodología

Paso 1: LA IDEA:

Toda investigación, como se planteo en la teoría del método de investigación, parte de la determinación de una idea o necesidad. Para el caso del proyecto que se presenta, la idea atiende a la determinación de dos elementos principales que serán los que definirán el diseño del Sistema de Gestión para el Manejo y Seguridad de la Información, los elementos son los siguientes:

- ✓ **Conocer la situación actual del manejo y seguridad de la información en los procesos claves y de apoyo dentro de la Comisión.**
- ✓ **Identificar las necesidades y requerimientos de los usuarios y productores de la información que participan en los procesos claves y de apoyo de la Comisión.**

Luego de haber establecido los elementos que dan origen a la idea, el enunciado final de la misma para la investigación se ha redactado de la siguiente manera:

"Identificar y determinar la situación actual en cuanto al Manejo y Seguridad de la Información, así como las necesidades y requerimientos de los usuarios y productores de la misma, dentro de los procesos claves y de apoyo de la Comisión"

Paso 2: PLANTEAMIENTO DEL PROBLEMA:

Una vez planteada la idea de la investigación se procederá al planteamiento del problema que no es más que la estructuración de esta idea de manera formal, este paso es crítico ya que toda la investigación girará alrededor de este planteamiento, lo cual indica que si éste no ha sido definido correctamente la investigación se desarrollará para la solución de un problema que no es el de interés.

Por tanto, el planteamiento del problema para la investigación se redacta en forma de pregunta y se plantea de la siguiente manera:

"¿Cual es la situación actual que posee la Comisión Ejecutiva Hidroeléctrica del Rio Lempa en cuanto al Manejo y Seguridad de la Información, así como, cuales son las necesidades y requerimientos de los usuarios y productores de la misma, dentro de los procesos claves o procesos de negocio y procesos de apoyo?"

Se procederá ahora a la determinación de los objetivos de la investigación que serán una guía para el desarrollo de ésta.

a) Objetivos de la Investigación

- **Objetivo general:**
  - ✓ Realizar un diagnostico de la **situación actual del Manejo y Seguridad de la Información en los procesos claves y de apoyo, así como también identificar y determinar las necesidades y requerimientos de los usuarios y productores de la información,** con el propósito de conocer que está haciendo la Comisión para manejar y asegurar la información que genera de su actividad comercial.
- **Objetivos específicos:**
  - ✓ Determinar la existencia de un mecanismo que sea capaz de garantizar los niveles de seguridad de la información dentro de cada proceso clave.
  - ✓ Evidenciar la existencia de mecanismos de control, revisión y auditorias de la información aplicados a los procesos claves de la Comisión.
  - ✓ Verificar si el protocolo de seguridad actual garantiza que la información utilizada no sea alterada en el almacenamiento, transporte o procesamiento.
  - ✓ Establecer si la información proporcionada en cada proceso cumple con los niveles de veracidad exigibles por la organización.
  - ✓ Comprobar si la información permanece accesible cuando se requiera y durante el tiempo que sea necesario.
  - ✓ Establecer si la información se utiliza eficazmente cuándo se necesita y si se posee la capacidad de localizarla en ese instante.
  - ✓ Conocer si sólo la persona correcta accede a la información que se manipula en los procesos claves.
  - ✓ Determinar las amenazas y vulnerabilidades actuales de la seguridad de la información en los procesos claves de la Comisión.

b) Desarrollar las preguntas de la investigación.

Además de plantear los objetivos de la investigación, es conveniente plantear el problema a través de varias preguntas que facilitarán el análisis de las necesidades de información que se posean en el desarrollo de la investigación, el plantear el problema a través de preguntas tiene la ventaja de presentarlo de manera directa, concreta, minimizando la distorsión:

i. ¿Cuentan los procesos claves y de apoyo con un mecanismo que garantice la seguridad de la información dentro de cada uno de estos?

ii. ¿Cuál es la garantía de integridad que posee el protocolo de seguridad de la información en los procesos? ¿Existen controles, revisiones, auditorias?

iii. ¿La información que fluye por cada proceso es autentica? ¿Y si es autentica que nos garantiza?

iv. ¿Qué tan accesible es la información en tiempo y espacio necesario?

v. ¿Es toda la información que fluye dentro de casa proceso Útil? ¿Qué porcentaje de esta es inútil?

vi. ¿Es la información conocida solo por el grupo o persona definido por el responsable de la información

vii. ¿Qué amenazas y vulnerabilidad atacan y debilitan la información de los Procesos?

c) Justificación de la investigación.

1. Existe una necesidad explicita, expresada por la Unidad de Gestión Integrada de la Comisión, por conocer el estado actual que posee la institución en cuanto al manejo y seguridad de la información de los procesos claves y de apoyo se refiere.

2. La Unidad de Gestión Integrada desea conocer las necesidades y requerimientos en cuanto al manejo y seguridad de la información, que poseen los usuarios y productores de la misma.

3. Existe serios problemas de seguridad de la información que generan cuantiosos costos a la Comisión.

4. Se identifica la oportunidad de darle valor agregado a los procesos claves y de apoyo, mejorando la seguridad de la información que generan los mismos.

Paso 3: ELABORAR EL MARCO TEÓRICO:

Una vez planteado el problema de estudio es necesario tener un apoyo teórico y esto consiste en exponer teorías, enfoques técnicos, investigaciones previas y antecedentes en general que se relacionen con el tema en estudio.

Este marco teórico se ha desarrollado en el capitulo C y contiene la información y literatura acerca de la Seguridad de la Información basada en la norma ISO/IEC 27000 donde se tratan los requerimientos para la gestión de un sistema que garantice el control, integridad, autenticidad, disponibilidad, utilidad y confidencialidad de la información, siendo estos seis elementos, los principios fundamentales que sostiene la Norma.

Paso 4: DEFINIR EL ALCANCE Y EL TIPO DE INVESTIGACIÓN A REALIZAR:

El campo de acción de la investigación está delimitado por las ***fronteras de operación de los procesos claves y sus respectivos procesos de apoyo***, dichos procesos han sido establecidos previamente, basados en la implementación de la norma ISO 9000 y como parte de un sistema de Gestión Integrada.

¿Qué tipo de metodología de utilizara?

En el caso de esta investigación y por las características de la misma, se ha optado por utilizar el tipo de ***Investigación Descriptiva***.; este tipo de investigación se describe en el Cap. C Marco Teórico, Sección II: Metodologías de Investigación, Apartado 3: Tipos de Investigación.

Paso 5: ESTABLECER LAS HIPÓTESIS:

Por encontrarnos en una investigación de tipo mixto, cualitativa/cuantitativa, la cual mide tanto apreciaciones y/o percepciones como niveles, frecuencias e impactos económicos; la elaboración de Hipótesis NO APLICA.

Paso 6: SELECCIONAR EL DISEÑO APROPIADO DE LA INVESTIGACIÓN:

Por la naturaleza y cualidades del estudio y sus objetivos es de Tipo NO experimental.

Paso 7: SELECCIÓN DE LA MUESTRA:

Por las cualidades del campo de investigación la metodología hará una investigación al 100% del universo, dirigida a la siguiente población.
Jefes y personal operativo de las unidades de:

1. Producción (Clave)
2. Comercialización (Clave)
3. Gestión de la Información (Apoyo)
4. Recursos Humanos (Apoyo)

i. Instrumentos para la recolección de datos.

Para recolectar los datos se establecerá un instrumento mediante el cual se pueda recoger la información necesaria basada en las preguntas de investigación mencionadas en el paso numero 1.
Para validar este instrumento se realizara una entrevista con los jefes de las unidades basado en los 6 principios del Manero y seguridad de la Información.
El siguiente cuadro presenta la descripción de los instrumentos a usar y los objetivos que persigue cada uno de ellos.

Instrumento	Objetivo	Población objeto de estudio
1. Cuestionario basado en la Norma ISO 27000.	Identificar la situación actual de los procesos claves y de apoyo con respecto a los requisitos	Jefes y personal operativo de las unidades:: ✓ Producción ✓ Comercialización

	establecidos en la norma.	✓ Gestión de la Información ✓ Recursos Humanos
2. Entrevista con los jefes de la unidades.	Validar la información que se obtuvo en el cuestionario basado en la norma ISO 27001:2005.	Jefes de las unidades de : ✓ Producción ✓ Comercialización ✓ Gestión de la Información ✓ Recursos Humanos

Tabla 10: Instrumentos para la recolección de datos.

ii. Cuestionario basado en la Norma ISO 27000.

Como parte del diseño del primer instrumento de investigación (Cuestionario basado en la Norma ISO 27000), se detallaran los objetivos que se persiguen en la investigación correspondientes a cada uno de los apartados que la norma ISO 27000 en la sección de los requisitos del SGSI se refiere, estos objetivos por cada requisitos, se presentan en un cuadro a continuación:

PUNTO DE LA NORMA	OBJETIVO DE LAS PREGUNTAS DE CADA PUNTO
4.0 sistema de gestión de seguridad de la información	
4.1 Requerimientos Generales	Conocer si la Comisión cuenta con un sistema de gestión de seguridad de la información y conocer si los procesos involucrados se basan en el modelo planificar, Hacer , controlar, Actuar (PDCA)
4.2 Establecer y manejar el SGSI	Establecer el alcance y políticas del sistema en términos de las características de los procesos. Definir el enfoque de evaluación de evaluación de riesgos e identificarlo. Analizar y evaluar los riesgos Establecer acciones de tratamientos de riesgos. Establecer el plan de tratamiento de riesgos e implementarlo Definir la efectividad de los controles Implementar programas de capacitación y conocimiento. Establecer mecanismos y recursos para gestionar las operaciones en el manejo y seguridad de la información. Establecer procedimientos que detecten incidentes de seguridad. Establecer procedimientos que detecten incidentes de seguridad Establecer si la Comisión ejecuta procedimientos de monitoreo y revisiones. Definir si la Comisión mide la efectividad de los controles y si revisa las evaluaciones de riesgo. Establecer si se realizan auditorías internas y revisiones gerenciales. Conocer si la Comisión cuenta con planes de seguridad actualizados. Verificar si la Comisión cumple con las mejoras identificadas y qué tipo de acciones se toman al respecto.
4.3 Requerimientos de la documentación	Establecer los requisitos que deben poseer los registros relacionados con la seguridad de la información, estableciendo el control de

	documentos y de registros.
5.0 Responsabilidad de la Gerencia	
5.1 Compromiso de la gerencia	Establecer si la alta gerencia de la Comisión presenta interés y un verdadero compromiso con el establecimiento de un sistema de gestión de seguridad de la información basado en el ciclo PDCA en sus procesos claves y de apoyo
5.2 Gestión de recursos	Determinar la disposición de la Comisión para proporcionar recursos necesarios y el compromiso de asegurar el entrenamiento, conciencia y competencia hacia los mismos.
6.0 Auditorías internas SGSI	Establecer si la Comisión conduce auditorías internas de acuerdo a los requisitos de seguridad de información internacionales.
7.0 Revisión gerencial del sistema SGSI	
7.1 Generalidades	Determinar si las revisiones se encuentran claramente documentada y sus registros mantenidos.
7.2 Insumo de revisión	Determinar si los elementos de entrada están debidamente establecidos
7.3 resultado de la revisión	Establecer si los elementos de salida están debidamente establecidos
8.0 Mejoramiento de SGSI	
8.1 Mejoramiento continuo	Establecer si la Comisión mejora continuamente la eficacia de su sistema de seguridad
8.2 Acción Correctiva	Determinar si la Comisión posee acciones para eliminar la causa de no conformidad en cuanto a los requisitos de sistema y prevenir su recurrencia
8.3 Acción Preventiva	Establecer si la Comisión determina acciones eliminando causas de no conformidad potenciales en cuanto a los requisitos del sistema y así prevenir su ocurrencia

Tabla 11: Objetivos del Cuestionario basado en los requisitos de la ISO 27000.

Cuestionario basado en los requisitos de la Norma ISO 27001:[10]

PUNTO DE LA NORMA	PREGUNTAS DE CADA PUNTO
4.0 sistema de gestión de seguridad de la información	
4.1 Requerimientos Generales	1. ¿Qué entiende por seguridad de la Información?_____ _____ _____ 2. ¿Existe un sistema dentro de La Comisión que busque asegurar la Información? Si_____ No____ si no, como se asegura:_____

[10] Ver Anexo 7: Cuestionario basado en las normas ISO 27000

	_____ 3. ¿Los procesos Claves y de Apoyo se encuentran basados bajo el modelo PDCA? Si_____ No____ si no, en que están basado:_____ _____
4.2 Establecer y manejar el SGSI	4. ¿Se cuenta con un alcance y limitaciones definidas en el manejo y seguridad de la Información? Si_____ No____ si no, como se delimitan:_____ _____ 5. ¿Se cuenta con políticas definidas en el manejo y seguridad de la Información? Si_____ No____ si no, que la rige:_____ _____ 6. ¿Existe una metodología para la evaluación de riesgos de información? Si_____ No____ si no, como se evalúan:_____ _____ 7. ¿Se tienen identificados y clasificados los riesgos de información, así como sus amenazas y vulnerabilidades? Si_____ No____ si no, como se hace:_____ _____ 8. ¿Se usan criterios para identificar y clasificar los riesgos? Si_____ cuales:_____ No____ si no, bajo que los identifican y clasifican:_____ _____ 9. ¿Se ha previsto el impacto que ocasionan los riesgos de información? Si___ cual:_____ No___ 10. ¿Se han determinado nivel de riesgo admisible? Si_____ cual:_____ No____ 11. ¿Existen medidas a tomar ante la existencia de riesgos? Si_____ cuales:_____ No____
4.2 Establecer y manejar el SGSI	12. ¿Existe un plan de tratamiento de riesgos? Si_____ No____ No se tratan____ 13. Si existe un plan de tratamiento de riesgos, ¿Se actualiza constantemente? Si_____ No____ Cada cuanto: 1 mes____ 3 meses_____ 6 meses_____ 1 año____ Otros intervalos_____ 14. ¿Se cumplen las mejoras propuestas? Si_____ No____ 15. ¿Qué tipo de acciones se toman? Preventivas:____

	Correctivas:____ Otras:_____ 16. ¿Existen controles para el tratamiento de los riesgos? Si_____ cuales:_____ No____ 17. ¿Existen capacitación al personal en cuanto al manejo y seguridad de la información? Si_____ con qué frecuencia:_____ No____ 18. ¿Qué recursos se destinan para el manejo y seguridad de la Información? Equipo____ Infraestructura____ Tecnología____ Efectivo$$___ Personal____ Ninguno____ Técnicas____ Otros:____ Capacitaciones____ 19. ¿Posee un mecanismo que detecte incidentes de seguridad? Si_____, especifique_____ No____ 20. ¿Se ejecutan procedimientos de revisión y monitoreo dentro de las formas de manejo y seguridad de la información? Si_____ No____ 21. ¿Se revisa la efectividad de los controles existentes? Si_____ con qué frecuencia:_____ No____
4.3 Requerimientos de la documentación	22. ¿Qué tipo de documentos existen en la Comisión? Manual de Organización _____ Manual de puestos_____ Manual de procedimientos_____ Otros_____ 23. ¿Cada cuánto tiempo se revisan y actualizan los documentos? Una vez al año _____ Cada semestre _____ Cada trimestre _____ Siempre que hay un cambio _____ No los revisan _____ 24. ¿Los documentos en uso se encuentran actualizados? Si_____ No____ Algunos(Cuantos)___ No se___ Ultima fecha de actualización _____ 25. ¿Se trabaja siempre de acuerdo a los procedimientos establecidos? Si_____ No____ No siempre, especifique:_____ _____ 26. ¿Los documentos están disponibles en los puntos de uso y permanecen legibles y fácilmente identificables? Si_____ No____ donde se encuentran:_____ _____ 27. ¿De qué manera se controlan los documentos del establecimiento? Hay un encargado de documentos _____

	No hay ningún control _____ Otros _____
5.0 Responsabilidad de la Gerencia	
5.1 Compromiso de la gerencia	28. ¿La gerencia ha expresado al personal la importancia de la seguridad de la información? Si_____ De qué forma_____ No____
5.2 Gestión de recursos	29. ¿Se destinan recursos para asegurar la información? Si_____ Si en forma limitada:_____ No____ 30. Si se destinan recursos, ¿Existen un adiestramiento y concientización para el uso de los mismos? Si_____, Cuales:_____ No____ 31. ¿Los recursos destinados alcanzan a cubrir la demanda? Si_____ No____ ¿Porque?_____
6.0 Auditorías internas SGSI	
	32. ¿Se realizan auditorías internas sobre el manejo y la seguridad de la información en base a requisitos internacionales? Si_____ No____ Otro tipo de auditoría:_____ Otros: _____ 33. ¿Existe un plan de auditorías establecidos? Si_____ No____ ¿Se aplica debidamente? Si_____ No____ 34. ¿Quién o quiénes es/son el/los responsables de efectuar las auditorias?_____
7.0 Revisión gerencial del sistema SGSI	
7.1 Generalidades	35. ¿La gerencia realiza revisiones generales en cuanto al manejo y seguridad de la Información? Si_____ No____ 36. Si se realizan revisiones, ¿Estas se encuentran documentadas debidamente? Si_____ No____ 37. Si se realizan, ¿Cada cuanto tiempo se realizan? Cada mes____ Cada 3 meses____ Cada 6 meses____ Cada año____ Otros intervalos_____
7.2 Insumo de revisión	38. ¿Qué insumos se utilizan para realizar las revisiones? Resultados de auditorias____

	Retroalimentación de usuarios____ Técnicas, productos o procedimientos de mejora____ Estado de acciones preventivas y correctivas____ Vulnerabilidades o amenazas latentes____ Resultados de mediciones de controles____ Otros especifique_____
7.3 resultado de la revisión	39. ¿Qué tipo de resultados arroja las revisiones? Mejora la eficacia____ Actualización del plan de tratamiento de riesgos____ Modificación de procedimientos y controles____ Necesidades de recursos____ Otros especifique_____
8.0 Mejoramiento de SGSI	
8.1 Mejoramiento continuo	40. ¿Existe un mecanismo establecido por la Comisión que mejore continuamente el manejo y seguridad de la información? Si_____ cual:_____ No____
8.2 Acción Correctiva	41. Ante un fallo de seguridad ¿Se toman medida o acciones correctivas para eliminar el fallo? Si_____ cuales:_____ No____
8.3 Acción Preventiva	42. ¿Se toman acciones o medidas preventivas ante fallos de seguridad potenciales? Si_____ cuales:_____ No____

Tabla 12: Preguntas del Cuestionario basado en los requisitos de la ISO 27000.

iii. Guía de entrevista con los jefes de la unidades.

A continuación se presenta el diseño de la Entrevista a realizase a cada uno de los jefes de Unidad en donde se desarrollan los procesos claves del negocio (Producción y Comercialización) y dos de los procesos de apoyo (Informática y Desarrollo Humano); la entrevista está basada en los seis principios fundamentales que establece la Norma ISO 27000, y tiene como objetivo conocer en qué medida se está garantizando la aplicación de estos principios apegados a los requerimientos que dispone la norma.

PRINCIPIO	INFORMACIÓN REQUERIDA
1. Control	Conocer si la información manejada dentro del departamento es controlada, con que periodo se hace, como se hace, que impacto incurre el no hacerlo.
2. Integridad	Conocer como se garantiza que la información es integra en su contenido es decir que en todo el proceso del flujo y manipulación de esta no sea alterada de forma indebida o no autorizada, durante su almacenamiento y transporte.

3. Autenticidad	Conocer si los usuarios de la información gozan de información veraz y real, es decir si la información que se manipula en verdadera, autentica.
4. Disponibilidad	Establecer si la información es accesible en el tiempo oportuno y espacio adecuado.
5. Utilidad	Determinar si la información suministrada o requerida le es útil para el desarrollo de las tareas asignadas y en qué porcentaje los es. Verificar la capacidad de localizar, evaluar y utilizar eficazmente la información.
6. Confidencialidad	Asegurar si se cumple que solo la persona correcta accede a la información aun cuando se intercambie entre los mismos individuos de La Comisión.

Tabla 13: Objetivos de la entrevista basada en los principios de seguridad de Información.

GUÍA DE ENTREVISTA

Proceso:	**Fecha:**	**Hoja:**
Departamento o Área:		
Nombre del entrevistado:		
Cargo:		
Posee personal a su cargo:	**Cuantos:**	

CONTROL:

¿Qué tipo de información o documentos maneja?
Existe un control para esta información
Quien controla toda o parte de la información
Como se controla
Cada cuanto se controla
Que beneficio trae el aplicar estos controles
Que impacto tiene el no controlar.

INTEGRIDAD:

Quien manipula los documentos (durante el transporte y el proceso)
Quien autoriza y define las responsabilidades de manipulación
Qué tipo de manipulación está autorizada a hacerse en esta área
Como se garantiza que el documento tenga únicamente alteraciones autorizadas
Como se asegura en el almacenamiento del documento el acceso al personal autorizado
Que impacto genera una alteración no autorizada de la información.

AUTENTICIDAD:

Como se garantiza que la información suministrada es real y veraz

Como se respalda la información para su verificación: se hace a petición, autocontrol o como parte del proceso de emisión.
Que impacto genera que la información no sea veraz o real.

DISPONIBILIDAD

Como llega la información (solicitud, o flujo de proceso)
La información llega con los tiempos establecidos y oportunos.
La información que necesita está disponible
Que canales y medios se utiliza para el manejo de la información ¿son adecuados?
El personal autorizado al acceso de la información cuenta con la información cuando la requiere (esta área genera atrasos para poner la información a disposición de clientes)
Que impacto o que dificultades le genera no disponer de la información necesaria en el tiempo preciso.

UTILIDAD

Como obtiene la información que necesita para desempeñar sus funciones (la obtiene por solicitud o como parte del flujo del proceso)
Que volumen de información demanda para su uso
Utiliza toda la información que recibe, toda le es útil
Como la identifica si es útil o no
Qué porcentaje utiliza
Con que frecuencia la utiliza
Que impacto positivo o negativo le genera el uso o mal uso de la información

CONFIDENCIALIDAD

Manipulan información confidencial
En porcentaje representa del total de información manipulada
El acceso a la información confidencial es solo de la persona o grupo autorizado para hacerlo
Existen otras personas o grupos que accedan a la información
Que medios se utilizan para el transporte de la información
Existe la posibilidad que la información llegue a la persona incorrecta, antes, durante y después de proceso (transito o flujo)
Que impacto genera que la información llegue a las manos equivocadas

Paso 8: RECOLECCION DE DATOS.

i. Resultados del Cuestionario.

1) Unidad de Producción[11]

PUNTO DE LA NORMA	OBJETIVO DE LAS PREGUNTAS DE CADA PUNTO	PREGUNTA	PORCENTAJE %				
			SI	NO	ALGUNAS	NO SE TRATAN	NO RESPONDIÓ
4.0 sistema de gestión de seguridad de la información							
4.1 Requerimientos Generales	Conocer si la Comisión cuenta con un sistema de gestión de seguridad de la información	2	25%	75%			
	Conocer si los procesos involucrados se basan en el modelo planificar, Hacer , controlar, Actuar (PDCA)	3	75%	25%			
4.2 Establecer y manejar el SGSI	Establecer el alcance y políticas del sistema en términos de las características de los procesos.	4	0%	100%			
		5	100%	0%			
	Definir el enfoque de evaluación de riesgos, identificación, clasificación y análisis de los riesgos, medir el impacto que ocasiona y nivel admisible.	6	0%	100%			
		7	0%	100%			
		8	0%	100%			
		9	0%	100%			
		10	0%	100%			
	Establecer acciones de tratamientos de riesgos.	11	100%	0%			
	Establecer el plan de tratamiento de riesgos e implementarlo	12	75%	25%		0%	
		13	0%	100%			
	Verificar si la Comisión cumple con las mejoras identificadas y qué tipo de acciones se toman al respecto.	14	0%	100%			
		15	Prev: 0%	Corr:100%			
	Establecer si la comisión ejecuta procedimientos de monitoreo y revisiones	16	0%	100%			
		19	100%	0%			

[11] Ver Anexo 8 Tabulación de datos de encuesta para la Unidad de Producción.

	Implementar programas de capacitación y conocimiento.	17	25%	75%			
	Establecer procedimientos que detecten incidentes de seguridad.	18	100%	0%			
	Definir si la Comisión mide la efectividad de los controles y si revisa las evaluaciones de riesgo.	20	0%	100%			
	Conocer los recursos que destina la comisión para gestionar las operaciones en el manejo y seguridad de la información	29		Equipo:0, personal:0, Tecnologia:0, Tecnicas:0, Capacitaciones:0, infraestructura:0, efectivo:0, ninguno:0, otros:4			
4.3 Requerimientos de la documentación	Establecer los requisitos que deben poseer los requisitos relacionados con la seguridad de la información, estableciendo el control de documentos y de riesgos	21		RC derivados del proceso de producción (Operación, mantenimiento, Gestión Ambiental PRL)			
		22		No se revisan			
		23	100%	0%			
		24	100%	0%			
		25	100%	0%			
		26		Encargado de documentos: 4, no hay control: 0, otros:0			
5.0 Responsabilidad de la Gerencia							
5.1 Compromiso de la gerencia	Establecer si la alta gerencia de la Comisión presenta interés y un verdadero compromiso con el establecimiento de un sistema de gestión de seguridad de la información basado en el ciclo PDCA en sus procesos claves y de apoyo	27	75%	25%			
5.2 Gestión de recursos	Determinar la disposición de la Comisión para proporcionar recursos necesarios y el	28	100%	0%			
		30	0%	100%			

	compromiso de asegurar el entrenamiento, conciencia y competencia hacia los mismos	31	75%	25%			
6.0 Auditorías internas SGSI	Establecer si la Comisión conduce auditorías internas de acuerdo a los requisitos de seguridad de información internacionales.	32	0%	100%			
		33	0%	100%			
		33a	0%	100%			
		34		no existe			
7.0 Revisión gerencial del sistema SGSI							
7.1 Generalidades	Determinar si las revisiones se encuentran claramente documentada y sus registros mantenidos.	35	100%	0%			
		36		cada mes			
		37	0%	100%			
7.2 Insumo de revisión	Determinar si los elementos de entrada están debidamente establecidos	38		Resultado de aud:0, Retro alimentación de usuarios :3, Técnicas: 0, Acciones preventivas y corr.:0, vulnerabilidad o amenazas: 3, resultado de medición de controles :0			
7.3 resultado de la revisión	Establecer si los elementos de salida están debidamente establecidos	39		Necesidad es de recurso: 4			
8.0 Mejoramiento de SGSI							
8.1 Mejoramiento continuo	Establecer si la Comisión mejora continuamente la eficacia de su sistema de seguridad	40	0%	100%			
8.2 Acción Correctiva	Determinar si la Comisión posee acciones para eliminar la causa de no conformidad en cuanto a los requisitos de sistema y prevenir su recurrencia	41	0%	100%			
8.3 Acción Preventiva	Establecer si la Comisión determina acciones eliminando causas de no conformidad potenciales en cuanto a los requisitos del sistema y	42	0%	100%			

	así prevenir su ocurrencia						

Tabla 14: Resultados del cuestionario de la Unidad de Producción.

- ***EL DEPARTAMENTO DE PRODUCCIÓN REFLEJA UN 38% DE CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA ISO 27000.***

2) Unidad de Comercialización[12]

PUNTO DE LA NORMA	**OBJETIVO DE LAS PREGUNTAS DE CADA PUNTO**	**pregunta**	porcentaje	
			si	no
4.0 sistema de gestión de seguridad de la información				
4.1 Requerimientos Generales	Conocer si la Comisión cuenta con un sistema de gestión de seguridad de la información	2	83%	17%
	Conocer si los procesos involucrados se basan en el modelo planificar, Hacer , controlar, Actuar (PDCA)	3	100%	0%
4.2 Establecer y manejar el SIG	Establecer el alcance y políticas del sistema en términos de las características de los procesos.	4	83%	17%
		5	50%	50%
	Definir el enfoque de evaluación de riesgos, identificación, clasificación y análisis de los riesgos, medir el impacto que ocasiona y nivel admisible	6	17%	83%
		7	33%	67%
		8	33%	67%
		9	83%	17%
		10	17%	83%

[12] Ver Anexo 9 Tabulación de datos de encuesta para la Unidad de Comercialización.

	Establecer acciones de tratamiento de riesgos	11	67%	33%
	Establecer el plan de tratamiento de riesgos e implementarlo	12	33%	67%
		13	100%	0%
	Verificar si la Comisión cumple con las mejoras identificadas y qué tipo de acciones se toman al respecto.	14	0%	100%
		15	0%	100%
	establecer si la comisión ejecuta procedimientos de monitoreo y revisiones	16	17%	83%
		19	33%	67%
	Implementar programas de capacitación y conocimiento.	17	17%	83%
	Establecer mecanismos que detecten incidentes de seguridad.	18	0%	100%
	Definir si la Comisión mide la efectividad de los controles y si revisa las evaluaciones de riesgo.	20	17%	83%
	Establecer mecanismos y recursos para gestionar las operaciones en el manejo y seguridad de la información.	29	Equipo: 30%, Tecnología: 40%, Personal: 10%, Técnicas: 5%, Capacitaciones: 5%, Infraestructura: 5%, Efectivo: 5%	
4.3 Requerimientos de la documentación	Establecer los requisitos que deben poseer los registros relacionados con la seguridad de la información, estableciendo el control de documentos y de registros.	21	el 100% afirmo poseer manual de organización, de puestos, de procedimientos, reglamento interno y manual de Gestión Integrada	
		22	una vez al año	siempre que hay un cambio
			33%	67%
		23	33%	67%
		24	100%	0%

		25	100%	0%
		26	Existe un encargado de documentos: 83%	No existe control de documentos: 17%
5.0 Responsabilidad de la Gerencia				
5.1 Compromiso de la gerencia	Establecer si la alta gerencia de la Comisión presenta interés y un verdadero compromiso con el establecimiento de un sistema de gestión de seguridad de la información basado en el ciclo PDCA en sus procesos claves y de apoyo	27	100%	0%
5.2 Gestión de recursos	Determinar la disposición de la Comisión para proporcionar recursos necesarios y el compromiso de asegurar el entrenamiento, conciencia y competencia hacia los mismos	28	33%	67%
		29		
		30	67%	33%
		31	33%	67%
6.0 Auditorías internas SGSI	Establecer si la Comisión conduce auditorías internas de acuerdo a los requisitos de seguridad de información internacionales.	32	17%	83%
		33	33%	67%
		33 a	33%	67%
		34	UGI es la encargada	
7.0 Revisión gerencial del sistema SGSI				
7.1 Generalidades	Determinar si las revisiones se encuentran claramente documentada y sus registros mantenidos.	35	33%	67%
		36	el 100% afirma que se hacen periódicamente	
		37	50%	50%
7.2 Insumo de revisión	Determinar si los elementos de entrada están debidamente establecidos	38	resultados de auditorías: 10%, retroalimentación de usuarios: 70%, procedimientos de mejora: 5%, estado de las acciones: 5%, amenazas latentes: 5%, resultados de medir controles: 5%	

7.3 resultado de la revisión	Establecer si los elementos de salida están debidamente establecidos	39	mejorar la eficacia: 10%, actualizar plan de riesgos: 5%, modificar procedimientos y controles: 5%, necesidad de recursos: 80%	
8.0 Mejoramiento de SGSI				
8.1 Mejoramiento continuo	Establecer si la Comisión mejora continuamente la eficacia de su sistema de seguridad	40	17%	83%
8.2 Acción Correctiva	Determinar si la Comisión posee acciones para eliminar la causa de no conformidad en cuanto a los requisitos de sistema y prevenir su recurrencia	41	83%	17%
8.3 Acción Preventiva	Establecer si la Comisión determina acciones eliminando causas de no conformidad potenciales en cuanto a los requisitos del sistema y así prevenir su ocurrencia	42	67%	33%

Tabla 15: Resultados del cuestionario de la Unidad de Comercialización.

- ***LA UNIDAD DE COMERCIALIZACIÓN CUMPLE CON UN 47% DE LOS REQUISITOS RELACIONADOS CON LA NORMA ISO 27000.***

3) Unidad Informática Institucional[13]

PUNTO DE LA NORMA	OBJETIVO DE LAS PREGUNTAS DE CADA PUNTO	PREGUNTA	PORCENTAJE %				
			SI	NO	ALGUNAS	NO RESPONDIÓ	DESCONOCE
4.0 sistema de gestión de seguridad de la información							
4.1 Requerimientos Generales	Conocer si la Comisión cuenta con un sistema de gestión de seguridad de la información	2	85%	15%			

[13] Ver Anexo 10: Tabulación de datos de encuesta para la Unidad de Informática Institucional

	Conocer si los procesos involucrados se basan en el modelo planificar, Hacer , controlar, Actuar (PDCA)	3	92%	8%			
4.2 Establecer y manejar el SGSI	Establecer el alcance y políticas del sistema en términos de las características de los procesos.	4	69%	31%			
		5	77%	15%	8%		
	Definir el enfoque de evaluación de riesgos, identificación, clasificación y análisis de los riesgos, medir impactos que ocasionan y nivel admisible.	6	23%	69%		8%	
		7	62%	38%			
		8	62%	38%			
		9	61%	31%	8%		
		10	62%	38%			
	Establecer acciones de tratamientos de riesgos.	11	69%	31%			
	Establecer el plan de tratamiento de riesgos e implementarlo	12	61%	31%		8%	
		13	100%	0%			
			92%→1 año	8%→otros			
	Verificar si la Comisión cumple con las mejoras identificadas y qué tipo de acciones se toman al respecto.	14	100%	0%			
		15	62%→Pre	46%→Corr			
	Establecer si la Comisión ejecuta procedimientos de monitoreo y revisiones.	16	100%	0%			
		19	69%	16%			15%
		Mensual: 2; Anual: 4; No respondió: 2; Desconoce: 1					
	Implementar programas de capacitación y conocimiento.	17	62%	38%			
	Establecer procedimientos que detecten incidentes de seguridad.	18	46%	39%		15%	
	Definir si la Comisión mide la	20	46%	31%		23%	

	efectividad de los controles	Semestre: 1: anual: 2 Desconoce: 1; No respondió: 2					
	Conocer los recursos que destina la Comisión para gestionar las operaciones en el manejo y seguridad de la información.	29	Equipo: 11; Tecnología: 12; Personal: 10; Técnicas: 6; Capacitaciones: 10 Infraestructura: 11; Efectivo: 1; Ninguno: 1				
4.3 Requerimientos de la documentación	Establecer los requisitos que deben poseer los registros relacionados con la seguridad de la información, estableciendo el control de documentos y de registros.	21	Manual de Organización: 11; Manual de Puestos: 13; Manual de Procedimiento: 13; Otros: 7 (Políticas, Normativas e instructivos)				
		22	Siempre que hay un cambio: 12; Sin intervalo: 1				
		23	77%	0%	15%		8%
		24	100%	0%			
		25	100%	0%	Intranet: 6; Físicos: 1; No respon.: 6		
		26	Encargado: 9; Ningún control: 0; Otros: 2(Intranet, Control de vensiones); No respondió: 2				
5.0 Responsabilidad de la Gerencia							
5.1 Compromiso de la gerencia	Establecer si la alta gerencia de la Comisión presenta interés y un verdadero compromiso con el establecimiento de un sistema de gestión de seguridad de la información basado en el ciclo PDCA en sus procesos claves y de apoyo	27	85%	15%			
5.2 Gestión de recursos	Determinar la disposición de la Comisión para proporcionar recursos necesarios y el compromiso de asegurar el entrenamiento,	28	84%	8%	8%		
		30	92%	8%	Charlas: 9; Capa.: 7; Otras: 3 (Poner); No respondió: 1		
		31	46%	31%		23%	

	conciencia y competencia hacia los mismos						
6.0 Auditorías internas SGSI	Establecer si la Comisión conduce auditorías internas de acuerdo a los requisitos de seguridad de información internacionales.	32	69%	23%		8%	Anual: 8; No respondió: 1
		33	84%	8%		8%	
		33a	39%	15%		46%	
		34	Gestión Integrada: 8; Auditoría Interna: 8; Auditoría externa: 5; No respondió: 3; Corte de cuentas: 1				
7.0 Revisión gerencial del sistema SGSI							
7.1 Generalidades	Determinar si las revisiones se encuentran claramente documentada y sus registros mantenidos.	35	69%	31%			
		36	Anual: 7; Otros intervalos: 1; No respondió: 1				
		37	56%	22%		22%	
7.2 Insumo de revisión	Determinar si los elementos de entrada están debidamente establecidos	38	Resultados de auditorías: 7; Retroalimentación de usuarios: 3; Técnicas, productos o procedimientos de mejora: 2; Estado de acciones correctivas y preventivas: 6; Vulnerabilidades o amenazas latentes: 1; Resultados de medición de controles: 3; Otros: 0; No respondió: 2.				
7.3 resultado de la revisión	Establecer si los elementos de salida están debidamente establecidos	39	Mejora la eficacia: 6; Actualización del plan de tratamiento de riesgos: 2; Modificación de procedimientos y controles: 4; Necesidades de recursos: 3; Otros: 1; No respondió: 2.				
8.0 Mejoramiento de SGSI							
8.1 Mejoramiento continuo	Establecer si la Comisión mejora continuamente la eficacia de su sistema de seguridad	40	89%	0%		11%	
8.2 Acción Correctiva	Determinar si la Comisión posee acciones para eliminar la causa de no conformidad en cuanto a los requisitos de sistema y prevenir su recurrencia	41	84%	8%		8%	

8.3 Acción Preventiva	Establecer si la Comisión determina acciones eliminando causas de no conformidad potenciales en cuanto a los requisitos del sistema y así prevenir su ocurrencia	42	69%	23%			8%

Tabla 16: Resultados del cuestionario de la Unidad de Gestión de la Información.

- **EL PROCESO DE INFORMÁTICA TIENE COMO BASE UN 62% EN CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA ISO 27000**

4) Unidad de Desarrollo Humano

PUNTO DE LA NORMA	OBJETIVO DE LAS PREGUNTAS DE CADA PUNTO	PREGUNTA	PORCENTAJE %				
			SI	NO	ALGUNAS	NO SE TRATAN	NO RESPONDIÓ
4.0 sistema de gestión de seguridad de la información							
4.1 Requerimientos Generales	Conocer si la Comisión cuenta con un sistema de gestión de seguridad de la información	2	100%	0%			
	Conocer si los procesos involucrados se basan en el modelo planificar, Hacer , controlar, Actuar (PDCA)	3	100%	0%			
4.2 Establecer y manejar el SGSI	Establecer el alcance y políticas del sistema en términos de las características de los procesos.	4	100%	0%			
		5	100%	0%			
	Definir el enfoque de evaluación de riesgos, identificación, clasificación y análisis de los riesgos, medir el impacto que ocaciona y nivel admisible.	6	0%	100%			
		7	0%	100%			
		8	0%	100%			
		9	0%	100%			
		10	0%	100%			
	Establecer acciones de tratamientos de riesgos.	11	0%	100%			
	Establecer el plan de tratamiento de riesgos e implementarlo	12	0%	100%		0%	
		13					

	Verificar si la Comisión cumple con las mejoras identificadas y qué tipo de acciones se toman al respecto.	14					
		15					
	Establecer si la comisión ejecuta procedimientos de monitoreo y revisiones	16					
		19	100%	0%			
	Implementar programas de capacitación y conocimiento.	17	0%	100%			
	Establecer procedimientos que detecten incidentes de seguridad.	18	0%	100%			
	Definir si la Comisión mide la efectividad de los controles y si revisa las evaluaciones de riesgo.	20	100%	0%			
	Conocer los recursos que destina la comisión para gestionar las operaciones en el manejo y seguridad de la información	29		Personal, técnicas y equipo			
4.3 Requerimientos de la documentación	Establecer los requisitos que deben poseer los requisitos relacionados con la seguridad de la información, estableciendo el control de documentos y de riesgos	21		Manual de organización, manual de puestos, manual de procedimientos			
		22		Cada Trimestre			
		23	100%	0%	100%		
		24	100%	0%			
		25	100%	0%			
		26		Hay un encargado de procedimientos			
5.0 Responsabilidad de la Gerencia							
5.1 Compromiso de la gerencia	Establecer si la alta gerencia de la Comisión presenta interés y un verdadero compromiso con el establecimiento de un sistema de gestión de seguridad de la información basado en el	27	100%	0%			

	ciclo PDCA en sus procesos claves y de apoyo						
5.2 Gestión de recursos	Determinar la disposición de la Comisión para proporcionar recursos necesarios y el compromiso de asegurar el entrenamiento, conciencia y competencia hacia los mismos	28	100%	0%			
		30	100%	0%			
		31	0%	100%			
6.0 Auditorías internas SGSI	Establecer si la Comisión conduce auditorías internas de acuerdo a los requisitos de seguridad de información internacionales.	32	0%	100%			
		33	0%	100%			
		34		no existe			
7.0 Revisión gerencial del sistema SGSI							
7.1 Generalidades	Determinar si las revisiones se encuentran claramente documentada y sus registros mantenidos.	35	0%	100%			
		36					
		37					
7.2 Insumo de revisión	Determinar si los elementos de entrada están debidamente establecidos	38					
7.3 resultado de la revisión	Establecer si los elementos de salida están debidamente establecidos	39					
8.0 Mejoramiento de SGSI							
8.1 Mejoramiento continuo	Establecer si la Comisión mejora continuamente la eficacia de su sistema de seguridad	40					
8.2 Acción Correctiva	Determinar si la Comisión posee acciones para eliminar la causa de no conformidad en cuanto a los requisitos de sistema y prevenir su recurrencia	41	100%	0%			

8.3 Acción Preventiva	Establecer si la Comisión determina acciones eliminando causas de no conformidad potenciales en cuanto a los requisitos del sistema y así prevenir su ocurrencia	42	100%	0%			

Tabla 17: Resultados del cuestionario de la Unidad de Desarrollo Humano.

- **EL PROCESO DE RECURSO HUMANO CUENTA CON EL 52% DE LOS REQUISITOS DE LA NORMA ISO 27000 CUMPLIDOS.**

5) Matriz Consolidada

PUNTO DE LA NORMA	OBJETIVO DE LAS PREGUNTAS DE CADA PUNTO		PORCENTAJE %				
		PREGUNTA	SI	NO	ALGUNAS	NO RESPONDIÓ	DESCONOCE
4.0 sistema de gestión de seguridad de la información							
4.1 Requerimientos Generales	Conocer si la Comisión cuenta con un sistema de gestión de seguridad de la información	2	73%	27%			
	Conocer si los procesos involucrados se basan en el modelo planificar, Hacer , controlar, Actuar (PDCA)	3	92%	8%			
4.2 Establecer y manejar el SGSI	Establecer el alcance y políticas del sistema en términos de las características de los procesos.	4	63%	37%			
		5	82%	16%	2%		
	Definir el enfoque de evaluación de riesgos, identificación, clasificación y análisis de los riesgos, medir impactos que ocasionan y nivel admisible.	6	10%	78%		2%	
		7	24%	76%			
		8	24%	76%			
		9	36%	62%	2%		

		10	20%	80%			
	Establecer acciones de tratamientos de riesgos.	11	59%	41%			
	Establecer el plan de tratamiento de riesgos e implementarlo	12	42%	66%		2%	
		13	50%	50%			
	Verificar si la Comisión cumple con las mejoras identificadas y qué tipo de acciones se toman al respecto.	14	25%	75%			
		15	16%	84%			
	Establecer si la Comisión ejecuta procedimientos de monitoreo y revisiones.	16	29%	71%			
		19	76%	20%			4%
		Mensual: 2; Anual: 4; No respondió: 2; Desconoce: 1					
	Implementar programas de capacitación y conocimiento.	17	100%				
	Establecer procedimientos que detecten incidentes de seguridad.	18	37%	59%		4%	
	Definir si la Comisión mide la efectividad de los controles	20	41%	53%		6%	
	Conocer los recursos que destina la Comisión para gestionar las operaciones en el manejo y seguridad de la información.	29	equipo: 23%, Tecnología: 32%, personal: 12%, Técnicas:8%, Capacitaciones: 11%, Infraestructura: 12%, efectivo: 2%				
4.3 Requerimientos de la documentación	Establecer los requisitos que deben poseer los registros relacionados con la seguridad de la información, estableciendo el control de documentos y de registros.	21	el 100% afirmo poseer manual de organización, de puestos, de procedimientos, reglamento interno y manual de Gestión Integrada				
		22	una vez al ano	siempre que hay un cambio	no lo revisan		

			8%	55%	37%		
		23	78%	16%	4%		2%
		24	100%				
		25	100%				
		26	Existe un encargado de documento	No existe control de documento			
			92%	8%			
5.0 Responsabilidad de la Gerencia							
5.1 Compromiso de la gerencia	Establecer si la alta gerencia de la Comisión presenta interés y un verdadero compromiso con el establecimiento de un sistema de gestión de seguridad de la información basado en el ciclo PDCA en sus procesos claves y de apoyo	27	90%	10%			
5.2 Gestión de recursos	Determinar la disposición de la Comisión para proporcionar recursos	28	79%	21%			
		30	48%	52%			

	necesarios y el compromiso de asegurar el entrenamiento, conciencia y competencia hacia los mismos	31	47%	47%		6%	
6.0 Auditorías internas SGSI	Establecer si la Comisión conduce auditorías internas de acuerdo a los requisitos de seguridad de información internacionales.	32	26%	72%		2%	
		33	25%	73%		2%	
		33a	18%	70%		12%	
		34	La unidad responsable de realizar las auditorias es la Unidad de Gestión Integrada;				
7.0 Revisión gerencial del sistema SGSI							
7.1 Generalidades	Determinar si las revisiones se encuentran claramente documentada y sus registros mantenidos.	35	50%	50%			
		36	el 23% ki hace anualmente y el 77% lo hace en otros intervaleos				
		37	27%	73%			
7.2 Insumo de revisión	Determinar si los elementos de entrada están debidamente establecidos	38	resultados de auditorías: 38%, retroalimentación 16%,, procedimientos de mejora: 42%, estado de las acciones: 0%, amenazas latentes: 2%, resultados de medir controles: 2%				
7.3 resultado de la revisión	Establecer si los elementos de salida están debidamente establecidos	39	mejorar la eficacia	actualizar plan de riesgos	modificar procedimientos y controles	necesidad de recursos	
			10%	5%	5%	80%	
8.0 Mejoramiento de SGSI							
8.1 Mejoramiento continuo	Establecer si la Comisión mejora continuamente la eficacia de su sistema	40	27%	70%		3%	

	de seguridad						
8.2 Acción Correctiva	Determinar si la Comisión posee acciones para eliminar la causa de no conformidad en cuanto a los requisitos de sistema y prevenir su recurrencia	41	67%	31%		2%	
8.3 Acción Preventiva	Establecer si la Comisión determina acciones eliminando causas de no conformidad potenciales en cuanto a los requisitos del sistema y así prevenir su ocurrencia	42	59%	59%			2%

Tabla 18: Resultados consolidados del cuestionario basado en la ISO 27000.

- LA CONSOLIDACIÓN DE TODOS LOS PROCESOS REPRESENTA QUE SE CUENTA CON UN 49.75% DE CUMPLIMIENTO BASE DE LOS REQUISITOS DE LA NORMA ISO 27000.

ii. Resultados de las Entrevistas.[14]

Criterios de evaluación:

Valor	Criterio	Descripción
1	Malo	Se toma como criterio de calificación malo aquel proceso que cumpla con los principios básicos de la norma ISO 27000 en un rango de 0 a 20%.
2	Regular	Es todo aquel proceso que cumple del 21% a 40% de las características del principio evaluado.
3	Bueno	Se tomara como criterio de calificación bueno cuando el proceso cumpla entre un 41% a 60% del principio evaluado.
4	Muy Bueno	Se establecerá como muy bueno el hecho que el proceso pueda garantizar el logro de 61% hasta a 80% de aplicabilidad en el principio evaluado.
5	Excelente	Excelente se le denominara a aquel proceso que cumpla entre 81% a 100% del principio en estudio.

Tabla 19: Criterios de evaluación de la entrevista.

[14] Ver Anexo 11 Tabulación de información de entrevistas de la Unidad de Producción, comercialización, Informática Institucional y Desarrollo Humano.

1) Unidad de Producción

PRINCIPIOS	PUNTUACIÓN
CONTROL	2
INTEGRIDAD	2
AUTENTICIDAD	2
DISPONIBILIDAD	1
UTILIDAD	2
CONFIDENCIALIDAD	1

Tabla 20: Resultados de la entrevista de la Unidad de Producción.

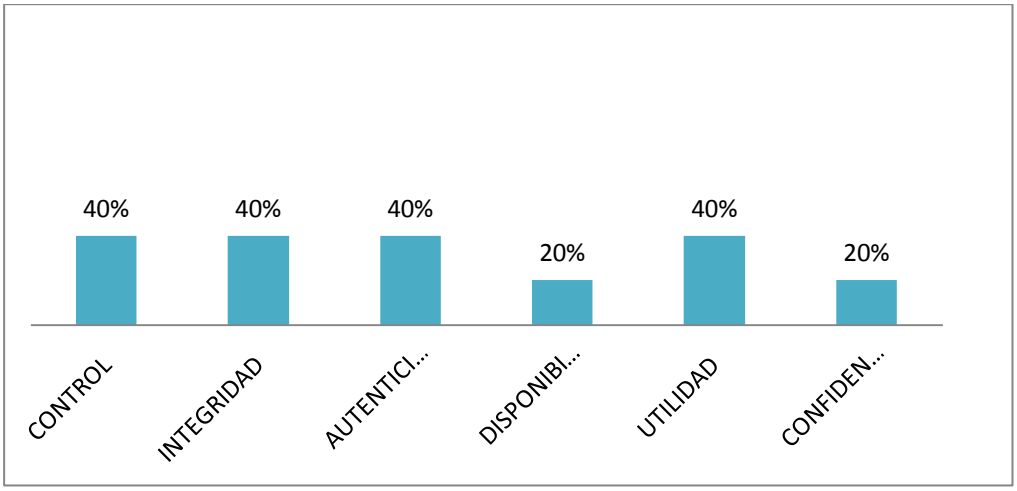


Grafico 1: Cumplimiento de principios en la Unidad de Producción.

2) Unidad de Comercialización

PRINCIPIOS	PUNTUACIÓN
CONTROL	1
INTEGRIDAD	2
AUTENTICIDAD	1
DISPONIBILIDAD	2
UTILIDAD	1
CONFIDENCIALIDAD	1

Tabla 21: Resultados de la entrevista de la Unidad de Comercialización.

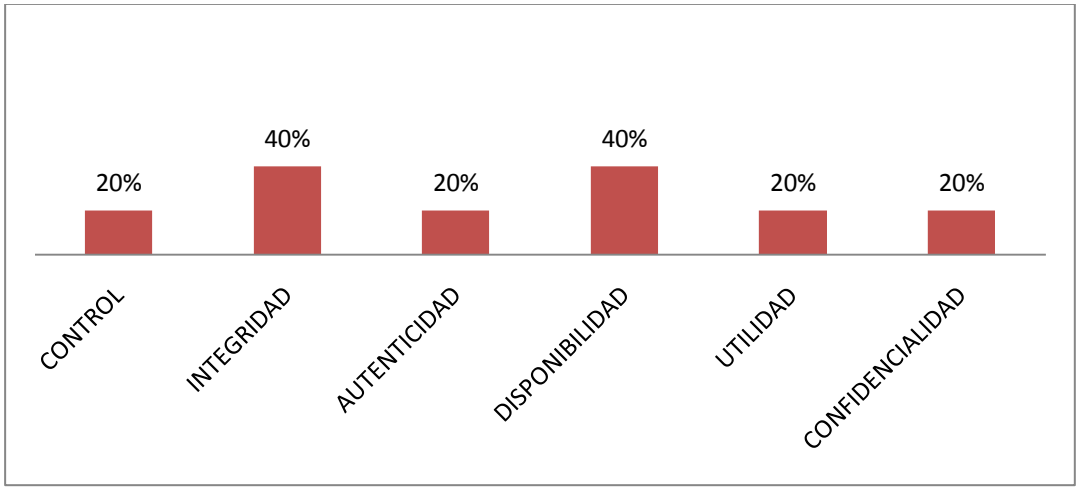


Grafico 2: Cumplimiento de principios en la Unidad de comercialización.

3) Unidad Informática Institucional

PRINCIPIOS	PUNTUACIÓN
CONTROL	2
INTEGRIDAD	1
AUTENTICIDAD	1
DISPONIBILIDAD	1
UTILIDAD	1
CONFIDENCIALIDAD	2

Tabla 22: Resultados de la entrevista de la Unidad de Informática Institucional.

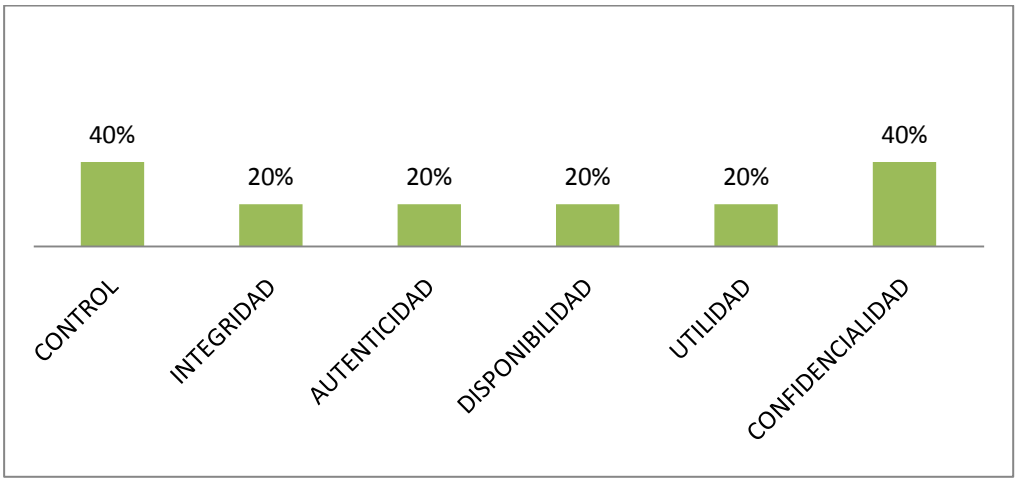


Grafico 3: Cumplimiento de principios en la Unidad de Informática Institucional.

4) Unidad de Desarrollo Humano

PRINCIPIOS	PUNTUACIÓN
CONTROL	1
INTEGRIDAD	1
AUTENTICIDAD	1
DISPONIBILIDAD	1
UTILIDAD	2
CONFIDENCIALIDAD	2

Tabla 23: Resultados de la entrevista de la Unidad de Desarrollo Humano.

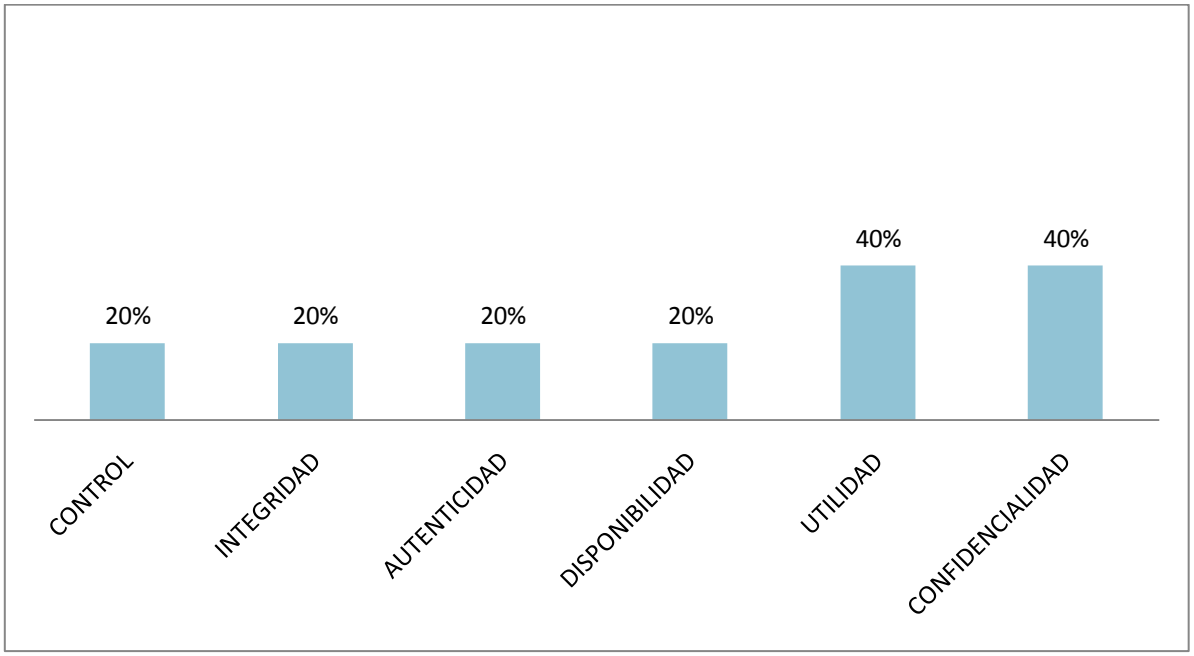


Grafico 4: Cumplimiento de principios en la Unidad de Desarrollo Humano.

Paso 9: ANALISIS DE LOS RESULTADOS

3. Identificación de amenazas y vulnerabilidades

Amenazas: (Inglés: Threat). Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

No.	Amenazas	Unidad afectada
1	Terremotos	Producción, Comercialización, Informática, Recursos Humanos
2	Incendios	Producción, Comercialización, Informática, Recursos Humanos
3	Robo de información	Producción, Comercialización, Informática, Recursos Humanos
4	Perdida de bases de datos	Producción, Comercialización, Informática, Recursos Humanos
5	Falsificación de firmas	Producción, Comercialización, Informática, Recursos Humanos
6	Falsificación de documentos	Producción, Comercialización, Informática, Recursos Humanos

Tabla 24: Identificación de Amenazas.

Vulnerabilidades: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

No.	Vulnerabilidades	Unidad afectada
1	NO se tiene definido un sistema de gestión para el manejo y seguridad de la información que respalden los procesos claves y de apoyo.	Producción, Comercialización, Informática, Recursos Humanos
2	NO existe definido un alcance y políticas para el manejo y seguridad de la información en todos los procesos	Producción, Comercialización, Informática, Recursos Humanos
3	NO existe un enfoque de evaluación de riesgos en todos los procesos	Producción, Comercialización, Informática,
4	NO se tiene plan de tratamiento de riesgos	Producción, Comercialización, Informática,
5	No se cuanta con acciones para el trato de riesgos	Producción, Comercialización, Informática, Recursos Humanos
6	NO hay controles definidos para el manejo y seguridad de la información en los procesos PARA 09-01, 17-02 y en el resto de las unidades	Producción, Comercialización, Informática, Recursos Humanos

No.	Vulnerabilidades	Unidad afectada
8	No hay programas de capacitación para el manejo y seguridad de la información en los PARA 22-01, 05	Recursos Humanos
9	No hay procedimientos definidos para el manejo y seguridad de la información en todos los procesos.	Producción, Comercialización, Informática, Recursos Humanos
10	NO se realizan auditorias que verifiquen el manejo y seguridad de la información	Producción, Comercialización, Informática, Recursos Humanos
11	No se tiene documentada información sobre el manejo y seguridad de la misma	Producción, Comercialización
12	No se tienen recursos destinados para el manejo y seguridad de la información	Producción
13	La gerencia no tiene conciencia sobre el valor de asegurar la información	Producción, Comercialización
14	No se tiene garantizada la integridad de la información	Producción, Comercialización, Recursos Humanos
15	Mucha información puede ser alterada con facilidad	Comercialización, Informática, Recursos Humanos
16	Hay personas que tienen acceso a documentos a los que no les concierne su uso	Producción, Comercialización
17	No se tienen definidos puntos de resguardo de la información	Producción, Comercialización, Informática, Recursos Humanos
18	No se posee con un archivo institucional	Producción, Comercialización, Informática, Recursos Humanos
19	El transporte de la información no es el adecuado, algunos documentos no regresan luego de ser prestados específicamente en los PRA 09-17,24, 44; 17-01, 08; 22-08,09,10,11; 41-01 al 11, 25 al 44	Producción, Comercialización, Informática, Recursos Humanos
20	Hay mucho manejo de información vía física, no hay definido un sistema de trasporte para documentación en todos los procesos	Producción, Comercialización, Informática, Recursos Humanos
21	Mucha información que se maneja no goza de autenticidad, solamente de un proceso de validación por firmas específicamente en los PRA 09-44, 17-11, 22-07 y 09-44, 17-11, 22-07 y 41-01, 41-33	Producción, Comercialización, Informática
22	La información no es accesible al 100%	Producción, Comercialización, Informática, Recursos Humanos
23	Los tiempos no son oportunos en algunas actividades de los procesos específicamente en el PRA 09-01, 44 y 41-01	Producción, Comercialización
25	Algunas actividades en los procesos no son cumplidas a cabalidad por ejemplo en el PARA 09-13, 17; 17-06, 07, 08; 22-03, 07; 41-17, 19, 67, 32, 27, 111.	Producción, Comercialización, Informática, Recursos Humanos
26	La información no es útil en su totalidad a los usuarios	Producción, Comercialización
27	Hay duplicidad de datos y de información por ejemplo en los	Informática, Recursos Humanos

No.	Vulnerabilidades	Unidad afectada
	PRA 17-11 y 21-03	
28	No hay definida una capacidad para localizar, evaluar y utilizar la información en todos los procesos.	Producción, Comercialización
29	Algunas personas tienen acceso a información confidencial y no les es de utilidad en el PRA 09-44	Comercialización
30	Cuando se intercambia información confidencial no se cuanta con procesos definidos para su resguardo en todas la unidades	Producción, Comercialización, Informática, Recursos Humanos
31	Los puestos de trabajo no cuentan con papeleras lo suficientemente seguras y bajo llave en todas las unidades	Producción, Comercialización, Informática, Recursos Humanos
32	Algunos escritorios no tienen sistemas de seguridad específicamente en las Unidades de procesos claves (los gerentes de las Unidades)	Producción, Comercialización
33	No se posee un manual para el manejo y seguridad de la información en todas las Unidades	Producción, Comercialización, Informática, Recursos Humanos
34	los hardwares no son lo suficientemente seguros	Informática
35	Los software para su almacenamiento no es el adecuado	Producción, Comercialización, Informática
36	No se respetan las horas y periodos de entrega de reportes en los PRA 09-44 y 41-01	Producción, Comercialización, Informática, Recursos Humanos
37	El personal no conoce sobre las bondades de aplicar un sistema de Gestión para el manejo y seguridad de la información	Producción, Comercialización, Informática, Recursos Humanos
38	Las contraseñas del sistema informático solo las posee una persona por ejemplo en las bases de datos de la Unidad de informática. No existe un respaldo por contingencia.	Informática
39	Algunas áreas del sistema no poseen contraseñas para evitar ser vistas por personas que no son de la Unidad tal es el caso de la Unidad de producción y Comercialización	Producción, Comercialización.

Tabla 25: Identificación de Vulnerabilidades.

De lo anterior se puede concluir que las unidades que poseen una mayor cantidad de vulnerabilidades son:

- **La unidad de producción y**
- **La unidad comercialización**

4. Análisis síntoma causa efecto[15]

SÍNTOMA	CAUSA	EFECTO
Quejas de los usuarios de los activos por no actualidad y disponibilidad de estos.	Falta de un protocolo para mantener los índices de actualidad y disponibilidad.	Retrasos en la toma de decisiones, que consumen tiempos ya pre establecidos por el reglamento legal interno.
Frecuente duplicidad de los activos con el fin de generar una copia a cada usuario que la solicite.	Desconocimiento y cuantificación del riesgo de extravío y duplicación de documentos.	Excesiva circulación de documentos e información de uso exclusivo en manos de personal que no debe poseerla.
Gran número de personas conocen datos de otros procesos que no tienen relación entre sí.	La garantía de privacidad y uso exclusivo es nula y se resume en el criterio del que genera el activo o lo posee en el momento.	Información de uso exclusivo en manos de personal que no debe poseerla.
Deficiente disponibilidad de la información en el tiempo requerido.	Documentos almacenados en base a criterios de espacio sin tomar en cuenta usos y tiempos de creación.	Retrasos en la toma de decisión en procedimientos administrativos.
18.2 % de las 325 transacciones mensuales sin retorno a sus emisores de préstamos.	Responsabilidades de uso y retornabilidad no establecidas. (tiempos y usos)	No se tiene como amparar y respaldar la ejecución de procedimientos.
Quejas de la administración de recurso por costos de materiales para transmisión de datos.	Duplicidad de documentos ya sea por reposición, solicitud de más de dos usuarios o pérdidas parciales.	Incremento en la demanda de materiales de 15% con relación al año anterior.
Quejas de proveedores por falta de pagos	Falta de controles en el manejo de facturas de proveedores	Pago de penalizaciones monetarias por incumplimiento de periodos de pago de facturas
Pocos licitantes para comercializar la energía hidroeléctrica	Inadecuada administración comercial de contratos de suministro	Mal servicio a los clientes
Datos equivocados sobre embalses	Mala administración de datos hidrológicos	Informes de generación equivocada y planes anuales con sesgo de información.
Reclamos de pobladores por no cumplir con los tiempos de descargas	Canales de flujo de información no son los adecuados atrasando envió de información para autorizar las descargas	Amonestaciones a CEL por incumplimiento y pago de multas.
Reclamos del mercado	Retrasos en la elaboración y envió de	Pérdidas económicas al no

[15] Ver Anexo 4: Herramientas y Técnicas de Ingeniería a utilizar

SÍNTOMA	CAUSA	EFECTO
mayorista	oferta de inyección al administrador del mercado mayorista	presentar la oferta a tiempo para su venta.
Maquinaria infectada con virus informáticos	No se cuentan con mantenimiento de sistemas informáticos de uso interno	Pérdida de tiempo y dinero, poca efectividad en la elaboración de informes comerciales a la gerencia
Atrasos en un mes para introducir datos históricos sobre la comercialización y producción de energía.	No existe control y seguimiento del análisis, diseño, desarrollo e implantación de sistemas informáticos.	Malas proyecciones para programación de venta y producción de energía.
Apagones en las maquinas del área de producción	Ineficiente gestión del mantenimiento preventivo a los equipos de computo	Perdida de información, eliminación de archivos importantes sobre niveles de producción, discos duros dañados y maquinas quemadas.
Archivos digitales removidos y/o modificados de las maquinas sin autorización	Rol de usuarios sin contraseñas	Pérdidas monetarias, atrasos de procesos, pérdida de tiempo para seguir con el flujo de proceso.
Personal con deficiencias en conocimientos técnicos	Elaboración del plan general de capacitación retrasado por falta de documentación externa de capacitadores.	Mal cálculo de presupuesto de personal generando saldo negativo al final del año fiscal 2007
Plazas sin personal a cargo	Reclutamiento y selección de personal engorroso debido a gran cantidad de información requerida y perdida de algunos curriculum de aspirantes	Atrasos en el proceso en proceso de recursos humanos y perdidas de efectividad en cumplimiento de actividades de la unidad
Personal de la unidad de Comercialización con asistencia irregular	Atención medica interna deficiente por atrasos en consultas y entrega de medicamentos	Proceso de comercialización paralizado y pérdidas de tiempo
Personal retirado sin pago de su pensión	Perdida de archivos con información de cotizantes con más de 20 años de antigüedad laborando para CEL	Pago de multas y mala imagen de la comisión
Distribuidoras de energía con déficit energético	La unidad comercializadora no dio el dato exacto a la Unidad de producción sobre cuando producir	Pérdidas económicas pues se produjo menos de lo requerido por las distribuidoras.
Energía que no se logra vender a las distribuidoras	No se acato la orden de paro de la Unidad generadora y/o la variación de potencia	Pérdidas económicas al no poder vender la energía en su totalidad.
Desconocimiento de personal de producción sobre niveles las presas de	Mal monitoreo de la instrumentación de las presas	Incumplimientos de la producción por contar con datos errados y suponer mayor cantidad de agua
Maquinaria con sonidos extraños y con irregularidades	No se da cuenta con un adecuado programa de mantenimiento	Paro de maquinaria, pérdidas monetarias, deterioro y fallas de

SÍNTOMA	CAUSA	EFECTO
	preventivo y correctivo	las mismas
Personal con enfermedades y accidentes ocupacionales	No se cuenta con una adecuada gestión de equipos para protección de personal	Pago de multas y pólizas de seguro por indemnizaciones a trabajadores

Tabla 26: Análisis Síntoma – Causa – Efecto.

5. Problemas e impactos detectados en los procesos claves y de apoyo

Los siguientes problemas fueron recopilados luego de una visita de campo a los diferentes procesos y a las entrevistas realizadas.

Nº	PROBLEMÁTICA ENCONTRADA	IMPACTO PERCIBIDO
	AÑO 2007	
1	En el año 2007 dentro del proceso de producción CEL registra 4 problemas de asunción de costos por firma de contratos con proveedores internacionales por no contar con las actas de contrato debidamente tratadas bajo un esquema sistemático de almacenamiento y ubicación	Se generaron costos de recontratación y pago de viáticos y honorarios alrededor de 60,000 dólares americanos así como retrasos de 1 mes en la puesta en marcha de proyectos de compra y modernización de maquinaria para procesos productivos
2	Desde el inicio del Año 2007 hasta el tercer trimestre del mismo se cuantifica 23 casos de falta de documentos digitalizados en medios magnéticos los cuales no entran al software de digitalización.	Perdida en tiempos productivos por parte de los jefes de las áreas de informática de 15 días por cada jefe (3) lo cual cuantifica 45 días de estos dedicados a resolver problemáticas, el costo de operación por pago de salarios asciende a 2,500 dólares americano, más retrasos en funciones adjudicadas a cada puesto
3	En agosto de 2007 se registra un caso de avería de una computadora central de un jefe de área en la cual se encontraba centralizada el consumo y cantidad a pagar de un cliente en mora.	Se estipula que el pago real del cliente fue de 4, 500,000.00 dólares americanos; pero el cliente alego que su consumo fue de 4, 415,000.00 dólares lo cual repercute en 85,000.00 dólares menos de facturación en mora.
4	En mayo de 2007 se presento un caso de ausencia de trabajo de un empleado por motivos de salud; que maneja de forma exclusiva los registros de salida de efectivo para pago de proveedores los cuales hacen sus cobros en base a contratos previos en transacciones bancarias sujetos a penalización. Dicho	CEL tuvo que pagar una clausula de penalización por incumplimiento de contrato por la suma de 10,000.00 dólares

Nº	PROBLEMÁTICA ENCONTRADA	IMPACTO PERCIBIDO
	problema se debió a la falta de mecanismos o protocolos de actuación ante la ausencia de personal clave y respaldo o copia de la información.	
	TOTAL IMPACTO MONETARIO 2007:	**157,500.00 dólares/Año 2007**
	AÑO 2008	
1	En el año 2008 en la Unidad de Comercialización por la falta de controles para el manejo y seguridad de la información se traspapelaron varias facturas las cuales tenían periodos de vencimiento para su respectivo pago,	Se cancelaron las facturas después del periodo de validez, dando lugar a una pérdida económica debida a pago de multas por un valor de $65,000
2	Debido a una mala administración de datos hidrológicos para el ano anterior se planificaron datos que al final se quedaron cortos para ser vendidos a las distribuidoras, se produjo muy poco para la proyección real de demanda.	Se produjo un costo de oportunidad al no producir energía que fácilmente puedo ser vendida a las empresas distribuidoras, la cantidad traducida monetariamente asciende a $ 850,000
3	Debido a un mal funcionamiento de los canales de comunicación en varias ocasiones el Sistema de Alerta Temprana no fue efectivo para las descargas de las presas. La información no fue oportuna y en ocasiones las descargas se realizaron antes de prever a la población de los riesgos dañando sus cultivos y viviendas	Debido a esos errores y falta de un buen manejo y aseguramiento de información CEL pago alrededor de $ 30,000 por daños a la propiedad privada de los pobladores cercanos a las represas.
4	CEL en diversas ocasiones no presento a tiempo las ofertas de inyección a la Unidad de producción, por lo que no se produjo lo demandado por la UT.	Se sufrieron costos de oportunidad significativos, alrededor de $ 150,000
5	Debido a un mal plan de actualización de actualización y desarrollo de sistemas informáticos CEL se atraso en la introducir los datos históricos para así proyectar los siguientes días.	CEL sufrió pérdidas al no poder realizar proyecciones reales en base a datos históricos. El costo de oportunidad fue de $180,000
6	Una mala gestión del mantenimiento preventivo de equipos informáticos ocasiono que dichas maquinas se arruinaran y todo como resultado de falta de controles y orden en las solicitudes recibidas.	Para CEL reponer activos fijos ocasiono un gasto que no estaba previsto en $7,000.
7	En el año 2008 a un analista de información le ocurrió que sin saber cómo unos archivos fueron extraídos de su computadora personal, todo indica que alguien robo dicha información pues no poseía password para poder ingresar a la misma, para suerte del analista dicha perdida de información no causo más estragos que pérdidas de tiempo en repetir los informes, el analista no tenia respaldo de la información.	Las pérdidas para CEL ocasionaron una semana de atraso en dichos informes, los costos de oportunidad ascendieron a las $6,000 pues no se pudieron atender diversas obligaciones que ya se tenían planeadas de no haber periodo el tiempo rehaciendo los informes
8	El año pasado se realizo la contratación de nuevo	En cuanto a costos dichos atrasos y el hecho

Nº	PROBLEMÁTICA ENCONTRADA	IMPACTO PERCIBIDO
	personal en CEL, dicho proceso fue lento y ocasiono que la plaza fuera cubierta con retrasos, al momento de que la persona tomo cargo desconocía algunos términos y formas de cómo realizar su trabajo, las capacitaciones no fueron hechas en su debido tiempo debido a una mala programación de las mismas pues la información de los capacitadores se extravió y tomo varios días localizarlos.	que la persona realizo mal cálculo del presupuesto del personal CEL cerró con un saldo negativo de $ 12,000 los gastos de de la Unidad de Recursos Humanos.
9	Recientemente un grupo de ex trabajadores llegaron a solicitar información para poder efectuar tramites de la pensión del INPEP, dichas personas solicitaron el historial de su trabajo en la comisión y se encontraron con que la Unidad encargada había Perdido dichos archivos, ya que por su antigüedad los archivos de microfilm se habían dañado por el mal resguardo de los discos. CEL tuvo que comprar una nueva máquina para leer microfilm y así poder leer dichos discos en mal estado, ya que la actual maquina no era lo suficientemente potente.	CEL gasto alrededor de $15,000 en la nueva máquina de microfilm y $8,000 en la remodelación del área de resguardo de dichos discos y así evitar que se siguieran dañando
10	La unidad de producción tubo varios inconvenientes en las cuales por falta de información no se pudieron hacer los mantenimientos de rutina, además que en una ocasión no se acato la orden de variación de potencia, en ambas ocasiones se tuvo que parar la producción y ocasiono costos de oportunidad	Los costos de oportunidad según el encargado de la presa cerrón grande ascendieron a $150,000 aproximadamente.
11	En la presa 15 de septiembre acontecieron una serie de accidentes de trabajo debido a falta de información que daba a conocer la necesidad de hacer uso de equipos de seguridad industrial, y alguna señalización sobre posibles zonas de riesgo. En total fueron 3 personas que se accidentaron y sufrieron daños leves pero que ocasionaron multas por parte del ISSS	El valor de las multas incurridas fue de $6,000 para bien de los trabajadores los daños no pasaron a mas y a los días retornaron a sus labores cotidianas.
	TOTAL DE IMPACTO ECONÓMICO 2008	**$ 1,479,000 /ano 2008**

Tabla 27: Identificación de problemas e impactos económicos 2007-2008.

6. Análisis de resultados relacionado con la norma (principios y requisitos).

El ramo de electricidad en El Salvador es uno de los sectores más importantes, generadores de ingresos y fuentes de trabajo, para el país, este sector ha sido uno de los más prósperos, es también uno de los sectores ejemplos de desarrollo organizacional e ingeniería y ha sido el que ha generado los más grandes avances en este sentido, en comparación con otras instituciones

nacionales, los cuales son utilizados para satisfacer la creciente demanda energética que El Salvador ha ido teniendo a lo largo de los últimos anos desde 1945 ano en el que fue instituida la comisión por decreto.

Desde los últimos cuatro años la Comisión ha venido resintiendo una desaceleración económica debida a políticas gubernamentales que le han exigido soportar con responsabilidades financieras fuera de su presupuesto, lo cual ha generado que la institución demande mucho más eficacia y eficiencia para la optimización de los recursos. En este sentido La Comisión mantiene una política de mejora continua, lo cual le ha permitido como se vio en los capítulos anteriores la obtención de diversas certificaciones en los ámbitos de calidad, gestión ambiental y seguridad laboral, dicha base abre la oportunidad de desarrollar nuevos sistemas encaminados a optimizar la estructura de procesos para generar resultados óptimos.
Sobre este contexto la información como activo juega un papel vital para el desarrollo económico de la empresa. La información en las instituciones nacionales es un tema complejo que requiere un buen manejo y seguridad que garantice la fidelidad de estos activos para mejorar la toma de decisiones con mayor certidumbre y mejores resultados.
Debido a lo valioso que resultan los activos de información para las instituciones nace la norma ISO 27000 cuyo tema central son los Sistemas de Gestión para el manejo y Seguridad de la Información (SGSI).

En nuestro país el tema de seguridad de información es un tema novedoso con grandes oportunidades de desarrollo en las principales instituciones gubernamentales y privadas, en el medio solo se cuenta con herramientas de Información enfocados a resguardar toda aquella información que se maneja por medio de tecnología electrónica, la cual viene diseñada por las grandes empresas productoras de Software y Hardware quedando con muchas limitaciones al aplicarlas en nuestro medio, para aquellos activos que no se manejan de manera electrónica; Dejando muchas amenazas y vulnerabilidades descubiertas y fuera de tratamiento tales como: desastres naturales y amenazas físicas generadas por la debilidad de los procesos.

En la actualidad solamente el Ministerio de Hacienda ha elaborado una plataforma de seguridad de la información bajo las normas ISO 27000 de manera parcial en una de sus aéreas mas criticas, la cual la convierte en una institución pionera en este tema, por lo demás, no hay ninguna institución nacional que cuente con un sistema de gestión de seguridad de la información que tome en cuenta los aspectos anteriores y que garantice niveles de seguridad internacionales.
En cuanto a la Comisión el tema relacionado con la seguridad de la información es también un tema novedoso y con mucho interés por parte de la junta directiva; y en este sentido se hace un análisis de cómo se encuentra la institución en aquellos procesos que son el centro de la actividad económica de CEL, identificados previamente en las certificaciones anteriores.

Por tanto se hace un análisis por cada proceso para presentar el estado actual de cada uno de ellos, partiendo de los instrumentos de análisis utilizados, encuestas, entrevistas y exploración de campo en estos procesos claves

Dado que la Comisión como se menciono anteriormente cuenta con una base de sistemas de gestión generados por las certificaciones obtenidas, se analiza cómo se encuentra cada proceso en relación a la evaluación de requisitos que busca la gestión y seguridad de la información según requerimientos internacionales.

a) Observaciones con respecto al cumplimiento de los Requisitos de la Norma ISO 27000

1. En la Unidad de Producción

En cuanto a los Requerimientos Generales (existencia de un SGSI y procesos bajo modelo PDCA), encontramos que el proceso de producción manifiesta en un 25% contar con un sistema estructurado de seguridad de la información, que al solicitar información del mismo se refieren a acciones de seguridad; mientras el restante 75% dice que no ó no lo conoce, así también basado en lo que se tiene, se asegura que en un 75% el proceso está basado en el ciclo PDCA

En relación al Establecimiento y manejo un SGSI; del total de items consultados bajo el criterio del establecimiento del sistema y manejo del mismo se obtiene que los requisitos se hayan cumplido en un 28%, mientras que un 62% respondieron que no se encuentra establecido adecuadamente un SGSI, es decir no existen políticas de seguridad, alcances definidos, identificación y tratamiento de vulnerabilidades, etc. Por tanto no se cumplen los requerimientos estipulados como de estricto cumplimiento por la Norma ISO 27000

Con respecto a los Requerimientos de la documentación, se observo que todos los involucrados en el proceso cuentes con los documentos requeridos, tales como manuales de organización, instructivo, etc.

Se encontró que un 75% de los encuestados considera que la gerencia presenta un interés verdadero en el sistema de gestión de seguridad de la información.

En contradicción con el requisito anterior se observa muy dividida la opinión del apoyo de la gerencia en relación a la gestión de recursos, observándose un 51.3% que reconocen que la institución si les brinda recursos suficientes mientras un 41.6% considera que los recursos no son suficientes o no existen

En relación a la revisión por parte de la gerencia este requisito se cumple en un 50% y que manifiestan que estas revisiones se llevan a cabo cada mes, mientras un 50% mantiene que estas revisiones no se realizan, demostrando un desinterés para controlar la información, esta situación se puede respaldar al observar en el año 2007, por un mal funcionamiento de los canales de información, en una clara violación a la disponibilidad de la misma, por no tener un efectivo Sistema

de Alerta Temprana ante las descargas que realizan las presas hidroeléctricas, CEL pago alrededor de $30,000 por daños a los cultivo y propiedades de los pobladores que se encuentran bajo la influencia del caudal proveniente de las descargas que realizan la presas.

En cuanto a los Insumo de revisión del sistema, se cuenta con dichos insumos de revisión, entre los mencionados tenemos Retroalimentación de usuarios, y las respectivas vulnerabilidades y amenazas; deja en evidencian como resultado la falta de recursos para controlar adecuadamente la información.

Con respecto al Mejoramiento continuo del sistema, el 100% de los encuestados establecen que la comisión no mejora continuamente la eficacia del sistema, por lo que ocasiona des actualidad del sistema que a su vez genera vulnerabilidades, tales como las planteadas en la tabla de Identificación de Amenazas y Vulnerabilidades, esto se evidencia al momento que CEL incurre en $60,000 en concepto de pago de penalización a proveedores de maquinaria y equipos de producción ya que el acta donde se encontraba el acuerdo de contrato con estos proveedores no estaba disponible en el momento adecuado.

En cuanto a la toma de acciones Correctivas, se obtuvo que el 100% de los encuestados manifiesta que dentro del proceso no se ponen en práctica las medidas correctivas ante una violación a la información, los que ocasiona que estas debilidades continúen presentándose como vulnerabilidades del sistema.

En relación con las acciones Preventiva, el 100% se reconoce que el sistema actual no cuenta con este tipo de acciones, generando así que estas debilidades potencialicen los riesgos.

2. En la Unidad de Comercialización

En cuanto a los Requerimientos Generales del sistema se encuentro que un 83% de los encuestados manifiesta que cuenta con un sistema de seguridad de la información, este alto porcentaje de debe a que en esta unidad se cuentan con la mayoría de procedimientos mecanizados por lo que las medidas de seguridad de los procedimientos representas según su interpretación un sistema de seguridad; así también en su totalidad conocen que este proceso está basado en un ciclo PDCA

Con respecto a establecer y manejar en SGSI, un 66% afirman que no se ha establecido ni se maneja un sistema de seguridad de la información, esto contrasta con el requisito anterior, esto es debido a que al conocer en qué consiste establecer y manejar un SGSI se dan cuenta que no poseen con cada una de los elementos que garantizar el establecimiento del Sistema (Alcance, políticas de seguridad, plan de tratamiento de riesgos, inventario de vulnerabilidades, etc.); por lo que queda en evidencia el desconocimiento de la Norma y la no existencia de un Sistema de gestión que asegure la información.

En relación a los Requerimientos de documentación, el 66.5% de los encuestados manifiesta poseer la documentación requerida; así como también la revisión de los documentos se realiza una vez al año y cada vez que hay cambios, cave denotar que existe un encargado para manipular la documentación.

En cuanto al Compromiso de la gerencia, Según lo recolectado en la encuesta si se percibe un interés por parte de la alta gerencia en lo que respecta a la seguridad de la información de un 100%, no así cuando a Gestión de recursos se refiere, este rubro se encuentran un tanto divididos ya que el 55% dice que al departamento no se le apoya con recursos orientados a la seguridad de la información y un 44% dice si percibir apoyo de la gerencia este en función de: Tecnología, equipo y personal.

Con respecto a las Auditorías internas del Sistema, un 72% de los encuestados afirman que dentro de comercialización si se audita el sistema de información, afirman que los encargados de esta tarea es la gestión de la información, es importante mencionar que las auditorias se limitan a medidas puntuales como revisión de contraseñas y mantenimiento de los sistemas operativos; por lo contrario un 28% de la población confirma no poseer ningún mecanismo de auditoría interna del Sistema.

En relación a los Insumo de revisión, el 70% contesto que los elementos de entrada para revisión del sistema se basan en las quejas de los usuarios, por lo que evidencia que no poseen un mecanismo que se encargue de revisar el sistema y detectar posibles fallas, dejando esta posibilidad solo cuando el usuario del mismo se queja, creando atrasos en la toma de decisión tal como se observo por la descarga del sistema de unas facturas que aun no se habían procesado, incurriendo en un pago de penalización por $65,000

En cuanto a los resultados de la revisión, en un 80% coinciden que el resultado del análisis de las quejas termina en establecer la necesidad de recursos, esto indica que se trabaja bajo un sistema de prueba y error.

Con respecto al Mejoramiento continuo del sistema, un 83% de los encuestados dice no percibir un mejoramiento continuo del sistema actual, por los que se experimenta un estancamiento en cuanto a mejorar el aseguramiento de la información, para evidenciar esta situación se observo que para el año 2008, por falta de una planeación y análisis de datos hidrológicos se produjo muy poca electricidad en comparación a la creciente demanda por lo que no se pudo abastecer eficientemente el producto a las distribuidoras, esto ocasiono perdidas traducidas en $850,000 en concepto de costo de oportunidad y costo de compra de energía mas cara a países de la región, esto con el propósito de no desabastecer el mercado demandante.

En relación a las acciones Correctivas, un 83% de los encuestados dice que siempre se toman acciones correctivas luego de descubrir una amenaza o vulnerabilidad en el sistema, partiendo de este hallazgo se puede inferir mediante inspección física del proceso que esta la capacidad de

respuesta de la unidad se restringida ya que se detiene el proceso cuando un usuario se queja y se debe atender de inmediato la necesidad, esta provoco una mala lectura de las ofertas de inyección arrojando un dato considerablemente equivocado que produjo perdidas cuantificadas en $150,000, como costo de oportunidad; este resultado encontrado los confirma la poca disposición a las Acciones Preventiva, ya que un 67% de los encuestados considera que el departamento no toma acciones que permitan reducir el riesgo futuro, propiciando que las vulnerabilidades actuales y futuras estén expuestas a las amenazar tanto actuales como las futuras, abriendo la posibilidad de incurrir en mayores costos por no poseer un sistema adecuado que garantice la plena seguridad de la información como un activo importante para el desarrollo de la Comisión, en su negocio.

3. En la Unidad Informática Institucional

En cuanto al cumplimiento de los Requerimientos Generales, según el universo de encuestados, el 85% manifiestan que el proceso de informática cuenta con un sistema de seguridad de información, es importante mencionar que como unidad Informática Institucional, son los generadores de toda la seguridad de la información en términos de informática, poseen un mecanismo que controla digitalmente entradas y salidas de información; pero no se posee un protocolo que este definido como un sistema de gestión general; también que un 92% contestaron que sus procesos se encuentran basados en el ciclo PDCA

Con respecto a establecer y manejar un SGSI, del universo consultado en el área de informática un 59% de su respuesta respaldan que cuentan con un sistema de seguridad que cumple con los requerimientos pero un 41% de su respuesta dice no cumplir con los requerimientos mínimos, aquí se evidencia la carencia de una estructura que se encargue de gestionar de manera armónica y articulada la información generada por los procesos claves del negocio.

En lo que corresponde a los Requerimientos de la documentación, Informática cuenta con documentos relacionados con los manuales de puestos y procedimiento así como también políticas, normas e instructivos, los documentos se actualizan siempre que hay un cambio, se cuenta con un encargado de procesos.

En relación al Compromiso de la gerencia, un 85% de los encuestados dicen que la gerencia del departamento presenta interés en la seguridad de la información, y que a su vez existe un 74% de los encuestados reconocen el apoyo de la gerencia en asignar recursos para resguardar la seguridad

En cuanto a las Auditorías internas del Sistema, un 64% de los encuestados dijeron conocer y saber que el departamento conduce auditorias relacionadas con la seguridad mientras un 20% respondió que no existe ninguna auditoría interna relacionada a la seguridad de la información, esta declaración es relevante mas cuando viene de la unidad que es la encargada de velas por la buena administración y resguardo de la información generada por los procesos claves de la Comisión.

Con respecto a la Revisión del sistema por la gerencia, un 37.5 admite que no se realiza ninguna acción de este tipo, es decir la gerencia poco o nada se interesa en realizar revisión para conocer las condiciones de la seguridad de la información; mientras que un 62.5% de los encuestados reflejan que las revisiones se encuentran claramente documentadas; esto se vio reflejado al incurrir en un costo de $180,000 por no mantener actualizado los registros históricos de la demanda de energía, ya que se detecto un atraso en su ingreso al sistema por lo que ocasiono una proyección de inyección deficiente.

En lo que corresponde al Mejoramiento continuo, un 89% afirma que la Comisión si mejora la eficacia de manera constante, está respaldado por un 84% que asegura que la comisión si realiza acciones correctivas para eliminar las causas de no conformidad, y un 69% dice que si se realizan acciones preventivas para disminuir el riesgo, esto como herramientas para mejorar la seguridad de la información; es importante señalar que un 31% de los encuestados manifiesta no realizar acciones preventivas para enfrentar y minimizar riesgos futuros, por lo que se observa una práctica aislada de estas acciones preventivas y no como parte de un manejo institucional dentro de la Comisión.

4. En la Unidad de Desarrollo Humano

En relación con los Requerimientos Generales del sistema, en el proceso de RRHH se puede observar que el 100% de los encuestados manifiestan contar con un sistema de seguridad de la información, el cual al investigar de que se trata, este consiste en uso de permisos, contraseñas y roles, es decir una serie de acciones de seguridad pero que no obedecen a un enfoque se sistema que gestiones la seguridad de manera estructurada.

En cuanto a establecer y manejar un sistema de seguridad, un 64% de las respuestas sostienen que no existe establecido ni en operación, es decir no se cuenta con el marco que de soporte a un sistema de aseguramiento como tal, esto respalda la conclusión anterior; solo un 28% respalda que si se cuenta con un sistema

Con respecto al cumplimiento de los Requerimientos de la documentación se encontró que se tienen documentos como manuales, procedimientos, etc., no así no poseen ningún documento que respalde la seguridad de la información tales como manual de tratamiento de riesgo, procedimientos ante amenazas latentes, etc.

En lo que corresponde al Compromiso de la gerencia, según lo recolectado en la encuesta si se percibe un interés por parte de la alta gerencia en lo que respecta a la seguridad de la información, lo que a su vez genera un 66% que indica que se gestionan recursos para asegurar la información frente a un 33% que manifiesta que la gerencia es muy reservada al momento de reiterar este apoyo con recursos necesarios, no se percibe una inversión tangible por parte de la gerencia para destinar recursos que fortalezcan la seguridad de la información.

En relación a las auditorías internas del sistema el 100% de las respuestas demuestran que no existen auditorías internas relacionadas con la seguridad de la información, este elemento es muy importante ya que demuestra el poco interés que se tiene en cuanto a verificar condiciones de seguridad existentes dentro de este proceso, esto lo respalda un costo de $6,000 generado por la falta de medidas de control, ya que se detecto la perdida de documentos que no poseían ningún respaldo de seguridad.

En cuanto a la revisión del sistema por la gerencia, la respuesta es contundente no revisiones por parte de la gerencia para verificar las condiciones de seguridad de la información, como consecuencia a lo anterior CEL estimo costos de hasta $12,000 por el atraso en un proceso de contratación imputado a la Unidad de Desarrollo Humano, ya que este atraso ocasiono la falta de un recurso y cumpliera funciones importantes en un puesto de trabajo, trayendo consigo retraso en resolver tramites de comercialización y por consiguiente retraso en la toma de decisiones.

En lo que corresponde a la ejecución de acciones correctivas el 100% de los encuestados manifiesta que aun cuando no se tiene un sistema completo de seguridad de la información, es evidente que se cuenta con una estructura la cual resguarda la seguridad y siempre que ocurre una violación al sistema y que ayuda a corregir la causa; así como también se ejecutan acciones preventivas en el 100% de las ocasiones que se detectan amenazas, minimizando así el riesgo potencial.

b) Observaciones con respecto al cumplimiento de los principios de la Norma ISO 27000

1. En el proceso de Producción.

Lo relacionado con el principio de control:

La información que se maneja es de dos tipos los RC (registros de calidad) y datos históricos, también se manejan información de proyectos (patrimonios de CEL), esta última información no se tiene controlada, los controles para toda la información se quedan cortos limitándose a los check list que llevan los RC, cada productor es responsable de controlar su información, no se tiene definidas políticas de control ni criterios definidos y ni documentados, para la información física como correspondencia, RC, y de proyectos se posee un inventario de archivo, los controles se realizan diarios y se ha, mejor manejo y aseguramiento de la misma, los impactos por no controlar la información son pérdidas económicas, tiempos inactivos y mala toma de decisiones como se observa en el cuadro de problemas e impactos detectados en los procesos claves y de apoyo

En el principio de integridad:

Las personas que manipulan los documentos durante su proceso y su transporte son los productores de la misma, solamente el Jefe de la Unidad puede autorizar su manipulación a personas ajenas y define a la vez las responsabilidades por hacerlo, los tipos de manipulaciones que se hacen a los documentos son registros y revisiones, y se garantiza que solo se hagan las modificaciones que provienen de la jefatura llevando un registro por medio de firmas, el almacenamiento se asegura de

igual manera, solamente el jefe tiene el poder para autorizar que y quien será el responsable de su almacenamiento, los impactos en una alteración a un documento pueden ser amonestaciones para los empleados y en el peor de los casos llegar a despidos, pueden caer en ilegitimidad de datos duplicidad de información y pérdida de tiempo. En general se está trabajando en asegurar la integridad pero no hay políticas y documentos que establezcan dicha normativa

Analizando el principio de autenticidad:
La forma de garantizar la veracidad de la información es revisándola previamente aunque es probable en un 20% que existan inconformidades en la misma, la forma de hacer dichas revisiones es como parte del proceso y se respalda con un autocontrol, los impactos al no garantizar y poseer información autentica pueden ser atrasos en la producción, atrasos en ordenes de mantenimiento de maquinaria, pérdidas económicas, aumentar costos de producción y mala toma de decisiones.

En lo que respecta al principio de disponibilidad:
La disponibilidad de la información se obtiene como parte del flujo del proceso, para estar disponible según sea requerida, los tiempos están establecidos pero en ocasiones el sistema de información no responde generando atrasos y los canales de información pasan de ser electrónicos para convertirse en vía telefónica, los planes contingenciales no están definidos para esos casos, generando ineficiencia en los procesos, es por tal motivo que la información no siempre está disponible, los canales de información en su mayoría son electrónicos. La información no siempre esta ordenada y/o documentada, los sistemas de información no son muy confiables, no se generan respaldos a la misma, esta situación ha generado hasta $150,000.00 por costo de oportunidad tal como lo vemos en el cuadro problemas e impactos detectados.

En el principio de utilidad se encontró que:
La información que se utiliza se obtiene como parte del flujo de proceso, los volúmenes de información son grandes pues esta unidad representa ser el corazón de CEL pues es la encargada de producir la energía hidroeléctrica, es por eso que toda la información recibida o generada es útil, y se identifica o categoriza de esa manera ya que contribuye de manera directa a los procesos, en porcentaje el 90% de la misma es útil, y la frecuencia de uso es diaria, los impactos que se pueden derivar de no darle un buen uso a la información son: que no se produzca lo requerido por la unidad de comercialización, o pérdidas económicas por aumento de costo o generación de costos de oportunidad, puede generar también subutilización de recursos y perdidas de mercados los cuales se encuentran cuantificados en el cuadro de problemas e impactos.

Del principio de confidencialidad se encontró:
Existe información confidencial, siendo del total el 80% confidencial (obtenido de jefe de unidad), manejada a niveles gerenciales, la información de uso general se encuentra en las computadoras de cada empleado de la Unidad y otra de manera física, los controles son pocos o casi nulo y no se cuenta con procedimientos de aseguramiento de la información, para acceder a ese tipo de documentos se tiene que poseer una autorización de parte de jede de la unidad, los medios que se

dedican para transpórtala son electrónicos y físicos, existen vulnerabilidades que pueden generar quebrantamiento en los sistemas dando lugar a fugas de información, por ejemplo si una persona no le da un uso correcto a la misma, o que alguien fuga la información con fines personales, los impactos son mala imagen para la institución, mal ambiente laboral y despidos.

2. **En el proceso de Comercialización.**

Del principio de control se encontró:
No se tiene definida una política, los controles no están definidos ni documentados, no se poseen índices, solamente el personal autorizado tiene control sobre la misma, se corre el riesgo de retrasos en el proceso, duplicidad de datos, infidelidad de la información, impactos y pérdidas económicas
En el año 2008 se traspapelaron varias facturas las cuales tenían periodos de vencimiento para su respectivo pago, eso provoco que las facturas se cancelaran después del periodo de validez, dando lugar a una pérdida económica debida a pago de multas por un valor de $65,000

Del principio de integridad se encontró:
No hay una persona encargada para manipular los documentos en la unidad, cada quien es responsable de cada documento emitido por el mismo, solamente el jefe de la unidad autoriza y define las responsabilidades de manipulación, las manipulaciones que se le hacen a la información básicamente son de monitoreo y para modificar algo en la data tiene que hacerse previa autorización del jefe de la unidad, No existen garantías de que los documentos tengas solamente las alteraciones autorizadas pues se carece de controles documentados, para fines de acceso a la información por personal autorizado existe una persona encargada y autorizada para manejar su integridad, los impactos que se pueden generar al infringir dicho principio son, impactos de tipo económico, mal ejecuta miento del proceso y una mala toma de decisiones

Del principio de autenticidad se encontró que:
El analista de mercado es el encargado de garantizar que la información suministrada es real y veraz, la verificación se hace como parte del análisis, del 100% de la información solo tiene control sobre la emitida por CEL cotejándola contra datos históricos filtrándola, a la vez mucha información proviene de fuentes externas y no hay manera de verificarla. Los impactos que generaría una información no veraz e mala toma de decisiones, pérdidas económicas por no ofertar lo que realmente se demanda. Un caso concreto que sucedió el año pasado es:
Debido a una mala administración de datos hidrológicos se planificaron datos que al final se quedaron cortos para ser vendidos a las distribuidoras, se produjo muy poco para la proyección real de demanda, Se produjo un costo de oportunidad al no producir energía que fácilmente puedo ser vendida a las empresas distribuidoras, la cantidad traducida monetariamente asciende a $ 850,000

Del principio de disponibilidad se encontró que:

La información llega a la unidad como parte del flujo de proceso, existen horas definidas para la disponibilidad de la misma, solamente cuando hay problemas de red se dan casas de indisponibilidad, o en casos de variaciones climáticas, en condiciones normales el 70% de la información está disponible, la información llega en su mayoría de forma electrónica por medio de e mails, bases de datos de la UT, por la intranet y físicamente por medio de Faxes por lo que los canales son los adecuados, el personal autorizado al acceso a la información cuenta con ella cuando él la requiere ya que la UT es independiente de la comisión y ella es la que abastece a los analistas, los impactos que se pueden generar al no poseer información oportuna son: pérdidas económicas al no ofertar lo que realmente el mercado demanda, pueden haber malas decisiones y atrasos en el proceso de comercialización.

Un caso concreto sucedió en el año 2008, en diversas ocasiones no se presento a tiempo las ofertas de inyección a la Unidad de producción, por lo que no se produjo lo demandado por la UT, originando costos de oportunidad significativos, alrededor de $ 150,000

Del principio de utilidad se encontró:

La información que se utiliza se obtiene como parte del proceso y se utiliza en horas ya establecidas, el volumen de información es grande ya que se manejan bases de datos, la información física es poca, toda la información es importante pero no toda se utiliza pudiéndose dividir en datos oficiales y no oficiales, la manera de identificar si la información es útil es de manera empírica no se tienen controles no políticas de utilidad, solamente se identifica como útil si el proceso la requiere, el 95% de la misma es útil y se utiliza diariamente. Los impactos al no usar de buena manera la información pueden ser en su mayoría perdidos de tiempos, atrasos en el proceso y pérdidas económicas.

Debido a un mal funcionamiento de los canales de comunicación en varias ocasiones el Sistema de Alerta Temprana no fue efectivo para las descargas de las presas. La información no fue oportuna y en ocasiones las descargas se realizaron antes de prever a la población de los riesgos dañando sus cultivos y viviendas. Debido a esos errores y falta de un buen manejo y aseguramiento de información CEL pago alrededor de $ 30,000 por daños a la propiedad privada de los pobladores cercanos a las represas

Del principio de confidencialidad se encontró:

Dentro de la unidad si existen datos confidenciales, en su mayoría es externa solamente un 25% es de CEL, pero a la vez no se tiene definidos criterios de confidencialidad, aunque se cuenta con contraseñas para ingresar a las bases de datos de las mismas, actualmente solamente las personas que el jefe de la unidad ha autorizado pueden tener acceso, por lo que la probabilidad de que personas ajenas a dicha unidad tengan acceso a la misma es mínima de no ser que se quebranten dichas contraseñas, existen casos especiales de personas que pueden tener acceso a dicha información atribuidas a la alta tenencia. Los medios para trasportarla son en medios electrónicos y en medios físicos, se generan back up para poder tener un respaldo de toda la información, aunque dicho back up no es el 100% seguro. Es muy poco probable que la información confidencial sea vista por personas ajenas a la unidad ya que existen sistemas de correspondencia interna contra firmas y

claves de acceso. Los impactos generados pueden ser negativos si cae información de este tipo en manos equivocadas, generando mala imagen a la comisión, mal manejo político, amonestaciones y despidos al personal, etc. en general hay ciertos temas trabajando en este sentido pero nada está definido ni documentado

3. **En el proceso de Gestión de la Información.**

Del principio de control se encontró:
Los documentos que se manejan en su mayoría son de tipo digital, en esta unidad la labor es más de procesamiento de información que de producción de la misma. Al igual que las demás unidades posee RC los cuales tienen sus controles definidos, para la información física se llega un control de correspondencia, cada área de la Unidad es encargada de llevar sus controles, en términos generales los controles más estrictos son hacia las bases de datos que desde acá se alimentan, los controles son estrictos y se basan en juegos de contraseñas, además se llevan back ups los cuales son otros controles para su aseguramiento, solamente la jefe de la unidad y de las aéreas son los encargados de controlarla. Una mala gestión del mantenimiento preventivo de equipos informáticos ocasiono que dichas maquinas se arruinaran y todo como resultado de falta de controles y orden en las solicitudes recibidas. Para CEL reponer activos fijos ocasiono un gasto que no estaba previsto en $7,000

Del Principio de integridad se encontró:
Para asegurar la integridad los documentos son manipulados solo por personas de la unidad, en algunos casos se hace uso de los ordenanzas pero para manejar memos y documentos de menor relevancia. La jefa es quien autoriza quien y bajo que responsabilidades se manejara la información, pero nada está documentado, no hay un sistema que asegura la integrada de la misma. Las manipulaciones son de tipo física y digital, y se garantiza que el documento solo tenga las modificaciones ordenadas por medí o de firmas, para que el usuario tenga acceso a la información no hay medidas que regulen dicho acceso no hay políticas de restricción, y para su almacenamiento solo el jefe del área posee las llaves de acceso. Los impactos al no asegurar la integridad de la información pueden ocasionar grandes pérdidas de tiempo, además de penalidades definida en el reglamento interno.

Del principio de autenticidad se encontró:
Para asegurar la autenticidad, se verifican que las firmas sean originales, no hay procedimientos establecidos, para respaldar la información se realizan prácticas de autocontrol y generación de respaldo de datos. Básicamente por no poseer documentos e información autentica pueden generarse decisiones inadecuadas y atrasos en el proceso.

Del principio de disponibilidad se encontró:
La información se encuentra disponible como parte del proceso y por medio de solicitudes, los tiempos de arribo son oportunos a pesar de que no se tienen registrados los tiempos de respuesta ni

de entrega/recibo. Cuando es información del área siempre esta oportuna, se generar atrasos cuando se requiere consultar información que es ajena a la unidad de comercialización. Los canales para su disponibilidad son intranet, por e mail, y de manera física, el personal cuenta con la información cuando la requiere, los atrasos son mínimos, los impactos al no poseer la información disponible son resultados atrasados, inconformidades y pérdidas económicas

Debido a un mal plan de actualización de actualización y desarrollo de sistemas informáticos CEL se atraso en la introducir los datos históricos para así proyectar los siguientes días. CEL sufrió pérdidas al no poder realizar proyecciones reales en base a datos históricos. El costo de oportunidad fue de $180,000

Del principio de Utilidad se encontró:

Para asegurar la utilidad la información se obtiene como parte del proceso, el volumen de información para ser utilizado es mínimo pues en esta unidad no se produce mucha, sino más bien se procesa. Y se identifica su utilidad bajo un proceso de depuración y eliminación, la frecuencia de uso es diaria y se utiliza el 100% de lo que se recibe. El mal uso de la información puede generar malas interpretaciones y malos entendidos así como atrasos y pérdida de tiempo.

Del principio de confidencialidad se encontró:

Por ser anda unidad de apoyo y que brinda servicios a toda la comisión posee una gran cantidad de información confidencial, en un 60% lo es, ya que se manejan bases de datos, redes, información sobre palmillas, tesorería, etc. para tener acceso a la información se tiene definido un procedimiento y se garantiza por medio de roles de acceso, usuarios especiales, etc. cada persona en su procesamiento es responsable de cuidar su información, y solamente las personas del área tiene acceso previa autorización de los jefes superiores o en máxima instancia de la Jefe de la Unidad, también tiene acceso la alta gerencia. Los medios de transporte son sobres sellados y por medio de e mail, bases de datos con llaves. Cualquier pérdida o fuga de información puede darse y se atribuyen más a errores humanos pues se tiene bastante confianza en el sistema informático. Cualquier violación a la información de este tipo generara amonestaciones o despidos. Y para la comisión los impactos negativos pueden ocasiones mala imagen, y vulnerabilidades en las redes

En el año 2008 a un analista de información le ocurrió que sin saber cómo unos archivos fueron extraídos de su computadora personal, todo indica que alguien robo dicha información pues no poseía password para poder ingresar a la misma, para suerte del analista dicha perdida de información no causo más estragos que pérdidas de tiempo en repetir los informes, el analista no tenia respaldo de la información. Las pérdidas para CEL ocasionaron una semana de atraso en dichos informes, los costos de oportunidad ascendieron a las $6,000 pues no se pudieron atender diversas obligaciones que ya se tenían planeadas de no haber periodo el tiempo rehaciendo los informes

4. **En el proceso de Desarrollo Humano.**

Del principio de control se encontró:
Los documentos que manejan son sobre el personal que labora en la comisión, hay desde formularios hasta acciones al personal, se maneja en forma digital y en forma física, los controles hacia ellos están declarados en el sistema de gestión como registros de calidad, existen controles mecanizados y numerado para cada documento siento este único, por medio de códigos correlativos, a la vez hay diferentes puntos de control en todo el proceso de recursos Humanos, la Jefe de la unidad es la responsable de la información así como también los analistas y archivadores de la misma, existen firmas y permisos delimitados para su control, el control de hace de manera continua en el proceso y los beneficios son generar eficiencia, optimización de tiempos, confidencialidad en las mismo y seguridad de la misma
Recientemente un grupo de ex trabajadores llegaron a solicitar información para poder efectuar tramites de la pensión del INPEP, dichas personas solicitaron el historial de su trabajo en la comisión y se encontraron con que la Unidad encargada había Perdido dichos archivos, ya que por su antigüedad los archivos de microfilm se habían dañado por el mal resguardo de los discos. CEL tuvo que comprar una nueva máquina para leer microfilm y así poder leer dichos discos en mal estado, ya que la actual maquina no era lo suficientemente potente. CEL gasto alrededor de $15,000 en la nueva máquina de microfilm y $8,000 en la remodelación del área de resguardo de dichos discos y así evitar que se siguieran dañando por falta de controles.

Del principio de integridad se encontró:
Cada empleado es responsable de la información que el produce, la Jefa de la Unidad autoriza y define las responsabilidades de la información, tanto de manera física como electrónica, en el manual se establecen las responsabilidades sobre qué información pueden manejar cada uno de ellos, a la vez que se delimita en sus funciones del puesto, solamente se tiene autorizado hacer actualizaciones y modificaciones menores, la forma de garantizar la información es por medio de firmas y autorizaciones, a la vez existe una normativa para almacenar los expedientes, en ocasiones se delegan a personas pero es poco común, el mismo personal es quien transporta los documentos, los impactos al atentar contra la integridad son mal uso de datos, amonestaciones y acciones al personal.

Del principio de autenticidad se encontró:
Existen filtros para garantizar la veracidad al igual que se verifican con respaldos. Dicha verificación se hace como parte del procedimiento y como autocontrol, los impactos que genera información no real son: se pierde legalidad de documentos, penalizaciones al personal. Hay pocos controles para ello y pueden no hay criterios para establecer la autenticidad, todo es de forma empírica y por la experiencia.

Del principio de disponibilidad se encontró:
La información se encuentra disponible como parte del flujo de proceso o como solicitud ya sea de la misma o de otra unidad, la información no siempre se dispone de forma inmediata, hay casos en los que no llega con los tiempos oportunos, a pesar de ellos la información se encuentra disponible, Existen atrasos en su acceso debido a fuerzas externas por ejemplo las planillas o procesos de declaración de renta, cuando alguna información no está disponible se acostumbra a utilizar notas señalando que aun no está disponible dicho documento.
El año pasado se realizo la contratación de nuevo personal en CEL, dicho proceso fue lento y ocasiono que la plaza fuera cubierta con retrasos, al momento de que la persona tomo cargo desconocía algunos términos y formas de cómo realizar su trabajo, las capacitaciones no fueron hechas en su debido tiempo debido a una mala programación de las mismas pues la información de los capacitadores se extravió y tomo varios días localizarlos. En cuanto a costos dichos atrasos y el hecho que la persona realizo mal cálculo del presupuesto del personal CEL cerró con un saldo negativo de $ 12,000 los gastos de de la Unidad de Recursos Humanos

Del principio de utilidad se encontró:
La información se obtiene por medio de solicitudes y como parte del flujo del proceso, el volumen de información demandada no se tiene definido y se encuentra en diferentes puntos almacenada, no se posee un archivo institucional, al revisarla es cuando se determina la utilidad o no, regularmente el 100% es la que se utiliza y de manera diaria. Los impactos al no usar de manera correcta la información pueden ser, no proveer del servicio a la comisión, reclamos, perjuicios hacia algún empleado, incumplimiento de derechos.

Del principio de confidencialidad se encontró:
Efectivamente si se maneja información confidencial, el 90% de la información procesada es confidencial pues es referente a cada trabajador, el acceso es solo para el personal de la unidad y personas de alta gerencia, la forma de trasportar la información es por medio de sobres sellados, existe posibilidad de que personal fugue información a pesar de que cada productor de la misma es el responsable, esto ya que no se tiene definidas políticas ni reglamento de confidencialidad, los impactos al revelar información de este tipo pueden ser amonestaciones, despidos, malos entendidos, señalamientos, en general para todo el volumen de información la confidencialidad de la misma es poca.

Paso 10: PRESENTACION DE LOS RESULTADO DEL DIAGNOSTICO

7. **Diagnostico del manejo y seguridad de la información dentro de la Comisión**

CUMPLIMIENTO DE LOS REQUISITOS DE LA NORMA ISO 27000 POR PROCESO

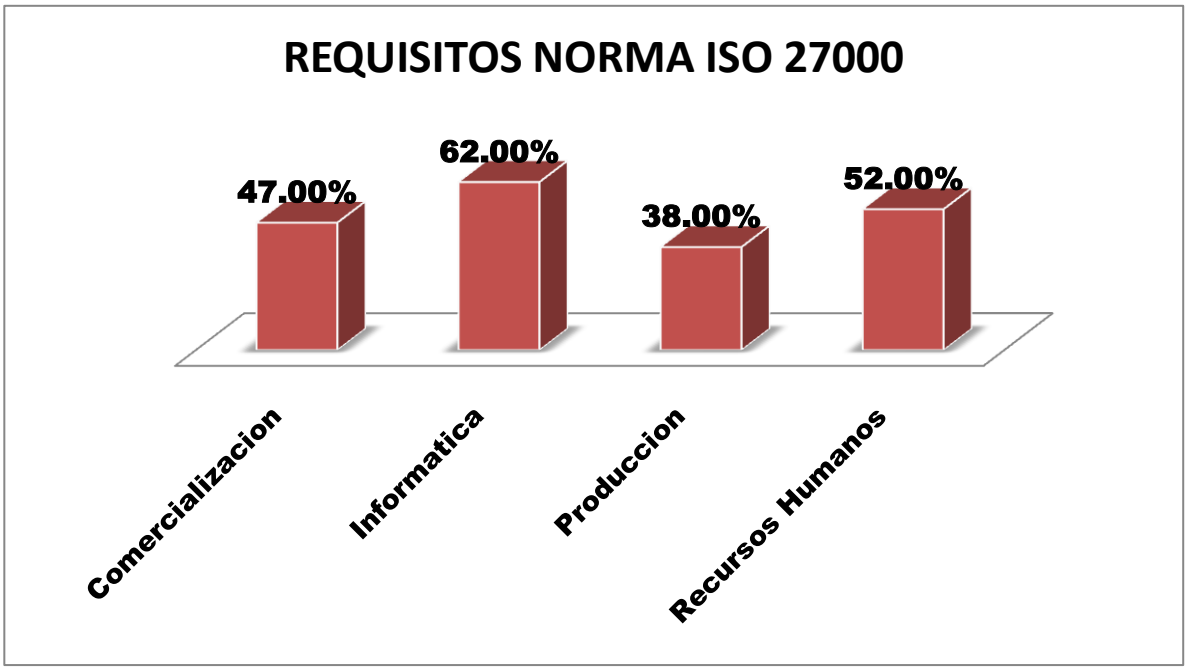


Grafico 5: Cumplimiento de los requisitos de la norma ISO 2700 por procesos

Del grafico 5 podemos observar que el proceso de informatica es el que cuenta con un promedio porcentual aprobado arriba del 62% con relacion a los requisitos de la norma ISO 27001, seguido por los procesos de RRHH con un 52%, comercializacion con un 47% y produccion en un 38%, es relevante señalar que son los dos procesos claves de la Comisión (Producción y Comercialización) los que presentan los niveles mas bajos en cuanto al cumplimiento de los requisito planteados por la Norma ISO 27001, ya que ni siquiera llegan al 50%, es decir, en estos procesos claves se observan importantes vulneravilidades a la información que como se observara en el análisis de impactos, se generan cuantiosas perdidas económicas para la Comisión.; estas perdidas economicas se presentas mas adelante en un gráfico comparativo del año 2007 y 2008.

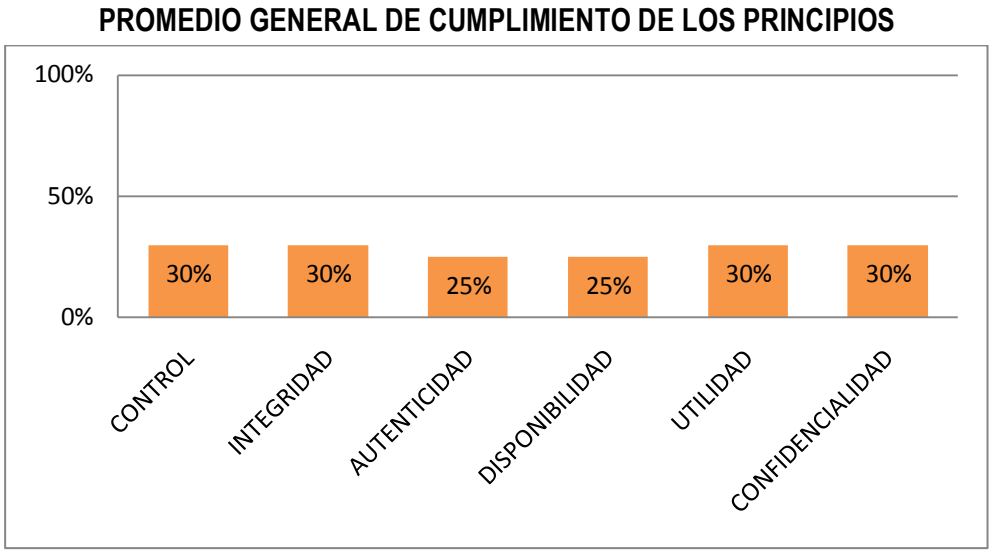


Grafico 6: Promedio general de cumplimiento de los principios de seguridad de informacion.

Desde la lectura del grafico 6 se puede concluir que: al someter los principios básicos de la norma ISO 27000 a la evaluación, se obtuvo que en su totalidad se han visto evaluados por debajo de la media de cumplimiento, con un repunte de los principios de control, integridad, utilidad, confidencialidad en 30%, y los principios de autenticidad y disponibilidad están a un 25% de su máxima calificación, en importante aclarar que el 30% que refleja en principio de control es mas producto de aplicación de acciones de control y seguridad que de controles sistematizados; por tanto CEL no cumple con los principios fundamentales de la seguridad de la información, lo cual genera perdida en la garantía de seguridad del flujo de la información .

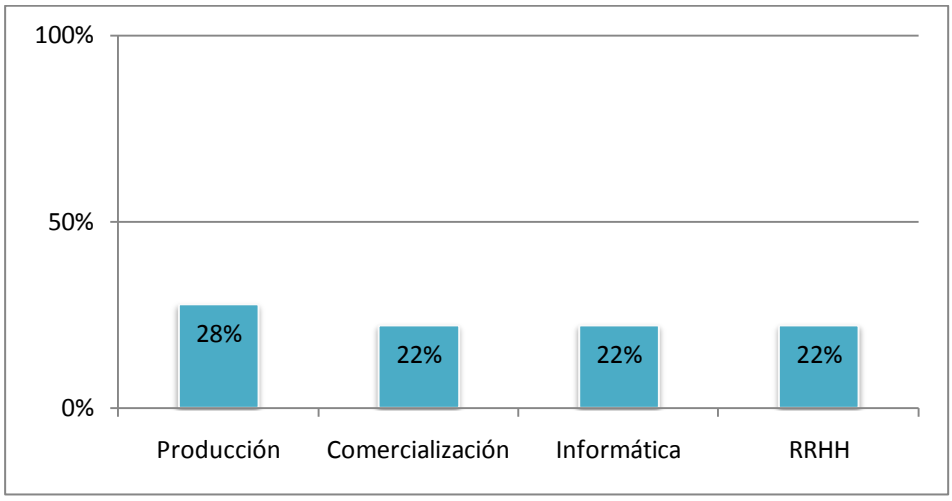


Grafico 7: Promedio general de Cumplimiento de principios de seguridad de informacion por cada departamento

Analizando el grafico 7 encontramos que la Unidad de Producción es la que cumple con el 28% de los principios de la Norma, pero al iguak que las demas unidades están muy por debajo de niveles aceptable de cumplimiento de principios; en terminos generales ninguna de las unidades cumple nisiequierra en promedio, (50%), la aplicabilidad de los principios, esto evidencia muy pocos esfuerfos por parte de la Comisión en virtud de mejorar la seguridad de la información, propiciando un escenario fragil en vulnerabilidades, con claras limitaciones en seguridad de la información frente a las amenazas que vilonetan y ponen en riesgo la eficiencia de los procesos claves y de apoyo vitales para la estrategia del negocio de CEL.

8. Impacto económico ocasionado a CEL

Total de impacto económico:

AÑO	GASTOS / PERDIDAS	PORCENTAJE
2007	$ 157,500	9.6 %
2008	$ 1,479,000	90.4 %
Total	**$ 1,636,500**	**100 %**

Tabla 28: Pérdidas económicas 2007-2008.

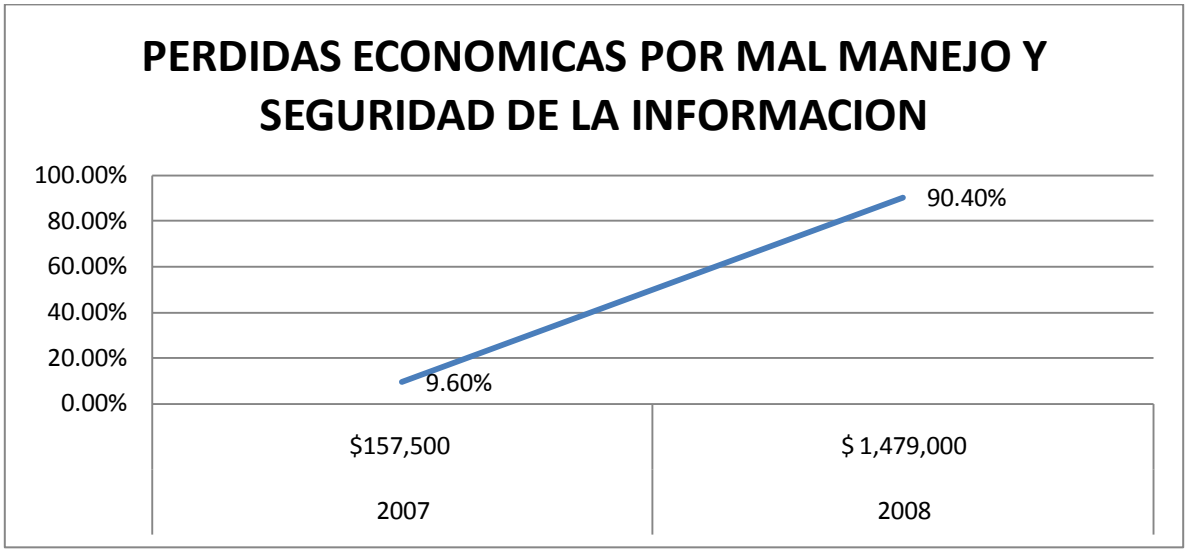


Grafico 8: Perdidas econimicas por mal manejo de la seguridad de la informacion.

Del cuadro anterior se puede ver un incremento significativo en gastos incurridos por un mal manejo y seguridad de la información, se incremento la tasa en 10 veces con respeto al año anterior, lo cual es alarmante; por lo que se evidencia la necesidad de una alternativa de solución capaz de disminuir generada en la Comisión.

Tomando en cuenta lo expuesto anteriormente en lo que respecta a los principios, requisitos e impactos generados, se genera una problemática en la cual se encuentra agrupadas todos estos resultados de la investigación

B. ENUNCIADO DEL PROBLEMA

"Existe información que se genera y manipula en La Comisión a través de sus procesos claves y de apoyo, la cual es de gran valor tanto para sus clientes como para su propio funcionamiento, que se encuentra en riesgo de ser atacado por una amenaza, potencializando las vulnerabilidades existentes, así mismo carece de los métodos adecuados de registro, flujo y resguardo de la información, generando costos de aproximadamente $ 1, 636,500 entre los años 2007 y 2008."

C. SELECCIÓN DE ALTERNATIVA DE SOLUCIÓN

1. Evaluación de las alternativas de solución propuestas.

CRITERIOS DE EVALUACIÓN:

- Costos de implantación
- Alcance del sistema
- Aplicabilidad
- Facilidad de aplicación
- Tiempos de implantación
- Adaptación al contexto

La evaluación se basa en los criterios anteriormente definidos, a continuación se presentan las posibles soluciones:

- ✓ **Alternativa 1:**

Sistema de Gestión del Manejo y Seguridad de la información bajo las normas internacionales ISO 27000[16]

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Empresas certificadas bajo la norma ISO 27000[17]

A Junio de 2009 las empresas que se certifican bajo la métrica ISO 27000 son más y más, el siguiente cuadro muestra la cantidad de empresas certificadas por país mundialmente:

[16] Ver Anexo 12 Enfoque basado en procesos y el ciclo PHVA aplicados al SGSI

[17] Fuente: http://www.iso27001certificates.com/

Esta información puede obtenerse mes a mes de forma detallada por países y empresas en International register of ISMS certificates.

Japan	3273	France	12	Peru	3
India	477	Netherlands	12	Vietnam	3
UK	401	Saudi Arabia	12	Belgium	2
Taiwan	331	Pakistan	11	Isle of Man	2
China	205	Singapore	11	Kazakhstan	2
Germany	120	Norway	10	Morocco	2
Korea	102	Russian Federation	10	Portugal	2
USA	95	Slovenia	10	Ukraine	2
Czech Republic	82	Sweden	9	Argentina	1
Hungary	65	Slovakia	8	Armenia	1
Italy	57	Bahrain	6	Bangladesh	1
Poland	40	Indonesia	6	Belarus	1
Spain	37	Kuwait	6	Bosnia Herzegovina	1
Austria	31	Switzerland	6	Denmark	1
Hong Kong	31	Canada	5	Kyrgyzstan	1
Australia	29	Colombia	5	Lebanon	1
Ireland	29	Croatia	5	Lithuania	1
Mexico	28	South Africa	5	Luxembourg	1
Malaysia	26	Sri Lanka	5	Macedonia	1
Brazil	23	Bulgaria	4	Mauritius	1
Greece	22	Qatar	4	Moldova	1
Turkey	21	Chile	3	New Zealand	1
Thailand	20	Egypt	3	Sudan	1
UAE	18	Gibraltar	3	Uruguay	1
Romania	16	Iran	3	Venezuela	1
Philippines	15	Macau	3	Yemen	1
Iceland	13	Oman	3	**Total**	**5823**

Tabla 29: cantidad de empresas certificadas mundialmente bajo la ISO 27000.

Algunos ejemplos de empresas reconocidas en Latinoamérica certificadas bajo ISO 27000 son:

- Primer Banco del Istmo S.A. BANISTMO
- PEDEVESA (Venezuela)

✓ **Alternativa 2:**

COSO-Enterprise Risk Management/SOX

El Committee of Sponsoring Organizations of Treadway Commission (COSO) es una iniciativa del sector privado estadounidense formada en 1985. Su objetivo principal es identificar los factores que causan informes financieros fraudulentos y hacer recomendaciones para reducir su incidencia. COSO ha establecido una definición común de controles internos, normas y criterios contra los cuales las empresas y organizaciones pueden evaluar sus sistemas de control.

El COSO Enterprise Risk Management – Integrated Framework COSO Enterprise Risk Management - Integrated Framework está diseñado para proporcionar las mejores prácticas de orientación para la gestión de empresas y otras para mejorar la forma en que se ocupan de estos problemas.
Integra varios conceptos de manejo de riesgo en un marco común se ha establecido, los componentes son identificados, y los principales conceptos

Esto permite proporcionar un punto de partida para las organizaciones a evaluar y mejorar su gestión de riesgos empresariales

- ✓ **Alternativa 3:**

ITIL
Information Technology Infraestructure Library, ITIL por sus siglas en inglés es un compendio de libros para la gestión de los servicios de Tecnologías de la Información, TI.
La ***Biblioteca de Infraestructura de Tecnologías de Información*** es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI).

Desarrollada a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (**ITIL**) se ha convertido en el estándar mundial de de facto en la Gestión de Servicios Informáticos. Iniciado como una guía para el gobierno de UK, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, **ITIL** es conocido y utilizado mundialmente. Pertenece a la OGC, pero es de libre utilización.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones.

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70-80% del total del tiempo y del coste, y el resto se invierte en el desarrollo del producto (u obtención). De esta manera, los procesos eficaces y eficientes de la Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI. Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada, con servicios TI centralizados o descentralizados, con servicios TI internos o suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de coste aceptable.

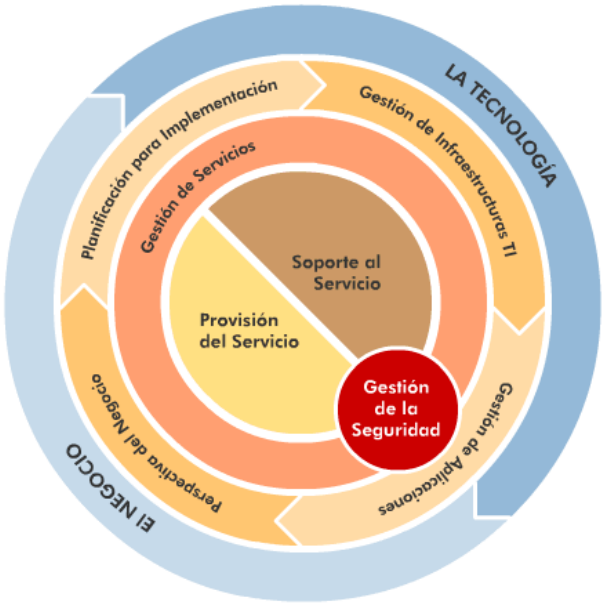


Figura 21: Metodología de funcionamiento del ITIL

ITIL fue producido originalmente a finales de 1980 y constaba de 10 libros centrales cubriendo las dos principales áreas de Soporte del Servicio y Prestación del Servicio. Estos libros centrales fueron más tarde soportados por 30 libros complementarios que cubrían una numerosa variedad de temas, desde el cableado hasta la gestión de la continuidad del negocio.. En esta revisión, **ITIL** ha sido reestructurado para hacer más simple el acceder a la información necesaria para administrar sus servicios. Los libros centrales se han agrupado en dos, cubriendo las áreas de Soporte del Servicio y Prestación del Servicio, en aras de eliminar la duplicidad y mejorar la navegación.

Criterios de evaluación	Alternativa 1 ISO 27000	Alternativa 2 COSO-	Alternativa 3 ITIL
Costos de implantación menor			X
Costo de operación menor	X		X
Menor costo por requerimiento de personal		X	
Mejor beneficio/costo			X
Amplio Alcance del sistema	X	X	
Facilidad de ejecución	X		
Mayor porcentaje de cumplimiento de objetivos	X	X	
Amplia aplicabilidad en los procesos	X	X	
Mejor aprovechamiento de los recursos		X	

Criterios de evaluación	Alternativa 1 ISO 27000	Alternativa 2 COSO-	Alternativa 3 ITIL
Tiempos de implantación mínimos	X		X
Facilidad para auditar	X		
Respaldo internacional	X	X	X
Adaptación con otros sistemas	X		X
TOTAL	**9**	**6**	**6**

Tabla 30: Evaluación de alternativas de solución.

2. Justificación de la solución seleccionada.

De acuerdo con la evaluación anterior la solución que cuenta con la aprobación de los criterios es la alternativa 1 **(Sistema de Gestión del Manejo y Seguridad de la información bajo las normas internacionales ISO 27000)**, por lo que dicha alternativa es viable en concordancia con la situación problemática encontrada en la comisión. Cabe mencionar que uno de los elementos por medio del cual esta solución se vuelve viable, es que La Comisión cuenta con un Sistema de Gestión Integrada basado en la familia de las normas ISO, por ende se cuenta con una plataforma de acción para la implementación de dicha solución.
Dentro de los productos o beneficios que dicha alternativa de solución nos ofrece y marca la diferencia con las otras alternativas de solución y tenemos:

Productos del SGSI basado en la noma ISO 27001.

- Manual de Seguridad de la Información.
- Metodología para la Continuidad y contingencia del negocio.
- Formularios
- Procedimiento para la preparación de documentos del SGSI
- Procedimiento para el control de documentos del SGSI
- Procedimiento para la Preparación de Fichas de Proceso de Seguridad y Seguimiento de Puntos de Control
- Procedimiento para el mantenimiento de requisitos de seguridad de la información de documentos del SGSI
- Procedimiento de planificación de auditorías internas del SGSI
- Procedimiento para acciones preventivas y correctivas del SGSI
- Procedimiento de Gestión de Debilidades, Incidentes, Problemas y Violaciones de Seguridad de la Información
- Procedimiento para la Revisión del SGSI por la Dirección
- Procedimiento para la clasificación y marcado de la información del SGSI

Beneficios esperados:

De manera Cuantitativa tenemos:

- Reducción en un 80% de 58 de reclamos por perdidas de información (datos obtenidos de UGI según bitácora de RC)
- Menor Tiempo de respuesta para reportar Gestionar incidentes o perdidas de la seguridad de la información
- Reducción de un 85% de pérdidas económicas por incidentes o problemas con la seguridad de la información aproximadamente de $ 1, 636,500.

Entre los otros **beneficios tangibles como intangibles** aportados por un SGSI destacamos los siguientes:

- Documentos normados en base a la norma ISO 27000
- Procedimientos documentados y diagramados con el plus de aseguramiento de la información.
- Aseguramiento de los activos de información
- Personal adiestrado y capacitado en materia de seguridad de la información.
- Desde el punto de vista organizacional, permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización en todos sus niveles y probar la diligencia de sus administradores.
- Permite demostrar el cumplimiento de las leyes y normativas legales.
- Garantiza la implantación de medidas de seguridad consistente, eficiente y apropiada al valor de la información protegida.
- Contempla planes de contingencia ante cualquier tipo de incidencia (pérdidas de datos, incendio, robo, terrorismo, etc.)
- Transmite credibilidad y confianza ante clientes, socios e inversores.
- Puede ser utilizada como herramienta de diferenciación frente a la competencia.
- Mejora la concienciación del personal en todo lo que se refiere a la seguridad y a sus responsabilidades dentro de la organización.
- Elaboración de una estrategia de la organización en conjunto que implique a la dirección.

D. CONCEPTUALIZACIÓN DEL DISEÑO

1. Descripción de la norma ISO 27001

La Seguridad de la Información es el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso, con el fin de minimizar las amenazas y riesgos continuos a los que está expuesta, a efectos de asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de inversiones y las oportunidades del negocio. Y en el caso de cada individuo de proteger la identidad y la privacidad

El estándar para la seguridad de la información **ISO/IEC 27001** especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming"; el cual es una estrategia de mejora continua de la calidad en cuatro pasos.[18]

Planear (Establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (Implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.
Verificar (Monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Tabla 31: Ciclo PHVA basado en ISO 27000.

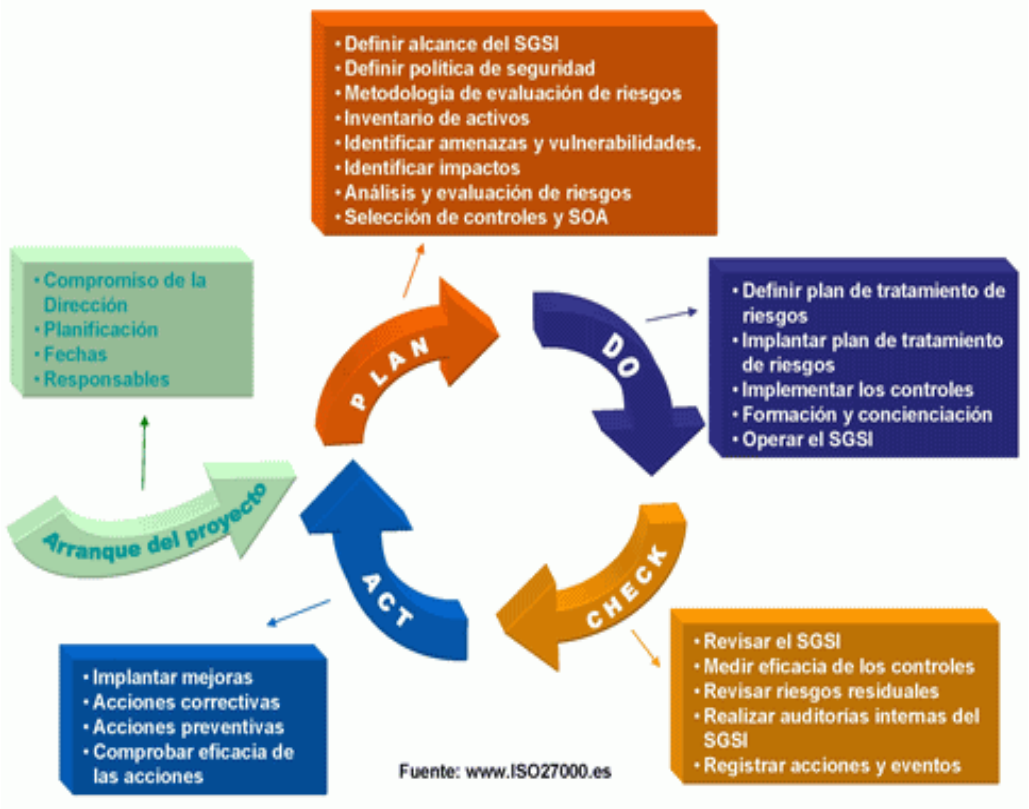


Figura 22: Ciclo PHVA basado en la norma ISO 27000.

[18] Ver Anexo 12 Enfoque basado en procesos y el ciclo PHVA aplicados al SGSI

PROPÓSITO DEL SISTEMA GESTIÓN PARA EL MANEJO Y SEGURIDAD DE LA INFORMACIÓN

El propósito del SGSI será garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.
Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

2. Componentes a realizar al aplicar la norma

La estructura que se pretende diseñar es la siguiente:
La norma ISO 27000, a través del SGSI establece once dominios estructurales[19] que cubren por completo la Gestión de la Seguridad de la Información:
Todo inicia con la ***elaboración de una estrategia de la organización*** en conjunto que implique a la dirección.

Luego se determinan:

1. El alcance del SGSI;
2. Política y objetivo de seguridad;
3. Manual de seguridad;
4. Procedimientos y mecanismos de control que soportan el SGSI
5. Metodología de evaluación de riesgos;
6. Informe de evaluación de riesgos;
7. Plan de tratamiento del riesgo;
8. Procedimientos documentados;
9. Registros requeridos por este Estándar Internacional;
10. La declaración de aplicabilidad.
11. Instructivos, checklists y formularios.

[19] Estos dominios se ilustran en el *ciclo PHVA* correspondiente a la aplicación del SGSI, y se especifica la elaboración de los mismos.

Modelo de Seguridad de la Información

Figura 23: Pirámide de productos de la norma ISO 27000.

Áreas que se deben cubrir con ISO 27000 en los procesos claves y de apoyo

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.
9. Gestión de continuidad del negocio.
10. Conformidad con la legislación.

CAPÍTULO IV: DISEÑO DEL SGSI

A. ESTABLECIMIENTO DEL SISTEMA DE GESTIÓN PARA EL MANEJO Y SEGURIDAD DE LA INFORMACIÓN

1. Establecimiento del Alcance del SGSI

Ya se ha planteado anteriormente que la razón principal de la Comisión en función de sus características del negocio son la producción y comercialización de energía hidroeléctrica, así como también se establece que de acuerdo a las certificaciones anteriores relacionadas con ISO se determino que los procesos claves de la Comisión son: producción y comercialización, así también se establecen sus procesos de apoyo como lo son informática y recursos humanos. Por lo mencionado anteriormente el sistema operara en los procesos claves de la institución y sus procesos de apoyo.

Los procesos claves y de apoyo se desarrollan en las instalaciones centrales de la Comisión ubicadas en el centro de gobierno y es por eso que el sistema gestionara los activos desde esta ubicación.

En cuanto al alcance del sistema en función de los usuarios de la información, el SGSI tendrá impacto en los usuarios internos de los activos en los niveles operativos, usuarios de reportes relacionados con los mandos medios y usuarios de indicadores generales como la alta gerencia; los usuarios de los activos generados por la Comisión también se ven afectados, estos usuarios son la Unidad de transacciones eléctrica y AESS (Asociación de Eléctricas Salvadoreña).

Para mayor explicación del alcance del sistema de seguridad de la información ver el siguiente cuadro

- **Relación entre procesos claves, procesos de apoyo y entidades externas.**

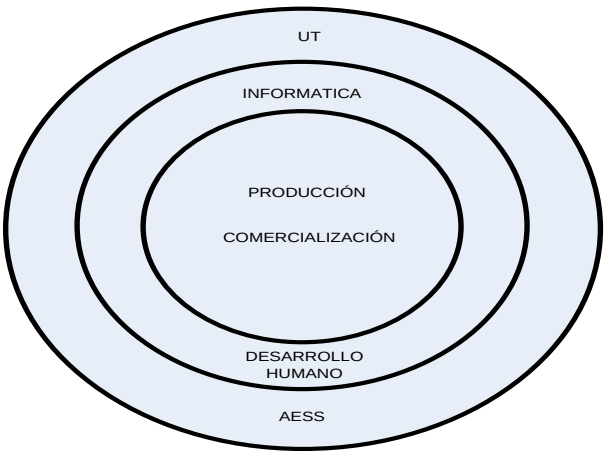


Figura 24: Alcance del SGSI.

En la Figura 44 de la pagina 272 se muestra la metodología diseñada para la operación del SGSI, en ella se presenta para cada una de las fases de la metodología la pagina correspondiente para documentar o ampliar cada fase.

2. Definición de las políticas y objetivos de seguridad de la información.

a) Objetivos de Seguridad:

a. Contar con un Sistema de Gestión de Seguridad de la Información, con la finalidad de mitigar los riesgos operativos y de tecnología de información para el tercer trimestre del 2009.

b. Fortalecer la cultura de administración del riesgo en función de los valores éticos y morales respecto a la seguridad de la información.

c. Fomentar con los colaboradores la responsabilidad del manejo de la seguridad de la información, desde la perspectiva de la confiabilidad, integridad y la disponibilidad de la misma.

d. Obtener la certificación bajo la Norma ISO 27001:2005 en el periodo de un año después de implementado y operado el SGSI

b) Políticas de Seguridad de la Información

- **OBJETIVO**

Gestionar a través de procedimientos, normas y herramientas la seguridad de la información, con el propósito de garantizar un nivel de riesgo aceptable ante las posibles amenazas asociadas a esta.

- **POLÍTICAS ESPECÍFICAS**

1. CEL contará con la estructura organizativa adecuada, para la gestión de la seguridad de la información, asegurando que se proveerán los recursos necesarios.
2. Los Jefes de las Unidades de de Producción, Comercialización, Gestión de la Información y Desarrollo Humano mantendrán responsabilidades definidas en cuanto a la gestión de los activos relacionados a los sistemas de información y a la clasificación de la información.
3. Los Jefes de las Unidades de de Producción, Comercialización, Gestión de la Información y Desarrollo Humano mantendrán los controles necesarios respecto al personal, relacionados a su acto contractual, Formación, respuesta a incidentes y desarrollo de sus actividades laborales en cuanto a seguridad de la Información se refiere.
4. La Unidad de Gestión Integrada establecerá los controles físicos y ambientales adecuados para asegurar los activos que alberguen información crítica de La Comisión
5. La Unidad de Gestión Integrada mantendrá los controles necesarios para lograr que las comunicaciones y operaciones de La Comisión, relacionadas con la información, cumplan con los requisitos definidos de seguridad.
6. La Unidad de Gestión Integrada mantendrá las normas, responsabilidades y lineamientos necesarios para controlar el acceso a la información de La comisión.
7. La Unidad de Gestión Integrada mantendrá los requisitos y controles necesarios de Seguridad relativos a la adquisición, desarrollo y mantenimiento de sistemas de información.

8. Los Jefes de las Unidades de de Producción, Comercialización, Gestión de la Información y Desarrollo Humano establecerán las responsabilidades, requisitos y canales de comunicación adecuados para la gestión de incidentes relacionados a la seguridad de la información.
9. Los Jefes de las Unidades de de Producción, Comercialización, Gestión de la Información y Desarrollo Humano realizarán todas las acciones y planes necesarios que garanticen una reacción adecuada y oportuna ante la interrupción de las actividades de La Comisión y proteger todos sus procesos críticos frente a grandes fallos por desastres.
10. Los Jefes de las Unidades de de Producción, Comercialización, Gestión de la Información y Desarrollo Humano mantendrán los controles necesarios para evitar los incumplimientos de cualquier ley civil o penal, requisitos reglamentarios, regulaciones u obligaciones contractuales y de todo requisito de seguridad.
11. Los Jefes de las Unidades de de Producción, Comercialización, Gestión de la Información y Desarrollo Humano velarán por la Seguridad de la Información, a través del cumplimiento de lo establecido en los documentos del Sistema de Gestión de Seguridad de la Información (SGSI).

3. Determinación del enfoque de gestión de riesgos.

El enfoque y la filosofía para el riesgo están determinando de manera muy precisa por el ISO 27001:2005. En la clausula 4.2.1 (c) se requiere que la organización identifique y adopte un método y un enfoque sistemático para el calculo del riesgo de sus activos de información.

Es importante que la información de seguridad se gestione con transparencia y conciencia a través de la organización. La gestión de los riesgos puede utilizar distintos enfoques gerenciales y métodos de cálculo que satisfagan las necesidades de la organización. La organización (CEL) decidirá que método de cálculo de riesgo se escoger. No importa el método que decida la organización, pero debe cerciorarse de que el enfoque es el adecuado y apropiado para atender los requerimientos organizacionales, legales o regulatorios.

En la clausula 4.2.1 (c) el ISO 27001:2005 establece el marco conceptual para escoger el enfoque para hacer el cálculo del riesgo, describiendo los elementos obligatorios que el proceso del cálculo del riesgo debe contener. Los elementos obligatorios a tener en cuenta son:

1. Determinación del criterio para la aceptación del riesgo. Se deben documentar las circunstancias bajo las cuales la organización está dispuesta a aceptar los riesgos
2. Identificación de los niveles aceptables del riesgo. Al margen del tipo de enfoque que se utilice para el cálculo del riesgo, deben estar identificados los niveles de riesgo que la organización considera aceptables.
3. Cobertura de todos los aspectos del alcance del SGSI. El enfoque escogido debe de completar un análisis de todos los controles y objetivos de control
4. El cálculo del riesgo debe lograr un claro entendimiento sobre los factores que deben de controlarse, en la medida en que estos factores afecten sistemas y procesos que sean críticos para la organización. Una eficaz gestión del riesgo significa un buen balance entre el gasto en recursos contra el deseado grado de protección, y asegurando que los recursos gastados sean correlacionados con la potencial perdida y el valor de los activos protegidos.

El enfoque que la empresa escoja y su nivel de detalle y complejidad influencian el esfuerzo y los recursos requeridos durante el proceso del cálculo del riesgo. El cálculo del riesgo debe ser tan detallado y complejo como sea necesario, para así poder atender todos los requerimientos de la organización y lo que se requiera por el alcance del SGSI, El exceso de detalles puede determinar un exceso de trabajo, y un enfoque muy genérico puede conducir a subestimar aspectos de riesgos importantes.
El ISO 27001:2005 no exige un enfoque extremadamente detallado o técnico, en la medida en que todos los riesgos estén apropiadamente atendidos por la metodología utilizada. A continuación de detalla todo la metodología aplicada en CEL

4. **Gestión de debilidades, incidentes, problemas y violaciones a la seguridad de la información**

a) Responsabilidades y funciones del personal involucrado

Es responsabilidad de los Titulares o quién delegue:
Emitir lineamientos y autorizar los recursos cuando sea necesario, con el fin de reducir los impactos ocasionados por los incidentes, problemas y violaciones a la seguridad de la información con base al informe anual de incidentes, problemas y violaciones a la seguridad de la información o cuando se detecten incidentes de seguridad producidos de forma deliberada por empleados de La Comisión o terceros.

Es responsabilidad de la Unidad de Gestión Integrada:

- Tomar las acciones correctivas cuando le sean notificados:
  a. Incidentes o debilidades de seguridad en los sistemas de información.
  b. Infracciones, problemas de seguridad informática, daños, pérdidas y mal funcionamiento de hardware, software.
  c. Condiciones que pudieran llevar a una interrupción de las actividades del negocio.
  d. Divulgación de la información confidencial o sensible y de uso interno.
  e. Alertas y advertencias de vulnerabilidades relacionadas a personas no autorizadas, incluyendo: la pérdida o cambios en los datos de producción y el uso cuestionable de archivos, bases de datos o redes de comunicación.
  f. Solicitudes inusuales de información efectuadas por personas externas.
  g. Conducta atípica del sistema.
  h. Fallas o indisponibilidad de los controles que aseguran la integridad de la información.
- Autorizar el acceso a la información de los sistemas informáticos.
- Actuar y aplicar lo establecido en las disposiciones legales y técnicas vigentes, según corresponda cuando se detecten incidentes de seguridad producidos de forma deliberada por empleados de La Comisión o terceros.
- Elaborar, revisar, aprobar y mantener un proceso de gestión de incidentes y problemas de seguridad de la información, el cual debe contar con la tipificación de incidentes y niveles de impacto de los Tipos e Impactos de Incidentes de Seguridad (descritos en la evaluación del riesgo)
- Revisar mensualmente los informes de incidentes y problemas de seguridad, resultado de dicho proceso de gestión, elaborado por los Encargados de Seguridad de la Información.
- Tomar en cuenta las acciones preventivas o correctivas que provengan del análisis de incidentes para incorporarlas al plan de seguridad o plan de calidad.

- Hacer de uso oficial en su dependencia para la atención, análisis y registro de incidentes de seguridad y sus respectivas soluciones, la herramienta de "SIG".
- Asegurar la disponibilidad del SIG.
- Brindar apoyo para el uso, la instalación, el acceso y la operación del SIG en las dependencias de La Comisión.

Es responsabilidad de la Dirección Ejecutiva

- Aprobar y remitir a los Titulares el informe anual de incidentes, problemas y violaciones a la seguridad de la información
- Comunicar al encargado de La Unidad de Gestión Integrada, las acciones correctivas o preventivas a incluir en sus Planes de Trabajo de Seguridad, atendiendo los lineamientos de los Titulares.

Es responsabilidad de los Jefes de las Unidades Organizativas:

- Gestionar el acceso y permisos a los sistemas informáticos al personal bajo responsabilidad o terceros.
- Reportar al encargado de seguridad de su dependencia, a través del SIG de la Unidad de Gestión Integrada, los problemas asociados con sistemas informáticos, que no se han abordado adecuadamente por los proyectos existentes o planificados.
- Participar en la definición las huellas de auditoría y acciones de monitoreo en los sistemas de información automatizados bajo su responsabilidad, con el fin de detectar actividades maliciosas que conlleven a una violación de la política de seguridad o divulgación de información confidencial o sensible y de uso interno.
- Solicitar inmediatamente al área o unidad de informática según corresponda, el aislamiento de la estación de trabajo y mantenerla intacta hasta que se presente el encargado de seguridad de su dependencia, cuando la misma esté involucrada en una violación o incidente de seguridad con el fin de recabar evidencia o proteger la información contenida en ella.

Es responsabilidad del Coordinador de Seguridad de la Información o a quien delegue:

- Sugerir las acciones correctivas inmediatas cuando le sean notificados:
    a. Incidentes o debilidades de seguridad en los sistemas de información.
    b. Infracciones, problemas de seguridad informática, daños, pérdidas y mal funcionamiento de hardware, software.
    c. Condiciones que pudieran llevar a una interrupción de las actividades del negocio.
    d. Divulgación de la información confidencial o sensible y de uso interno.
    e. Alertas y advertencias de vulnerabilidades relacionadas a personas no autorizadas, incluyendo: la pérdida o cambios en los datos de producción y el uso cuestionable de archivos, bases de datos o redes de comunicación.
    f. Solicitudes inusuales de información efectuadas por personas externas.
    g. Conducta atípica del sistema.
    h. Fallas o indisponibilidad de los controles que aseguran la integridad de la información.
    i. Problemas asociados con sistemas informáticos en diseño y desarrollo, que no se han abordado adecuadamente por los proyectos existentes o planificados.
- Informar al Jefe de la Unidad de Gestión Integrada, cuando La Comisión haya sido víctima de un delito de computación o comunicación, con suficientes datos para tomar acciones que prevengan o reduzcan tales incidentes.

- Elaborar el informe anual de incidentes, problemas y violaciones a la seguridad de la información y presentarlo al Jefe de la Unidad de Gestión Integrada
- Actualizar las variables del análisis de riesgo tomando como base los resultados de los informes sobre incidentes.

Es responsabilidad del Técnico de Seguridad de la Información:

- Concientizar al personal de La Comisión sobre medidas para la prevención de incidentes de seguridad de la información.
- Ejecutar las acciones que le hayan sido delegadas por el Coordinador de Seguridad de la Información.

Es responsabilidad de los Encargados de Seguridad de la Información de cada dirección y Unidad:

- Apoyar en la clasificación los incidentes de seguridad de la información recibidos a través del SIG.
- Ingresar al SIG, todos aquellos incidentes reportados por los empleados o terceros, que no hayan sido reportados por este medio (notas, correo electrónico, llamada telefónica o visita en sitio).
- Sugerir o tomar las acciones correctivas inmediatas cuando le sea notificado:
    a. Incidentes o debilidades de seguridad en los sistemas de información.
    b. Infracciones, problemas de seguridad informática, daños, pérdidas y mal funcionamiento de hardware, software.
    c. Condiciones que pudieran llevar a una interrupción de las actividades del negocio.
    d. Divulgación de la información confidencial o sensible y de uso interno.
    e. Alertas y advertencias de vulnerabilidades relacionadas a personas no autorizadas, incluyendo: la pérdida o cambios en los datos de producción y el uso cuestionable de archivos, bases de datos o redes de comunicación.
    f. Solicitudes inusuales de información efectuadas por personas externas.
    g. Conducta atípica del sistema.
    h. Fallas o indisponibilidad de los controles que aseguran la integridad de la información.
    i. Problemas asociados con sistemas informáticos en diseño y desarrollo, que no se han abordado adecuadamente por los proyectos existentes o planificados.
- Elaborar mensualmente los informes de incidentes y problemas de seguridad.
- Concientizar al personal de su dependencia sobre medidas para la prevención de incidentes de seguridad de la información.
- Incorporar los resultados de análisis de incidentes a las variables del análisis de riesgo.

Es responsabilidad de los Empleados:

- Conocer quién es el Encargado de Seguridad de la Información de su dirección o Unidad.
- Notificar al Encargado de Seguridad de la Información de su dirección o Unidad a través del SIG; nota, llamada telefónica, correo electrónico o visita en sitio, las sospechas de/o incidentes de seguridad informática, debilidades de seguridad en los sistemas de información, infracciones, problemas de seguridad informática, daños, pérdidas y mal funcionamiento de hardware, software, condiciones que pudieran llevar a una interrupción de las actividades del negocio, divulgación de la información confidencial o sensible, alertas y advertencias de vulnerabilidades; a personas no autorizadas incluyendo, sin límites, la pérdida o cambios en los datos de producción y el uso cuestionable de archivos, bases de datos o redes de comunicación, solicitudes inusuales de información efectuadas por personas externas, la conducta atípica del sistema y las fallas o indisponibilidad de los controles que aseguran la integridad de la información.

- Reportar al encargado de seguridad correspondiente a través del SIG, nota, llamada telefónica, correo electrónico o visita en sitio, todos los errores importantes, los procesamientos incompletos y los procesamientos impropios de las aplicaciones de producción.

b) Procedimiento

GESTION DE DEBILIDADES, INCIDENTES, PROBLEMAS Y VIOLACIONES DE SEGURIDAD DE LA INFORMACION

ETAPA 1: REPORTE Y GESTIÓN DE EVENTOS, INCIDENTES, VULNERABILIDADES Y PROBLEMAS DE SEGURIDAD DE LA INFORMACION

RESPONSABLE	PASO	ACCION
Empleados y Partes Externas o Terceros	01	Reporta a través del SIG todos aquellos eventos, incidentes, vulnerabilidades y problemas de seguridad de la información que descubran en sus labores cotidianas; o a través nota, llamada telefónica, correo electrónico o visita en sitio, al encargado de seguridad de su dirección o unidad
Encargado de Seguridad de la Información	02	Recibe reporte de incidente, presentándose dos casos: a) Si el incidente es recibido a través del GIG, continua con el siguiente paso. b) Si el incidente es recibido a través de nota, llamada telefónica, correo electrónico o visita en sitio; abre un requerimiento en el SIG, completando los datos necesarios, con el objetivo que este quede registrado, luego continúa con el siguiente paso.
	03	Analiza el incidente determinando: c) Si el incidente es de su competencia, continua con el paso siguiente. d) Si el incidente no es relacionado con los servicios o componentes de su dependencia o su responsabilidad, reasigna incidente a la dependencia correspondiente.
	04	Realiza lo dispuesto en su respectivo proceso de gestión de incidentes y problemas.

Tabla 32: Reporte de gestión de eventos, incidentes, vulnerabilidades y problemas de seguridad de la información.

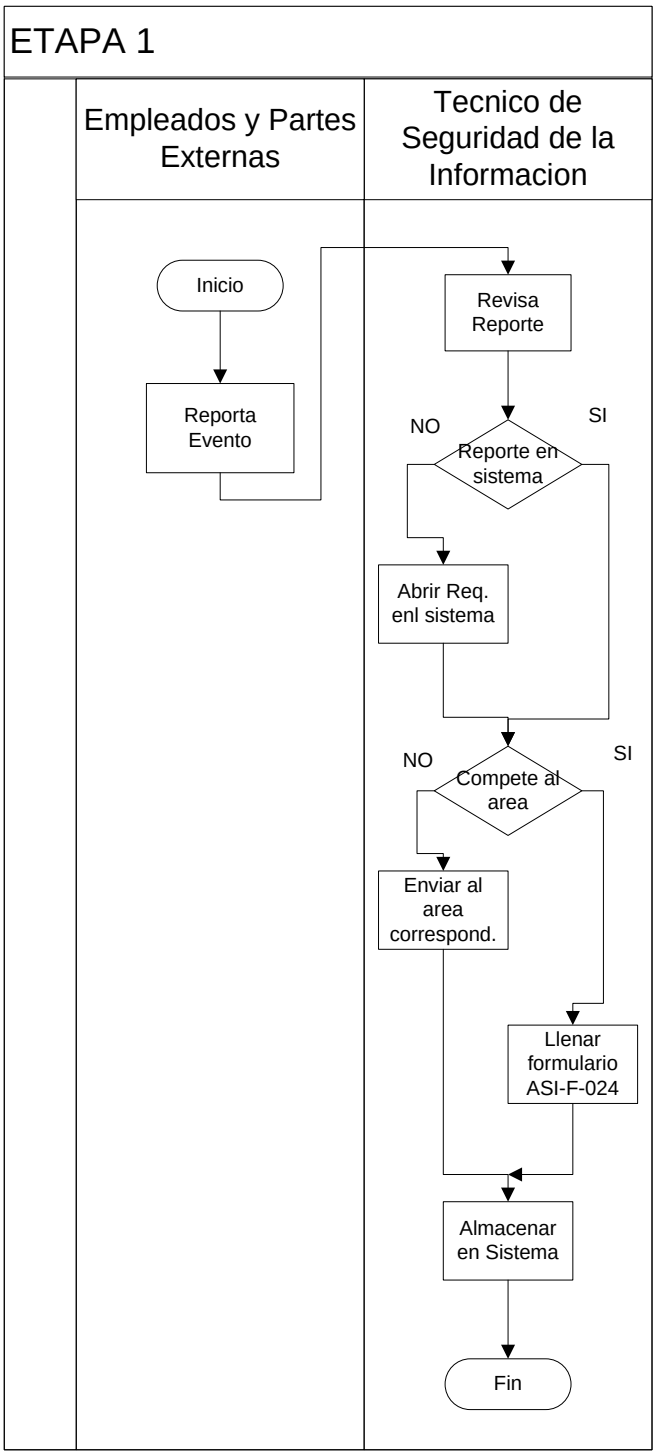


Figura 25: Diagrama de flujo para elaboración de reporte y gestión de eventos, incidentes, vulnerabilidades y problemas de seguridad de la información

ETAPA 2: ANÁLISIS Y ELABORACIÓN DE INFORME MENSUAL SOBRE GESTIÓN DE EVENTOS, INCIDENTES, VULNERABILIDADES Y PROBLEMAS DE SEGURIDAD DE LA INFORMACION

RESPONSABLE	PASO	ACCION
Encargado de Seguridad de la Información	01	Obtiene a través de las salidas del proceso de gestión de incidentes, la información necesaria para elaborar el reporte mensual de eventos, incidentes, vulnerabilidades y problemas de seguridad de la información.
	02	Elabora reporte mensual, tomando en cuenta como mínimo los requisitos del Modelo de Informe Mensual de Eventos, Incidentes, Vulnerabilidades, Problemas y Violaciones de Seguridad de la información.
	03	Envía por correo electrónico el reporte mensual a la Unidad de Gestión Integrada para su revisión.
Jefe de la Unidad de Gestión Integrada	04	Recibe el informe mensual y lo remite por correo electrónico al Encargado de Seguridad con la respectiva firma o rubrica de revisión.
Encargado de Seguridad de la Información	05	Recibe informe revisado por Jefe de la Unidad de Gestión Integrada y envía mensualmente a través de un correo electrónico y solicita por medio de un requerimiento a través del SIG, al Área de Seguridad de la Información, su publicación.
Técnico de Seguridad de la Información	06	Recibe Informe Mensual de Eventos, Incidentes, Vulnerabilidades, Problemas y Violaciones de Seguridad de la Información y realiza Publicación y Distribución

Tabla 33: Análisis y elaboración de informe mensual sobre gestión de eventos, incidentes, vulnerabilidades y problemas de seguridad de la información.

*****NOTA: Las acciones preventivas o correctivas que no puedan ser ejecutadas como parte de la gestión de operaciones de las unidades, deberán ser consideradas en los planes de seguridad (PLS) del siguiente año.

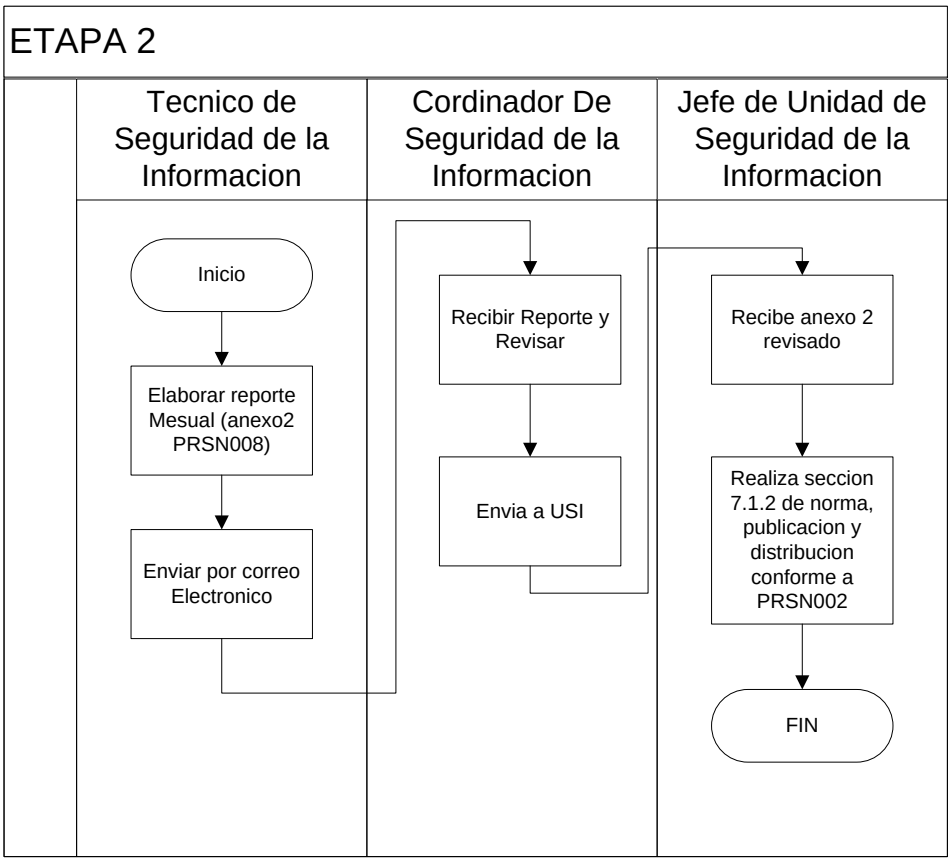


Figura 26: Diagrama de flujo para análisis y elaboración del informe mensual de reporte y gestión de eventos, incidentes, vulnerabilidades y problemas de seguridad de la información

ETAPA 3: ANÁLISIS Y ELABORACIÓN DE INFORME ANUAL SOBRE GESTIÓN DE EVENTOS, INCIDENTES, VULNERABILIDADES Y PROBLEMAS DE SEGURIDAD DE LA INFORMACION

RESPONSABLE	PASO	ACCION
Coordinador de Seguridad de la Información	01	Obtiene a través de los informes mensuales de eventos, incidentes, vulnerabilidades, problemas y violaciones de seguridad de la información, de la Unidad de Gestión Integrada; la información necesaria para elaborar el reporte anual de incidentes, problemas y violaciones de seguridad de la información.
	02	Elabora reporte anual de Análisis de Incidentes, Problemas y Violaciones de Seguridad de la Información.
	03	Envía por correo electrónico el reporte anual al Jefe de la Unidad de Gestión Integrada para su revisión.

Jefe de la Unidad de Gestión Integrada	04	Revisa el informe presentándose dos casos: a) Si no posee observaciones, continua con el siguiente paso. b) Si posee observaciones, las anexa y devuelve por correo electrónico el informe al Coordinador de Seguridad de la Información para que realice su corrección, pasando al paso 02.
	05	Envía por correo electrónico el informe a la Dirección Ejecutiva.
Dirección Ejecutiva	06	Recibe informe y lo aprueba.
	07	Envía por correo electrónico el informe a titulares para su conocimiento. Sugiriendo las acciones (correctivas y/o preventivas) y recursos necesarios para disminuir los incidentes, problemas y violaciones de seguridad de la información, en los sistemas y servicios de La Comisión.
Jefes de las Unidades Organizativas	08	Reciben informe, emiten opinión y envían por correo electrónico a la Dirección Ejecutiva
Dirección Ejecutiva	09	Recibe informe e indica según opinión de los Titulares, las acciones a ser incluidas en los planes de trabajo de las Unidades según corresponda.
	10	Devuelve por correo electrónico el informe y observaciones al Coordinador de Seguridad de la Información para su publicación.
Coordinador de Seguridad de la Información	11	Recibe informe presentándose dos casos: a) Si el informe contiene acciones (correctivas o preventivas) la UGI, las incluye el Plan de Seguridad correspondiente, y envía informe al Técnico de Seguridad de la Información para su publicación. b) Si el informe no contiene acciones (correctivas o preventivas) lo envía a Técnico de Seguridad de la Información para su publicación.
Técnico de Seguridad de la Información	12	Recibe informe y lo publica.

Tabla 34: Análisis y elaboración de informe anual sobre gestión de eventos, incidentes, vulnerabilidades y problemas de seguridad de la información.

NOTA: Para las etapa 1 de éste procedimiento, los eventos, incidentes, vulnerabilidades, problemas y violaciones de seguridad de la información, involucran la alteración de la conservación de los tres estados de la seguridad de la información, es decir: Integridad, Confidencialidad y Disponibilidad; y pueden ser descubiertas en sus labores cotidianas o por medio del monitoreo de sistemas, alertas y vulnerabilidades.

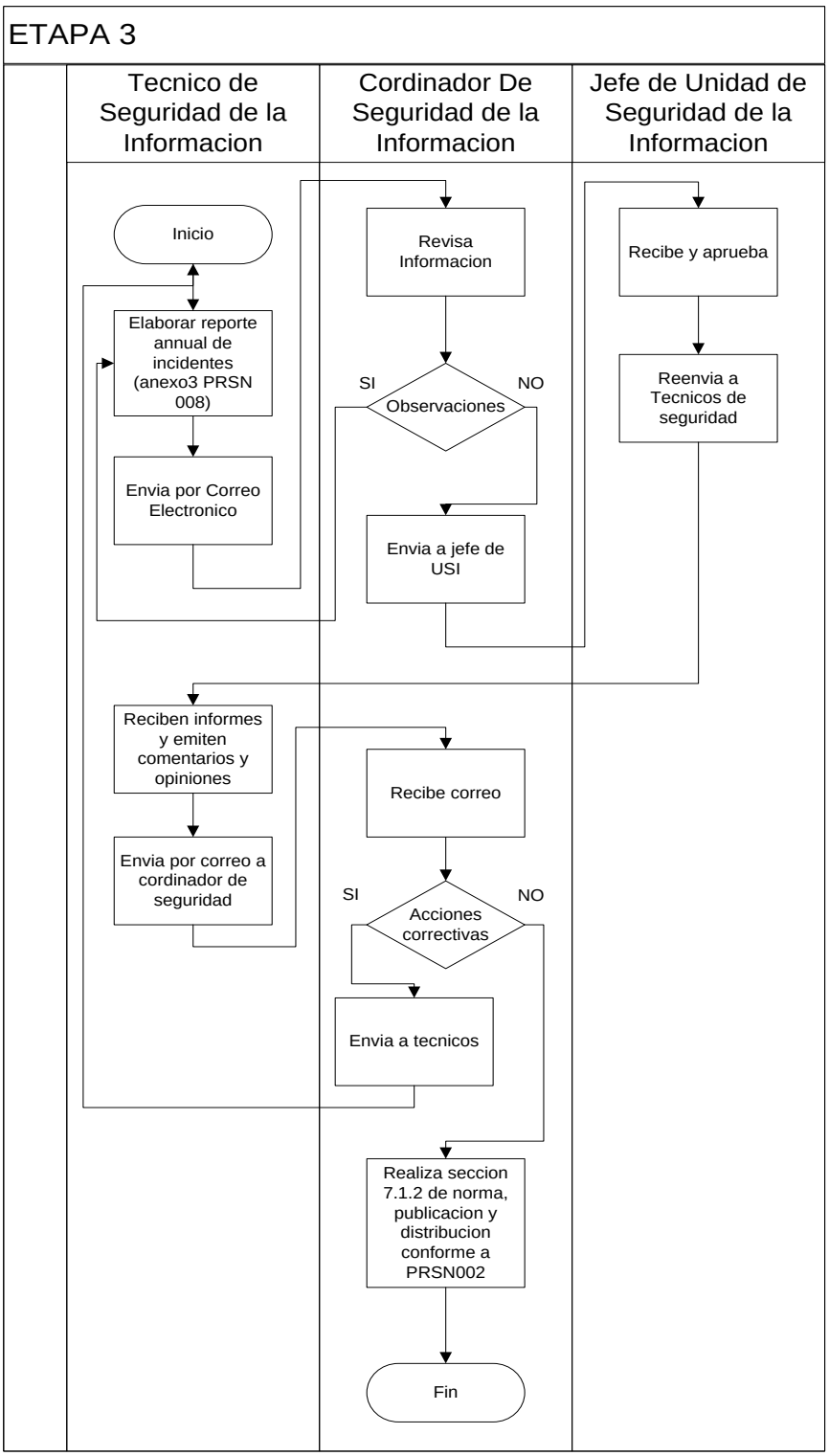


Figura 27: Diagrama de flujo para análisis y elaboración del informe anual de reporte y gestión de eventos, incidentes, vulnerabilidades y problemas de seguridad de la información

c) Información complementaria y formatos a utilizar

TIPOS E IMPACTOS DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad de la información pueden ser clasificados en los siguientes tipos:

TIPO	DETALLE
Perdida del servicio por falla en los sistemas	Ocurre cuando se interrumpe el servicio a los clientes y usuarios por falla en los diferentes componentes de los sistemas de información, como fallas de hardware, fallas de software en sistemas operativos o aplicaciones, fallas en la red.
Código malicioso	Ocurre cuando se interrumpe el servicio a los clientes y usuarios o se pierde la integridad de la información a causa de virus, troyanos, gusanos, etc.
Denegación de servicio	Ocurre cuando se deniega el acceso de los usuarios legítimos a los recursos de los sistemas y las aplicaciones.
Errores de proceso	Ocurren cuando se generan errores en los procesos debido a datos incompletos o imprecisos.
Perdida de confidencialidad e integridad	Ocurren cuando ha ocurrido una divulgación no autorizada de información o cuando la información ha cambiado de estado de manera no autorizada o controlada (modificación deliberada, borrado, cambiado, agregado)
Uso indebido de los Sistemas de Información	Ocurren cuando los usuarios han abusado de las facilidades o información de los sistemas.

Tabla 35. Tipos y Detalles de Incidentes de Seguridad de la Información

Los incidentes de seguridad pueden ocasionar los siguientes niveles de impacto:

NIVEL	DETALLE
Crítico	• El incidente ha afectado completamente la prestación de uno o más servicios críticos de La Comisión. • El incidente ha afectado a varias unidades de negocio, áreas, departamentos o direcciones) • Se ha divulgado información clasificada como confidencial o sensible a personas o terceros no autorizados. • Se ha modificado deliberadamente o destruido información confidencial o sensible, o vital para la prestación de un servicio crítico
Medio	• El incidente ha afectado de forma parcial la prestación de un servicio. • El incidente ha afectado a una unidad de negocio, área, departamento o dirección. • Se ha divulgado información clasificada como uso interno a personas o terceros no autorizados. • Se ha modificado deliberadamente o destruido información.
Bajo	• El incidente ha afectado un componente de un servicio lo cual ha degradado de alguna forma el nivel de prestación del mismo. • El incidente ha afectado a uno o varios individuos.

Tabla 36. Nivel y Detalle de los Incidentes de Seguridad de la Información

MODELO DE INFORME MENSUAL DE EVENTOS, INCIDENTES, VULNERABILIDADES, PROBLEMAS Y VIOLACIONES DE SEGURIDAD DE LA INFORMACIÓN

Preparado por :

Nombre: Firma: Fecha:
Cargo :

Revisado por:

Nombre: Firma: Fecha:
Cargo :

CANTIDAD DE INCIDENTES POR TIPO

Cant. de casos	TIPO	%	MEJORAS O ACCIONES REALIZADAS

Tabla 37: Cantidad de incidentes por tipo

CANTIDAD DE INCIDENTES POR NIVEL

TIPO	NIVEL		
	Crítico	Medio	Bajo

Tabla 38: Cantidad de incidentes por nivel.

INSTRUCCIONES

El Informe Mensual de Eventos, Incidentes, Vulnerabilidades, Problemas y Violaciones Reportados al Área de Seguridad de la Información, se completa de la siguiente forma:

Preparado por: Identifica(n) el(los) nombre(s), cargo(s) y firma(s) escaneada(s) de la(s) persona(s) que prepara(n) el Informe, así como la fecha (dd/mm/aa) en que lo elabora(n).

Revisado por: Se detalla(n) el(los) nombre(s), cargo(s) y firma(s) escaneada(s) de (las) persona(s) que revisa(n) el Informe, y fecha de revisión

- **Para la Cantidad de Incidentes por Tipo:**

Cant. de Casos: Se escribe la cantidad de incidentes de seguridad de la información de la misma índole ocurridos durante el mes.

Tipo: Se escribe el tipo de incidente,

Porcentaje (%): Se escribe el porcentaje de incidentes de cada tipo en base al total de icidentes ocurridos.

Mejoras o Acciones Realizadas: Se escriben las actividades que efectuaran las mejoras relacionadas con los eventos, incidentes, vulnerabilidades, problemas y violaciones de seguridad de la información, con el objeto de reducirlos o de que no vualvan a repetirse.

- **Para la Cantidad de Incidentes por Nivel**

Tipo: Se escribe el tipo de incidente,

Nivel Crítico/Medio/Bajo: Se escribe la cantidad de incidentes según corresponda de acuerdo al impacto causado,

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

ANÁLISIS ANUAL DE INCIDENTES, PROBLEMAS Y VIOLACIONES DE SEGURIDAD DE LA INFORMACIÓN

Preparado por :

Nombre: **Cargo :**	Firma:	Fecha:

Revisado por:

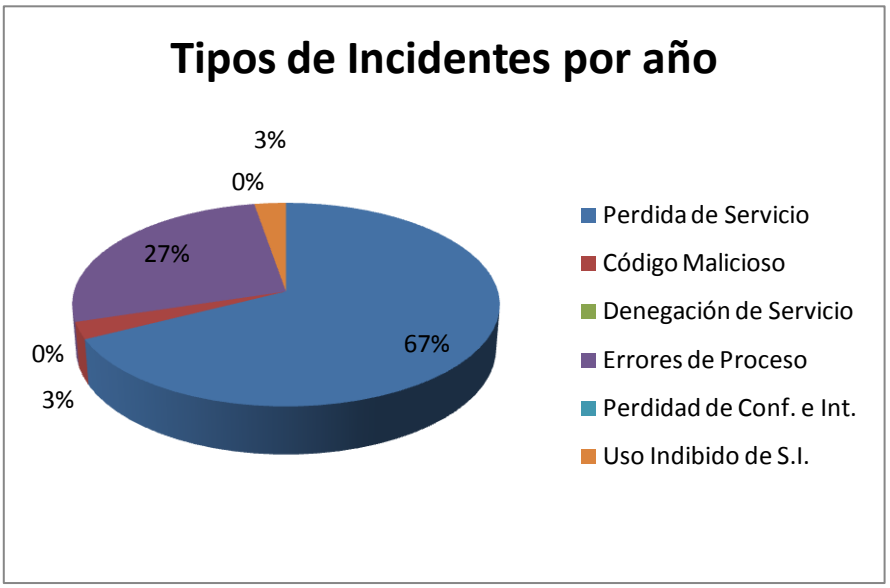
Nombre: **Cargo :**	Firma:	Fecha:

Aprobado por:

Nombre : **Cargo :**	Firma:	Fecha:

CANTIDAD DE INCIDENTES POR TIPO

Cant. de casos	TIPO	%	MEJORAS O ACCIONES REALIZADAS

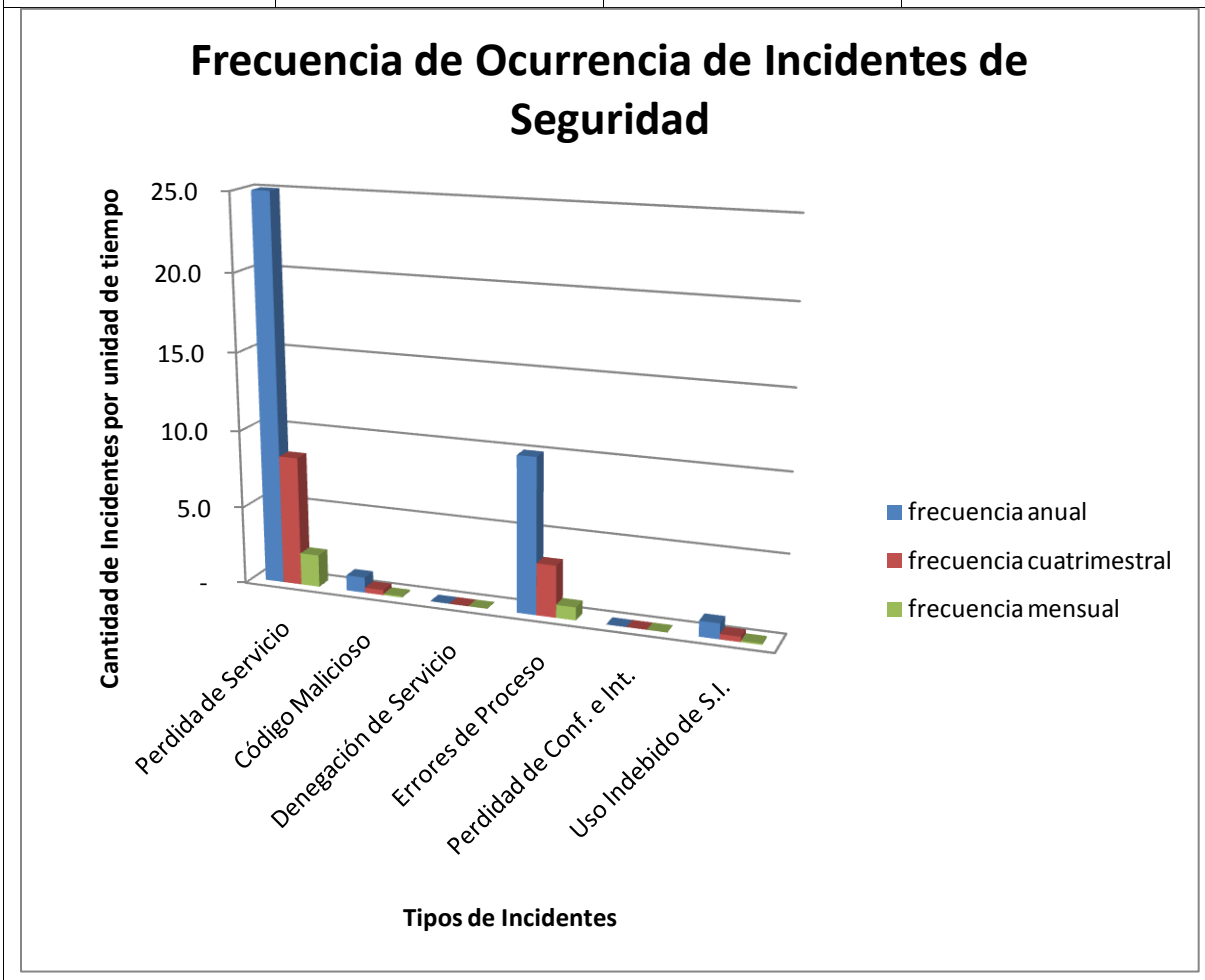


(Ejemplo)

Tabla 39: Cantidad de incidentes por ano

FRECUENCIA DE INCIDENTES POR TIPO

TIPO	FRECUENCIA		
	Anual	Cuatrimestral	Mensual

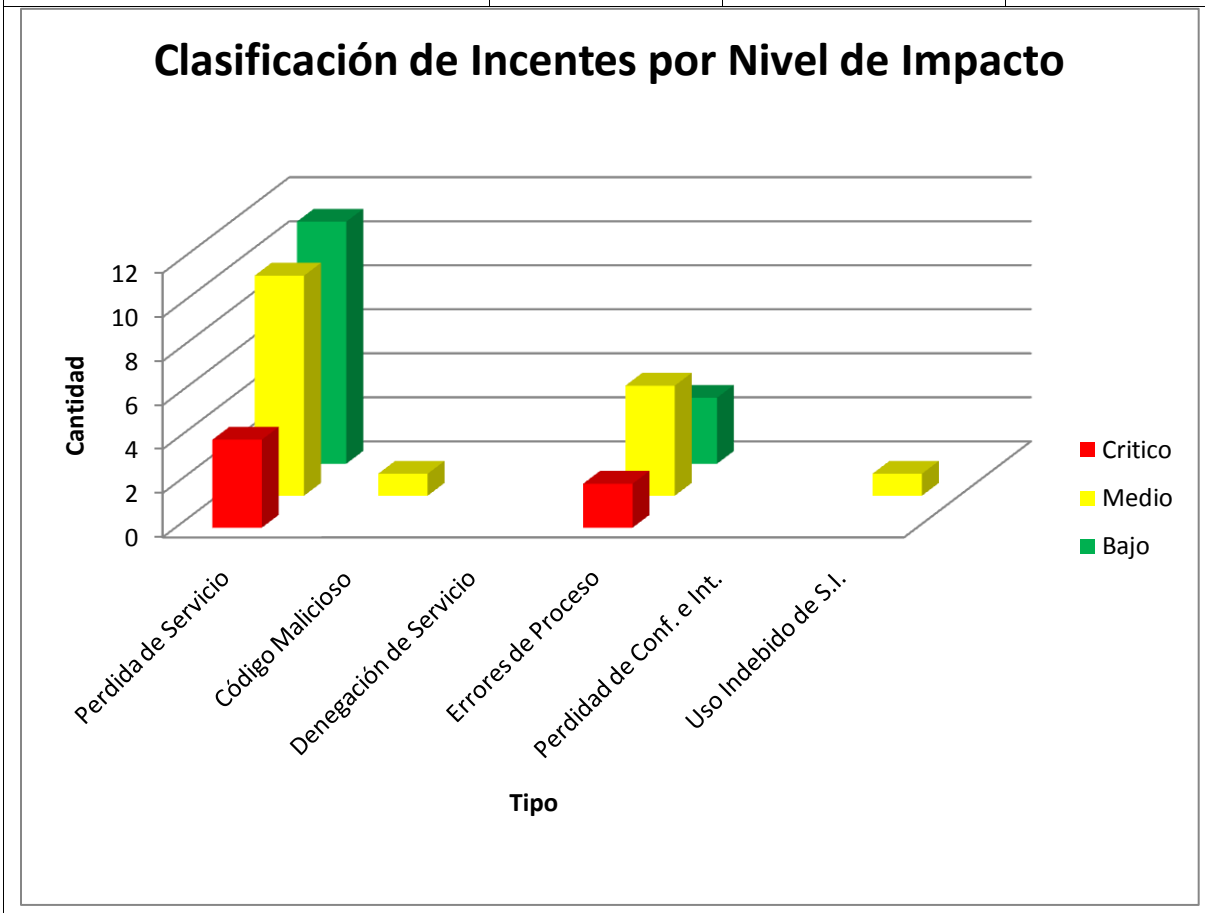


(Ejemplo)

Tabla 40: frecuencia de ocurrencia de incidente de seguridad

CANTIDAD DE INCIDENTES POR NIVEL

TIPO	NIVEL		
	Crítico	Medio	Bajo



(Ejemplo)

Tabla 41: Clasificación de incidentes por nivel de impacto

INSTRUCCIONES

El **Revisado por:** Se detalla(n) el(los) nombre(s), cargo(s) y firma(s) escaneada(s) de (las) persona(s) que revisa(n) el Análisis, y fecha de revisión

Aprobado por: Identifica el nombre, cargo y firma escaneada de la persona que aprueba el documento y la fecha en que lo aprueba.

Análisis Anual de Incidentes Problemas y Violaciones de Seguridad de la Información en La Comisión, se completa de la siguiente forma:

Preparado por: Identifica(n) el(los) nombre(s), cargo(s) y firma(s) escaneada(s) de la(s) persona(s) que prepara(n) el Análisis, así como la fecha (dd/mm/aa) en que lo elabora(n).

- **Para la Cantidad de Incidentes por Tipo:**

Cant. De Casos: Se escribe la cantidad de incidentes de seguridad de la información de la misma índole ocurridos durante el año.

Tipo: Se escribe el tipo de incidente

Porcentaje (%): Se escribe el porcentaje de incidentes de cada tipo en base al total de icidentes ocurridos.

Mejoras o Acciones Realizadas: Se escriben las actividades que efectuaran las mejoras relacionadas con los eventos, incidentes, vulnerabilidades, problemas y violaciones de seguridad de la información, con el objeto de reducirlos o de que no vualvan a repetirse.

- **Para la Frecuencia de Incidentes por Tipo:**

Tipo: Se escribe el tipo de incidente

Frecuencia Anual/Cuatrimestral/Mensual: Se escribe el número de veces que se repite un incidente, según su tipo por unidad de tiempo. Número de veces al año, número de veces cada 4 meses, número de veces al mes.

- **Para la Cantidad de Incidentes por Nivel**

Tipo: Se escribe el tipo de incidente.

Nivel Crítico/Medio/Bajo: Se escribe la cantidad de incidentes según corresponda de acuerdo al impacto causado,

5. Valuación del riesgo

a) Proceso de valuación del riesgo.

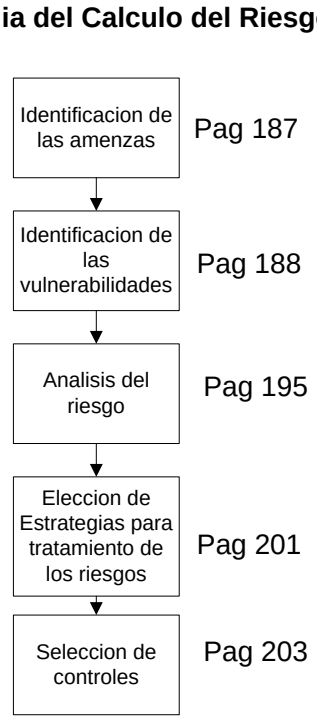


Figura 28: Metodología del cálculo del riesgo.

El cálculo de los riesgos de seguridad de información incluye normalmente el análisis y evaluación del riesgo.
El análisis del riesgo contempla:

1. Identificación de activos (ver ISO 27001:2005 4.2.1 (d)).
2. Identificación de requerimientos legales y comerciales que son relevantes para los activos identificados (ver ISO 27001:2005 4.2.1 (d))
3. Tasación de los activos identificados, considerando los requerimientos legales y comerciales, así como los impactos resultantes de una perdida por confidencialidad, integridad y disponibilidad (ver ISO 27001:2005 4.2.1 (c)).
4. Identificación de amenazas y vulnerabilidades para cada activo previamente identificado (ver ISO 27001:2005 4.2.1 (d)).
5. Calculo de la posibilidad de que las amenazas y vulnerabilidades ocurran (ver ISO 27001:2005 4.2.1 (e)).

La evaluación del riesgo incluye:

A. Calculo del riesgo (ver ISO 27001:2005 4.2.1 (e)).
B. Identificación del significado de los riesgos. Esto se hace definiendo criterios y evaluando los riesgos contra una escala predeterminada (ver ISO 27001:2005 4.2.1 (e)).

Es importante entender la exigencia de la norma ISO 27001:2005 en relación con el riesgo. La exigencia es bastante clara y no debería llevar a confusiones. En primera instancia, se deben seguir los pasos para realizar el análisis del riesgo, y posteriormente construir una escala para determinar la evaluación del riesgo. Son dos etapas claramente definidas, a continuación se desarrollaran cada una de las etapas aplicadas el SGSI en diseño.

b) Aspectos a contemplar para efectuar la metodología del análisis de riesgo.

i. Identificación de activos.

Los activos de información en cualquier organización, dentro del alcance del SGSI, son fundamentales para una correcta implementación del mismo. El análisis y la evaluación del riesgo y las decisiones que se tomen en relación con el tratamiento del riesgo en organización giran alrededor de los activos de información identificados.

Un activo es algo tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones. He ahí la vital importancia de la gestión y la responsabilidad por los activos.

Es importante clarificar que es un activo de información en el contexto del ISO 27001:2005. Según el ISO 17799:2005 (Código de práctica para la Gestión de Seguridad de Información), un activo de información es: "… algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger".

Es así como tomando como referencia el ISO 17799:2005 se clasificaron los siguientes activos de información para la Comisión:

No.	ACTIVOS DE INFORMACIÓN
1	Base de datos de clientes
2	Base de datos de empleados
3	Base de datos financieras
4	Base de datos de producción
5	Base de datos proveedores
6	Equipo de computo
7	Línea dedicada
8	Internet
9	Servicio de archivos
10	Copias de respaldo
11	Líneas telefónicas
12	Cámaras
13	Correspondencia interna
14	Correspondencia externa
15	Información intelectual
16	Correos electrónicos
17	Intranet

18	Documentos en papel impreso
19	Documentos en medio digital
20	Manuales de usuarios
21	Documentos legales
22	Software de sistemas

Tabla 42: Identificación de Activos.

Es muy importante estar conceptualmente claros que es un activo de información y conocer sus distintas modalidades, para así poder realizar un correcto análisis y una evaluación del riesgo, y por ende, poder establecer adecuadamente el modelo ISO 27001:2005

Dicha identificación de activos fue resultado de un proceso de identificación y de tasación de activos mediante un grupo multidisciplinario compuesto entre las personas involucradas en los procesos y subprocesos que abarca el alcance.

En esa reunión se estableció que las personas involucradas en cada proceso son los dueños de activos, entendiendo por ello toda aquella persona que tiene una responsabilidad por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos importantes deben identificarse con claridad y posteriormente deben ser tasados para visualizar el impacto por su deterioro o por sus fallas en: (1) confidencialidad, (2) integridad y (3) disponibilidad (ver ISO 27001:2005 4.2.1)

- **Identificación de requerimientos legales y comerciales relevantes para los activos identificados.**

El ISO 17799:2005 es bastante preciso al explicar la confección de los requerimientos de seguridad en cualquier clase de organización. Estos se derivan de tres aspectos:

1. La primera fuente es la evaluación de los riesgos que afectan a la organización, determinado las amenazas de los activos, ubicando las vulnerabilidades y posibilidad de ocurrencia estimando los potenciales impactos.
2. La segunda es el aspecto legal, los cuales están definidos al inicio de este documento
3. La tercera es el conjunto particular de principio, objetivos y requerimientos para procesar la información.

ii. Tasación de activos

En la siguiente tabla se presenta la tasación de activos que se realizo a la Comisión, cada activo se taso haciendo uso de la escala de Likert.

Escala	**1**	**2**	**3**	**4**	**5**
Significado	Muy bajo 10%	Bajo 20%	Medio 50%	Alto 80%	Muy alto 95%

Tabla 43: Escala de Likert.

Estos criterios serán utilizados para asignar la puntuación, totas las puntuaciones son resultado de un conceso de reuniones en las cueles se involucro a los principales usuarios y productores de información de las Unidades en estudio.

La pregunta que se efectuó es: ¿Como una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?

A continuación se procede a relacionar cada activo con la escala antes detallada y luego a promediar las tres puntuaciones para tener un total de cada activo, con ello estamos dando respuesta a la pregunta anterior y determinado como una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad de CEL, tanto cuantitativamente y cualitativamente al relacionar la puntuación obtenida con la tabla de criterios de likert que se presenta posterior a la siguiente tabla.

¿Como una pérdida o una falla en un determinado activo afecta la confidencialidad, la integridad y la disponibilidad?					
ACTIVOS DE INFORMACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL (aprox)	%
Base de datos de clientes	4	3	2	3	50%
Base de datos de empleados	3	4	2	3	50%
Equipo de computo	5	5	5	5	95%
Base de datos financieras	4	3	3	3	50%
Base de datos de producción	3	2	2	2	20%
Base de datos proveedores	4	3	3	3	50%
Línea dedicada	3	3	3	3	50%
Internet	3	5	4	4	80%
Servicio de archivos	4	3	2	3	50%
Copias de respaldo	4	2	3	3	50%
Líneas telefónicas	3	3	2	3	50%
Cámaras	2	2	2	2	20%
Correspondencia interna	5	3	4	4	80%
Correspondencia externa	5	3	4	4	80%
Información intelectual	5	4	2	4	80%
Correos electrónicos	3	3	2	3	50%
Intranet	3	3	3	3	50%
Documentos en papel impreso	5	4	2	4	80%
Documentos en medio digital	5	3	2	3	50%
Manuales de usuarios	5	3	3	4	80%
Documentos legales	5	4	4	4	80%
Software de sistemas	4	5	3	4	80%

Tabla 44: Tasación de Activos

- **Criterios para escala de LIKERT:**

El propósito de esta tabla es dar una traducción a la puntuación total que arroja la escala de likert, en ella encontramos los posibles escenarios que pudieran darse en La Comisión en relación con la Escala que cada activo obtenga. Cada escenario maneja las consecuencias de llegar a darse la pérdida o fallo de alguno de los activos, estas pérdidas o fallas se relacionan con actividades o riesgos.

La tabla se diseño con un grupo multidisciplinario de CEL y nosotros como diseñadores del SGSI.

Escala	Criterios
5 (95%)	• Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística • Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información • Seguridad: probablemente sea causa de un incidente excepcionalmente serios de seguridad o dificulte la investigación de incidentes excepcionalmente serios • Seguridad de las personas: probablemente suponga gran pérdida de vidas humanas • Orden público: alteración sería del orden constitucional • Probablemente cause un impacto excepcionalmente grave en las relaciones internacionales • Datos clasificados como secretos
4 (80%)	• Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo. • Administración y gestión: probablemente impediría la operación efectiva de la organización • Probablemente causaría una publicidad negativa generalizada • Probablemente cause perjudique la eficacia o seguridad de la misión operativa o logística • Probablemente cause serios daños a misiones importantes de inteligencia o información • Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación • Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves • Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos • Probablemente cause un impacto significativo en las relaciones internacionales • Datos clasificados como confidenciales
3 (50%)	• Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones • Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la organización • Probablemente sea causa una cierta publicidad negativa • Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local • Probablemente dañe a misiones importantes de inteligencia o información • Información personal: probablemente afecte a un grupo de individuos • Información personal: probablemente quebrante leyes o regulaciones • Seguridad de las personas: probablemente cause daños menores a varios individuos • Dificulte la investigación o facilite la comisión de delitos • Datos clasificados como de difusión limitada.

Escala	Criterios
2 (20%)	• Pudiera causar la interrupción de actividades propias de la Organización • Administración y gestión: pudiera impedir la operación efectiva de una parte de la organización • [Pudiera causar una pérdida menor de la confianza dentro de la Organización • Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local) • Pudiera causar algún daño menor a misiones importantes de inteligencia o información • Intereses comerciales o económicos: • Información personal: pudiera causar molestias a un individuo • Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley o regulación • Seguridad: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente • Seguridad de las personas: pudiera causar daños menores a un individuo • Orden público: pudiera causar protestas puntuales • Pudiera tener un impacto leve en las relaciones internacionales • Datos clasificados como sin clasificar
1 (10%)	• no afectaría a la seguridad de las personas • sería causa de inconveniencias mínimas a las partes afectadas • supondría pérdidas económicas mínimas • no supondría daño a la reputación o buena imagen de las personas u organizaciones

Tabla 45: Criterios de la escala de Likert

De igual forma la norma también exige detallar quienes son los dueños y propietarios de la información, en la siguiente tabla se muestran los activos tasados sus respectivos propietarios:

Activos de información	Propietario
Base de datos clientes	Unidad de comercialización
Base de datos de empleados	Unidad de recursos Humanos
Equipo de computo	Unidad de informática
Base de datos financieras	Unidad de comercialización
Base de datos de producción	Unidad de producción
Base de datos proveedores	Unidad de comercialización
Internet	Unidad de informática
Servicio de archivos	Unidad de recursos
Copias de respaldo	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Líneas telefónicas	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Cámaras	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Correspondencia interna	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y

Activos de información	Propietario
	Unidad Informática
Correspondencia externa	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Información intelectual	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Correos electrónicos	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Intranet	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Documentos en papel impreso	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Documentos en medio digital	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Manuales de usuarios,	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Documentos legales	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática
Software de sistemas	Unidad de comercialización, Unidad de Recursos Humanos, Unidad de producción y Unidad Informática

Tabla 46: Propietarios de los Activos de Información.

El propietario de los activos debe de ser responsable de definir apropiadamente la clasificación de seguridad y los derechos de acceso a los activos, y establecer los sistemas de control. También es el responsable de revisar los derechos de acceso y clasificación de seguridad. Cada propietario deberá definir, documentar e implementar las reglas para el uso aceptable de activos, describiendo las acciones permitidas y prohibidas en el uso cotidiano de los activos, las personas que utilicen los activos deben de estar consientes de dichas reglas como parte de sus funciones en cada puesto de trabajo.

iii. Identificación de amenazas y vulnerabilidades

Los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar incidentes no deseados que pueden generar daño a la organización y a sus activos. Teniendo en cuenta que toda amenaza es la indicación de un evento no deseado a continuación se presenta un resumen de ellas:

- **AMENAZAS**

(Inglés: Threat). Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Como es de notar las amenazas pueden originar de fuentes o eventos accidentales o deliberados. Para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema. Al mismo tiempo se ha definido una probabilidad de ocurrencia, dicha probabilidad ha sido calculada por un grupo de expertos que tienen conocimiento de la naturaleza de la amenaza y utilizando las estadísticas pertinentes.

Para ello se utilizo la escala de Likert.

Escala	1	2	3	4	5
Significado	Muy bajo 10%	Bajo 20%	Medio 50%	Alto 80%	Muy alto 95%

No.	Amenazas	Probabilidad de ocurrencia
1	Amenazas naturales como Terremotos	10%
2	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	20%
3	Amenazas humanas como huelgas, epidemias, perdidas de personal clave	10%
4	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	80%
5	Amenazas operacionales como crisis financieras, aspectos regulatorios	20%
6	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.	10%

Tabla 47: Probabilidades asociadas a las amenazas

- **VULNERABILIDADES**

(Inglés: Vulnerability). Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.
Las vulnerabilidades son debilidades en las políticas organizacionales o practicas que pueden resultar en acciones no autorizadas.
En el siguiente cuadro se han clasificado las vulnerabilidades por las distintas fuentes que las pueden originar, se utilizaron algunas clausulas del ISO 17799:2005 como consulta para efectuar la categorización.

Categoría	Vulnerabilidades asociadas	Unidad afectada
Seguridad de los Recursos Humanos	Personal con poco entrenamiento en seguridad	Producción, Comercialización, Informática, Recursos Humanos
	Carencia de conciencia en seguridad de la información	Producción, Comercialización, Informática, Recursos Humanos
	Falta de mecanismos de monitoreo	Producción, Comercialización, Informática,
	Falta de políticas para resguardo de documentos	Producción, Comercialización, Informática, Recursos Humanos
	NO se tiene plan de tratamiento de riesgos	Producción, Comercialización, Informática, Recursos Humanos
	Falta de políticas para el uso correcto de documentos confidenciales.	Producción, Comercialización, Informática, Recursos Humanos

Categoría	Vulnerabilidades asociadas	Unidad afectada
	No hay programas de capacitación para el manejo y seguridad de la información	Producción, Comercialización, Informática, Recursos Humanos
	NO se realizan auditorias que verifiquen el manejo y seguridad de la información	Producción, Comercialización, Informática, Recursos Humanos
	Mucha información que se maneja no goza de autenticidad, solamente de un proceso de validación por firmas	Producción, Comercialización, Informática, Recursos Humanos
	La información no es accesible al 100%	Producción, Comercialización, Informática, Recursos Humanos
	No hay definida una capacidad para localizar, evaluar y utilizar la información en todos los procesos.	Producción, Comercialización, Informática, Recursos Humanos
	Cuando se intercambia información confidencial no se cuanta con procesos definidos para su resguardo	Producción, Comercialización, Informática, Recursos Humanos
	No se posee un manual para el manejo y seguridad de la información en todas las Unidades	Producción, Comercialización, Informática, Recursos Humanos
	No se tiene garantizada la integridad de la información	Producción, Comercialización, Informática, Recursos Humanos
Control de acceso	Falta de política sobre escritorio y pantalla limpia	Producción, Comercialización, Informática, Recursos Humanos
	Falta de protección a equipos de telecomunicación	Producción, Comercialización, Informática, Recursos Humanos
	Niveles de seguridad en contraseñas bajo	Producción, Comercialización, Informática, Recursos Humanos
	No se cuanta con acciones para el trato de riesgos	Producción, Comercialización, Informática, Recursos Humanos
	NO existe un enfoque de evaluación de riesgos en todos los procesos	Producción, Comercialización, Informática, Recursos Humanos
	Política inapropiada para control de accesos	Producción, Comercialización, Informática, Recursos Humanos
	No se respetan las horas y periodos de entrega de reportes	Producción, Comercialización,

Categoría	Vulnerabilidades asociadas	Unidad afectada
		Informática, Recursos Humanos
	Las contraseñas del sistema informático solo las posee una persona. No existe un respaldo por contingencia.	Producción, Comercialización, Informática, Recursos Humanos
	los hardwares no son lo suficientemente seguros	Producción, Comercialización, Informática, Recursos Humanos
Seguridad Física y ambiental	Control de acceso físico inadecuado de oficinas y salones	Producción, Comercialización, Informática, Recursos Humanos
	Riesgo de daño de equipo informático por variaciones de voltajes.	Producción, Comercialización, Informática, Recursos Humanos
	Archivadores sin duplicado de llaves	Producción, Comercialización, Informática, Recursos Humanos
	Archivadores dañados sin chapa	Producción, Comercialización, Informática, Recursos Humanos
	No se tienen recursos destinados para el manejo y seguridad de la información	Producción, Comercialización, Informática, Recursos Humanos
	NO hay controles definidos para el manejo y seguridad de la información	Producción, Comercialización, Informática
	No se tienen definidos puntos de resguardo de la información	Producción, Comercialización, Informática, Recursos Humanos
	no hay definido un sistema de trasporte para documentación	Producción, Comercialización
	los hardwares no son lo suficientemente seguros	Producción, Comercialización, Informática, Recursos Humanos

Tabla 48: Identificación de Vulnerabilidades.

Es bueno tener claro que las vulnerabilidades y las amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos. Por esta razón es necesario entender la relación entre las amenazas y vulnerabilidades. La pregunta fundamental es: ¿Qué amenaza pudiese hacer explotar cuales de las vulnerabilidades? A ello se le llama cálculo de las amenazas y las vulnerabilidades y se desarrollara en los siguientes apartados, pero desde ya es necesario comprender la relación para tenerlo claro.

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de la relación causalidad y probabilidad de ocurrencia.

En el siguiente grafico se muestra la relación causa – efecto entre activos, riesgos, vulnerabilidades y amenazas:

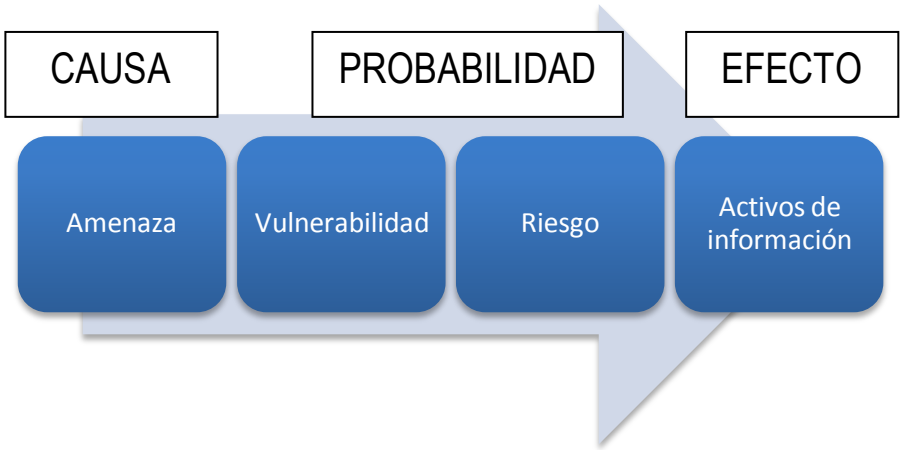


Figura 29: Flujo del impacto al activo.

Estos elementos del análisis no pueden verse de manera aislada. Existe una interdependencia de ellos bajo una relación de causa-efecto. Es fácil visualizar la variable que la organización podrá manipular y fortalecer, para minimizar que se ponga de manifiesto el riesgo y proteger los activos de información de una penetración e la amenaza, son la vulnerabilidad.

- **REVISIÓN DE LOS CONTROLES**

En algún momento previo al inicio de las actividades del cálculo del riesgo, o antes de identificar las amenazas y vulnerabilidades, deben identificarse los controles ya existentes y así medir su eficacia ya que un control ineficaz es una vulnerabilidad.
Para el caso de La Comisión, actualmente no se cuentan con controles destinados a la Seguridad y Manejo de la información por que se iniciara desde cero al diseñar los controles.

iv. Calculo de las amenazas y vulnerabilidades

Una vez identificadas las amenazas y las vulnerabilidades, es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo. El riesgo se define como la probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular.
Posibilidad de que puedan juntarse y causar un riesgo = (Probabilidad de ocurrencia de amenaza) x (Posibilidad de que la vulnerabilidad que sean explotadas por amenazas)
Este proceso incluye calcular: La Probabilidad de ocurrencia de amenaza (ya fue calculada anteriormente), y la Posibilidad de que la vulnerabilidad que sean explotadas por amenazas se calculo en base siempre a la escala de Likert

Escala	**1**	**2**	**3**	**4**	**5**
Significado	Muy bajo 10%	Bajo 20%	Medio 50%	Alto 80%	Muy alto 95%

Para este fin se deben considerar los siguientes aspectos de las amenazas:

- **Amenazas deliberadas:** la posibilidad de amenazas en la motivación, conocimiento, capacidad y recursos disponibles para posibles atacantes y la atracción de los activos para sofisticados atacantes.
- **Amenazas accidentales:** la posibilidad de amenazas, accidentales puede estimarse utilizando la experiencia y las estadísticas.
- **Incidentes del pasado:** los incidentes ocurridos en el pasado ilustran los problemas en el actual sistema de protección.
- **Nuevos desarrollos y tendencias:** esto incluye informes, novedades y tenencias obtenidas de diferentes medios, como internet.

➢ **CALCULO DE AMENAZAS Y VULNERABILIDADES**

No.	Amenazas	Vulnerabilidades asociadas	Probabilidad de ocurrencia de amenaza	Posibilidad de que la vulnerabilidad que sean explotadas por amenazas	TOTAL
1	Amenazas naturales como Terremotos	No hay definida una capacidad para localizar, evaluar y utilizar la información en todos los procesos.	10%	80%	8%
		NO hay controles definidos para el manejo y seguridad de la información		50%	5%
2	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	Falta de políticas para resguardo de documentos	20%	80%	16%
		NO se tiene plan de tratamiento de riesgos		50%	10%
		Control de acceso físico inadecuado de oficinas y salones		95%	19%
		Riesgo de daño de equipo informático por variaciones de voltajes.		80%	16%
		No se tienen recursos destinados para el manejo y seguridad de la información		50%	10%
3	Amenazas humanas como huelgas, epidemias, perdidas de personal clave	Falta de mecanismos de monitoreo	10%	20%	2%
		Falta de políticas para el uso correcto de documentos confidenciales		95%	9.5%
		No se tienen definidos puntos de resguardo de la información		50%	5%
4	Amenazas tecnológicas	No se posee un manual para el manejo y seguridad de la	80%	50%	40%

No.	Amenazas	Vulnerabilidades asociadas	Probabilidad de ocurrencia de amenaza	Posibilidad de que la vulnerabilidad que sean explotadas por amenazas	TOTAL
	como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	información en todas las Unidades			
		NO se realizan auditorias que verifiquen el manejo y seguridad de la información		20%	16%
		No se tiene garantizada la integridad de la información		20%	16%
		Falta de política sobre escritorio y pantalla limpia		20%	16%
		Niveles de seguridad en contraseñas bajo		80%	64%
		No se cuanta con acciones para el trato de riesgos		80%	64%
		NO existe un enfoque de evaluación de riesgos en todos los procesos		95%	76%
		Política inapropiada para control de accesos		80%	64%
		Las contraseñas del sistema informático solo las posee una persona. No existe un respaldo por contingencia.		80%	64%
		los hardwares no son lo suficientemente seguros		80%	64%
5	Amenazas operacionales como crisis financieras, aspectos regulatorios	Carencia de conciencia en seguridad de la información	20%	80%	16%
		No hay programas de capacitación para el manejo y seguridad de la información		80%	16%
		Mucha información que se maneja no goza de autenticidad, solamente de un proceso de validación por firmas		50%	10%
		Cuando se intercambia información confidencial no se cuanta con procesos definidos para su resguardo		95%	19%
		No se respetan las horas y periodos de entrega de reportes		20%	4%
		La información no es accesible al 100%		80%	16%
6	Amenazas sociales como	Personal con poco entrenamiento en seguridad de	10%	80%	8%

No.	Amenazas	Vulnerabilidades asociadas	Probabilidad de ocurrencia de amenaza	Posibilidad de que la vulnerabilidad que sean explotadas por amenazas	TOTAL
	motines, protestas, vandalismo, violencia laboral.	información			
		Falta de protección a equipos de telecomunicación		95%	9.5%
		Archivadores sin duplicado de llaves		80%	8%
		Archivadores dañados sin chapa		80%	8%
		no hay definido un sistema de trasporte para documentación		50%	5%

Tabla 49: Calculo de amenazas y vulnerabilidades.

v. Análisis del riesgo y evaluación[20]

➢ ANÁLISIS DEL RIESGO

El objetivo del análisis de riesgo es identificar y calcular los riesgos basados en la identificación de activos y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

La Comisión debe decidir el método para hace el cálculo del riesgo que sea más apropiado ella y los requerimientos de seguridad. Los niveles de riesgos calculados proseen un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos.

Todo riesgo tiene dos factores: uno que expresa el impacto del riesgo si ocurriera, también denominado "valor económico del activo en riesgo" y otro que expresa la probabilidad de que el riesgo ocurra. El factor de impacto del riesgo está basado en la tasación el riesgo. La probabilidad de que el riesgo ocurra se basa en las amenazas y vulnerabilidades y los valores que se han calculado. En la siguiente tabla se presenta el método que se utilizara en CEL para calcular el riesgo.

RIESGO		**FACTORES DEL RIESGO**		**MEDICIÓN DEL RIESGO**	**PRIORIZACIÓN DEL RIESGO**
Activos de información	Amenaza	impacto de la amenaza	probabilidad de ocurrencia		
Base de datos clientes	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones				
Base de datos de empleados	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones				
Base de datos financieras	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones				
Base de datos de producción	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de				

[20] Ver Anexo No. 13 Prueba Piloto del Análisis y evaluación del riesgo.

RIESGO		FACTORES DEL RIESGO		MEDICIÓN DEL RIESGO	PRIORIZACIÓN DEL RIESGO
Activos de información	Amenaza	impacto de la amenaza	probabilidad de ocurrencia		
	datos, fallas en líneas telefónicas y falsificaciones				
Base de datos proveedores	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones				
Equipo de computo	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso				
Internet	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones				
Servicio de archivos	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.				
Copias de respaldo	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.				
Líneas telefónicas	Amenazas naturales como Terremotos				
Cámaras	Amenazas naturales como Terremotos				
Correspondencia interna	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso				
Correspondencia externa	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso				
Información intelectual	Amenazas humanas como huelgas, epidemias, perdidas de personal clave				
Correos electrónicos	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones				
Intranet	Amenazas tecnológicas como virus, hacking,				

RIESGO		FACTORES DEL RIESGO		MEDICIÓN DEL RIESGO	PRIORIZACIÓN DEL RIESGO
Activos de información	Amenaza	impacto de la amenaza	probabilidad de ocurrencia		
	fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones				
Documentos en papel impreso	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.				
Documentos en medio digital	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones				
Manuales de usuarios,	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.				
Documentos legales	Amenazas operacionales como crisis financieras, aspectos regulatorios				
Software de sistemas	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso				

Tabla 50: Análisis del riesgo.

Una vez calculada la medición del riesgo (multiplicando los valores obtenidos del impacto de la amenaza y la probabilidad de ocurrencia), se procede a priorizar en orden, con base en su factor de exposición del riesgo. En una escala del 1 al 6, representado los riesgos con prioridad 1, 2 y 3 los de mayor peligrosidad para CEL (ver ISO 27001:2005 4.2.1 (e)).

- **EVALUACIÓN DEL RIESGO**

Una vez efectuado el cálculo del riesgo por cada activo, en relación con su amenaza, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los más significativos. A todo este proceso se le denomina evaluación del riesgo.

Para realizar la evaluación, los criterios que se han utilizado para determinar los niveles de riesgo son los siguientes:

- Impacto económico del riesgo.
- Tiempo de recuperación de la comisión
- Posibilidad real de ocurrencia del riesgo (calculado en la tabla anterior)
- Posibilidad de interrumpir las actividades de la comisión.

Para los datos que no han sido calculados siempre se utilizara de referencia la escala de liberta.
Una vez identificados los criterios, se procede a realizar la evaluación y determinar los grados de importancia que representan las amenazas para la comisión.

TOTAL = ((Impacto económico del riesgo) x (Tiempo de recuperación) x (Probabilidad de ocurrencia del riesgo) x (Probabilidad de interrumpir las actividades)) / 100

RIESGO		CRITERIOS PARA EVALUAR LA IMPORTANCIA DEL RIESGO				
Activos de información	**Amenaza**	**Impacto económico del riesgo**	**Tiempo de recuperación**	**Probabilidad de ocurrencia del riesgo**	**Probabilidad de interrumpir las actividades**	**TOTAL**
Base de datos clientes	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones					
Base de datos de empleados	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones					
Base de datos financieras	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso					
Base de datos de producción	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones					
Base de datos proveedores	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones					
Equipo de computo	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones					
Internet	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones					

RIESGO		CRITERIOS PARA EVALUAR LA IMPORTANCIA DEL RIESGO				
Servicio de archivos	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.					
Copias de respaldo	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.					
Líneas telefónicas	Amenazas naturales como Terremotos					
Cámaras	Amenazas naturales como Terremotos					
Correspondencia interna	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso					
Correspondencia externa	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso					
Información intelectual	Amenazas humanas como huelgas, epidemias, perdidas de personal clave					
Correos electrónicos	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones					
Intranet	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones					
Documentos en papel impreso	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.					
Documentos en medio digital	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones					
Manuales de usuarios,	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.					
Documentos	Amenazas operacionales como crisis					

RIESGO		CRITERIOS PARA EVALUAR LA IMPORTANCIA DEL RIESGO				
legales	financieras, aspectos regulatorios					
Software de sistemas	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso					

Tabla 51: Evaluación del riesgo.

La evaluación del riesgo debe poder identificar los niveles de riesgo generalmente aceptables, aquellos riesgos cuyo nivel y estimación de daño es pequeño puede aceptarse como parte de su trabajo cotidiano y en consecuencia no se requiere mayor acción. Todos los otros riesgos requieren acciones concretas que se detallaran en el plan de tratamiento de riesgos y al proceso de toma de decisión de la comisión.
El criterio que se toman para definir que un riesgo es pequeño se obtuvo de una discusión y consenso entre los diferentes jefes de las Unidades en estudio, luego de revisar la evaluación del riesgo.
Si el puntaje total de los criterios para la importancia del riesgo es menor que 1.0 se define un nivel de riesgo aceptable, para valores mayores o iguales de 1.0 se define que los riesgos son de relevancia para La Comisión por lo que se deberán tomar en cuenta para la elaboración del plan de tratamiento de riesgos.

- **TRATAMIENTO DEL RIESGO Y PROCESO DE TOMA DE DECISIÓN GERENCIAL**

Una vez efectuado el análisis y evaluación del riesgo, se debe decidir cuales acciones se han de tomar con esos activos que están sujetos a riesgos. Los riesgos descubiertos pueden manejarse con una serie de controles para la detección y prevención, las tácticas para evitar el riesgo.
En seguida se describen estos enfoques y el proceso de toma de decisiones involucrado.

- **PROCESO DE TOMA DE DECISIONES**

Una vez que el riesgo se ha calculado, se debe iniciar un proceso de toma de decisiones con respecto a cómo se tratara el riesgo. Distintos escenarios dictaminan la decisión a tomar. La decisión que guarda relación con el tratamiento del riesgo suele estar influenciada por los siguientes factores:

- El posible impacto si el riesgo se pone de manifiesto
- Que tan frecuente pude suceder el riesgo.

Estos factores dan una idea de la perdida esperada si el riesgo ocurriera, si nada se hiciera para mitigar este riesgo estimado. Más aun sabiendo que los riesgos relacionados con seguridad de la información pueden ser difíciles de cuantificar en términos de la probabilidad de ocurrencia.
Esto se presenta por la carencia de estadísticas de conocimiento público en relación con la frecuencia de ocurrencia. Las personas involucradas en la toma de decisiones, sobre tratamiento de riesgos, deben analizar con cuidado la precisión y la confiabilidad de la información en la cual basen su decisión, y también visualizar el grado de perdida que están dispuestas a aceptar.

vi. Estrategias posibles para el tratamiento del riesgo.

- **REDUCCIÓN DEL RIESGO.**

Para todos aquellos riesgos donde la opción de reducirlos se ha tomado, se deben implementar controles apropiados para poder reducirlos al nivel que se definió en el numeral anterior. Es importante mencionar que al haber identificado el nivel de control, conviene considerar los requerimientos de seguridad relacionados con los riesgos.
Los controles pueden reducir el riesgo estimado en dos maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza.
- Reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados, reaccionando y recuperándose de ellos.

Para proteger sus activos La Comisión escogió adoptar una combinación de ambas como decisión que depende de los requerimientos del negocio, el ambiente y las circunstancias en las cuales La Comisión opera.
Cabe decir que actualmente no existe un enfoque universal para realizar la selección de objetivos de control y controles. El proceso de selección involucro una serie de discusiones y consultas con distintas personas involucradas en los procesos, las cuales son de vital importancia en ellos. Este proceso de selección requirió una serie de resultados que más se adecuara a La Comisión en términos de sus requerimientos para la protección de sus activos y tolerancia al riesgo.

- **OBJETIVAMENTE ACEPTAR EL RIESGO.**

Muchas veces se presenta o se presentara la situación en la cual La Comisión no encuentra controles para mitigar el riesgo, o en la cual la implementación de controles tiene un costo mayor que las consecuencias del riesgo. En estas circunstancias la decisión de aceptar el riesgo y vivir con las consecuencias es la más adecuada. Cuando se toma una decisión de estas, se debe documentar y definir con precisión el criterio de aceptación del riesgo y así cumplir con las clausulas 4.2.1 (c) y 5.1 (f) del ISO 27001:2005. La gerencia debe de aprobar la decisión de aceptación del riesgo.

- **TRANSFERENCIA DEL RIESGO.**

La transferencia del riesgo es una opción cuando para La Comisión es difícil reducir o controlar el riesgo a un nivel aceptable. La alternativa de transferencia a una tercera parte es más económica ante estas circunstancias.
Existe una serie de mecanismos para transferir el riesgo a otra organización; por ejemplo, utilizar a una aseguradora. Se debe tener mucho cuidado al tratar con aseguradoras, porque siempre existe el elemento des riesgo residual. Con empresas aseguradoras siempre habrá condiciones y exclusiones que se aplicaran de acuerdo con la clase de ocurrencia.
Se requiere analizar la transferencia del riesgo a la aseguradora para identificar cuanto del riesgo actual se transferirá. De modo usual, las empresas aseguradoras no mitigan los impactos no financieros y tampoco proveen mitigación inmediata en el evento de un accidente.
Otra opción para la transferencia del riesgo es la utilización de terceros para manejar activos o procesos críticos, en la medida en que tengan la capacidad de hacerlo.

Algo muy importante que debe recordarse es el riesgo residual que siempre estará presente.
Por último, la responsabilidad por la seguridad de la información y por las instalaciones para el procesamiento de información, al haberse tercerizado estas, siempre le corresponde a La Comisión original.
Siempre al tercerizar puede creerse que la empresa prestadora de servicios debe estimar y gestionar nuevos riesgos.

- **EVITAR EL RIESGO**

Por el modo de evitar el riesgo se entiende cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad comercial en particular, para evitar la presencia del riesgo.
Para ello se definió que el riesgo puede evitarse por medio de:

- No desarrollar ciertas actividades (por ejemplo evitar el documentación en papel)
- Mover los activos de un área de riesgo a otra más segura.
- Decidir no procesar información particularmente sensitiva.

El hecho de evitar el riesgo debe de sopesarse contra necesidades financieras y comerciales. Pudiera ser que se concluya que esta decisión de evitar el riesgo no es factible. En el siguiente grafico se presenta en forma esquemática el proceso diseñado para la toma de decisiones para elegir una opción de tratamiento.

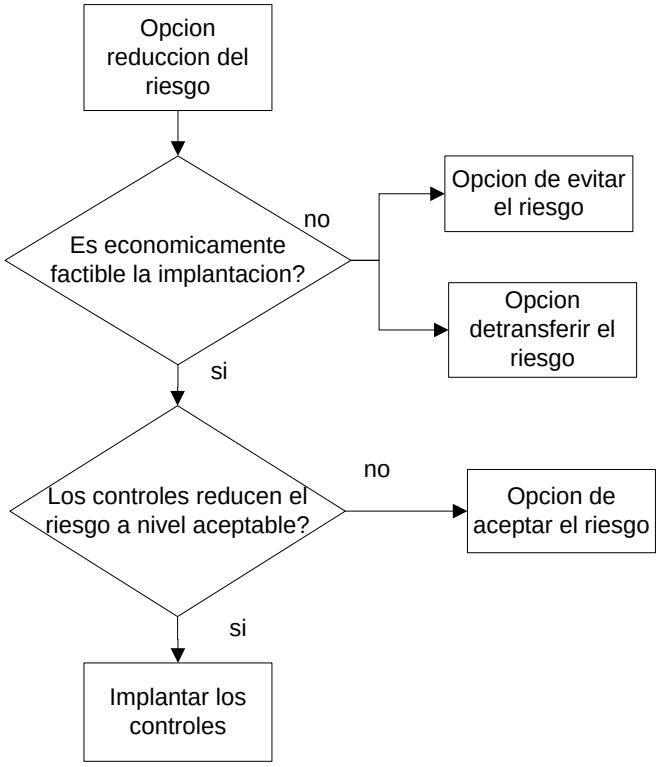


Figura 30: Proceso de toma de decisión.

Como se observa, el método ISO 27001:2005 le da un rol protagónico a la gerencia frente al riesgo residual.

vii. Riesgo residual

Después de implementar las decisiones relacionadas con el tratamiento de riesgo (detalladas en el diagrama anterior) siempre habrá un remanente de ese mismo riesgo. Justamente el riesgo que queda, después de implantar el plan de tratamiento, se denomina riesgo residual, que puede ser difícil de calcular, pero por lo menos debe realizarse una evaluación para asegurar que logra la protección suficiente.
Si el riesgo residual se considera inaceptable, deben de tomarse decisiones para resolver su caso, muy probablemente se someta de nuevo al proceso de toma de decisiones para saber cómo manejarlo. Otra opción es identificar diferentes opciones de tratamiento de riesgo; otra es instaurar más controles, o hacer arreglos con aseguradoras para reducir finalmente el riesgo a niveles aceptables.
Habrá casos debido a la naturaleza del negocio y a los riesgos inherentes, reducir los riesgos a un nivel aceptable pusiera ser no posible o financieramente aceptable.
Ante estas circunstancias, pudiera necesitarse objetivamente aceptar el riesgo. Todos los riesgos residuales que se hayan aceptado debieran ser documentados y aprobados por la gerencia. En la clausula 4.2.1 (h), el ISO 27001:2005 plantea que la gerencia debe de aprobar los riesgos residuales propuestos, y en la clausula 4.2.3 (d) precisa que la gerencia efectuara revisiones a las evaluaciones del riesgo a intervalos planteados, y revisara el nivel de riesgo residual y de riesgo aceptable identificado.

viii. Selección de objetivos de control y controles para el tratamiento de riesgos

Una vez se realiza el proceso de identificar las opciones de tratamiento de riesgo y haberlas evaluado, La Comisión debe de decidir cuáles objetivos de control y controles escoger para el tratamiento de riesgos.
La selección de objetivos de control y controles debe de efectuarse tomando en cuenta el criterio establecido para la aceptación del los riesgos, así como los requerimientos legales, como reguladores y contractuales. En la clausula 4.2.1 (g) y el ISO 27001:2005 es muy puntual al respecto.
La norma es bastante clara sobre el proceso de selección de objetivos de control y controles. En la clausula 4.2.1 (g) se plantea que los objetivos de control y controles pueden modificarse a medida se presentes los riesgos por si alguno de ellos no se apega a los controles diseñados en este apartado.
Para objetos de en un futuro buscar una certificación internacional se toman los siguientes controles para el plan de tratamiento de riesgos, dichos objetivos de control y controles están diseñados en conformidad con lo establecido en el ISO 27001:2005.

COD.	AGENTE A CONTROLAR	CONTROL
A.5 POLÍTICA DE SEGURIDAD		
A.5.1 Política de seguridad de la Información **Objetivo: Dirigir y dar soporte a la gestión de la seguridad de la información, de acuerdo con los requisitos de CEL, las leyes y reglamentos pertinentes.**		
A.5.1.1	Documento de la política de seguridad de la	Un documento de política de seguridad de información será aprobado por la dirección, publicado y comunicado a todos los empleados y partes

COD.	AGENTE A CONTROLAR	CONTROL
	información.	externas pertinentes.
A.5.1.2	Revisión de la política de seguridad de la información	La política de seguridad de la información debe Revisarse a intervalos planificados, o si ocurren cambios significativos asegurar su conveniencia, adecuación y eficacia continua.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1 Organización interna **Objetivo: Gestionar la seguridad de la información dentro de la organización**		
A.6.1.1	Compromiso de la dirección para la seguridad de la información	La dirección debe apoyar activamente la seguridad dentro de la organización a través de la dirección clara, del compromiso demostrado, la asignación explícita, y el reconocimiento de las responsabilidades de seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información	Las actividades de seguridad de la información deben coordinarse con representantes de diferentes partes de la organización, con soles y funciones de trabajo pertinentes.
A.6.1.3	Asignación de responsabilidades sobre seguridad de la información	Deben definirse claramente todas las responsabilidades de seguridad de la información.
A.6.1.4	Proceso de autoriza ión para los recursos de procesamiento de la información	Debe definirse e implementarse un proceso de autorización para cada nuevo recurso de procesamiento de la información.
A.6.1.5	Acuerdos de confidencialidad	Debe identificarse y regularmente revisarse los requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización, para la protección de la información,
A.6.1.6	Contacto con las autoridades	Deben mantenerse los contactos apropiados con las autoridades pertinentes.
A.6.1.7	Contacto con grupos interesados especiales	Deben mantenerse los contactos apropiados con grupos interesados especiales u otros foros de especialistas de seguridad y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la información y su implementación (es decir, objetivos de controles, políticas, procesos, y procedimientos para la seguridad información) deben revisarse de forma independiente, a intervalos planificados, o cuando ocurren cambios significativos en la implementación de la seguridad.
A.6.2 Partes externas **Objetivo: Mantener la seguridad de la información y recursos de procesamiento de la información de la organización que son accesados, procesados, comunicados, o gestionados por entidades o partes externas.**		
A.6.2.1	Identificación de riesgos relacionados a partes externas	Los riesgos a la información y recursos de procesamiento de la información de la organización, para los procesos del negocio que involucran partes externas, deben identificarse y deben implementarse los controles apropiados antes de otorgar el acceso.
A.6.2.2	Tratamiento de la seguridad en las	Todos los requisitos de seguridad identificados deben tratarse antes de dar el acceso al cliente a la información, o posesiones de la organización.

COD.	AGENTE A CONTROLAR	CONTROL
	relaciones con clientes	
A.6.2.3	Tratamiento de la seguridad en los acuerdos de terceras partes	Los acuerdos con usuarios de terceras partes que involucran acceder, procesar, comunicar o gestionar la información de la organización o los recursos para el tratamiento de la información, o agregar productos o servicios a recursos para el tratamiento de la información, deben cubrir todos los requisitos de seguridad pertinentes.
A.7 GESTIÓN DE ACTIVOS		
A.7.1 Responsabilidad por los activos **Objetivo: Alcanzar y mantener la protección apropiada de los activos de la organización.**		
A-7.1.1	Inventario de activos	Todos los activos deben identificarse claramente y elaborarse, y mantenerse el inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Toda información y activos asociados con las instalaciones de procesamiento de la información deben ser "dueño" por una parte J designada de la organización.
A.7.1.3	Utilización aceptable de los activos	Deben identificarse, documentarse e implementarse las reglas, para la utilización aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.
A.7.2 Clasificación de la información **Objetivo: Asegurar que la información reciba un nivel apropiado de protección.**		
A.7.2.1	Directrices de clasificación	La información debe clasificarse en relación con su valor, requisitos legales, sensibilidad y criticidad para la organización.
A.7.2.2	Etiquetado y manejo de la información	Un conjunto apropiado de procedimientos para etiquetar y manejar la información debe desarrollarse e implementarse de acuerdo con el esquema adoptado por la organización.
A.8 SEGURIDAD DE RECURSOS HUMANO		
A.8.1 Antes del empleo **Objetivo: Asegurar que los empleados, los contratistas y usuarios de terceras partes comprendan sus responsabilidades, y que sean apropiados para los roles considerados, y para reducir el riesgo del robo, fraude o mal uso de los, recursos.**		
A.8.1.1	Roles y responsabilidades	Los roles y responsabilidades de seguridad de los empleados contratistas y usuarios terceras partes deben definirse y documentarse de acuerdo con la política de seguridad de la información de la organización.
A.8.1.2	Selección	La verificación de los antecedentes sobre todos los candidatos para empleados, contratistas, y usuarios de terceras partes deben llevarse a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y proporcionales a los requisitos del negocio, a la clasificación de la información a ser acezada, y los riesgos percibidos,
A.8.1.3	Términos y condiciones de empleo	Como parte de su obligación contractual, los empleados contratistas y usuarios de terceras partes deben acordar y firmar los términos y condiciones de su contrato de trabajo, que debe declarar sus responsabilidades por la seguridad de la información de la organización.
A.8.2 Durante el empleo **Objetivo: Asegurar que todos los empleados, contratistas y usuarios de terceras partes son conscientes de las amenazas y aspectos relacionados con la seguridad de la información, sus responsabilidades y obligaciones, y**		

COD.	AGENTE A CONTROLAR	CONTROL
que estén equipados para respaldar la política de seguridad de la organización en el curso normal de su trabajo, y reducir el riesgo de error humano		
A.8.2.1	Responsabilidades de la dirección	La dirección debe requerir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos de la organización.
A.8.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización y, cuando sea pertinente, los contratistas y usuarios de terceras partes deben recibir la formación en toma de conciencia y las actualizaciones regulares apropiadas en las políticas y procedimientos de la organización como sea pertinente para su función de trabajo.
A.8.2.3	Proceso disciplinario	Debe haber un proceso disciplinario formal para los empleados quienes cometan un incumplimiento de seguridad.
A.8.3 Terminación o cambio de empleo **Objetivo: Asegurar que los empleados, contratistas y usuarios de terceras partes se retiran de una organización o cambian el empleo de una manera ordenada.**		
A.8.3.1	Responsabilidades de la terminación	Deben definirse y asignarse claramente las responsabilidades para llevar a cabo la terminación o cambio de empleo.
A.8.3.2	Devolución de los activos	Todos los empleados, contratistas y usuarios de terceras partes deben devolver todos los activos de la organización en su posesión, una terminado su empleo, contrato o acuerdo.
A.8.3.3	Retiro de los derechos de acceso	Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes a la información y recursos para el procesamiento de la información deben retirarse una vez terminado su empleo, contrato o acuerdo, o una vez ajustado el cambio.
A.9 SEGURIDAD FÍSICA Y AMBIENTAL		
A.9.1 Áreas seguras **Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones e información de la organización.**		
A.9.1.1	Perímetro de seguridad física	Los perímetros de seguridad (barreras tales como paredes, puertas de entrada controladas por tarjeta, o puesto de recepción manual) deben utilizarse para proteger las áreas que contienen la información, y las instalaciones de procesamiento de la información.
A.9.1.2	Controles físicos de entrada	Las áreas de seguridad deben estar protegidas por controles de entrada apropiados que aseguren el permiso de acceso sólo al personal autorizado
A.9.1.3	Seguridad de oficinas, habitaciones e instalaciones	Debe diseñarse y aplicarse la seguridad física para oficinas, habitaciones, e instalaciones.
A.9.1.4	Protección contra las amenazas externas y ambientales	Debe diseñarse y aplicarse la protección física contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre.
A.9.1.5	Trabajo en áreas seguras	Deben diseñarse y aplicarse la protección física y las directrices para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso al público, entrega y carga	Los puntos acceso, como las áreas de entrega y carga y otras donde las personas no autorizadas pueden entrar en las instalaciones, deben controlarse y, si es posible, aislarse de instalaciones de procesamiento de

COD.	AGENTE A CONTROLAR	CONTROL
		la información para evitar el acceso no autorizado.
A.9.2 Seguridad de los equipos Objetivo: Prevenir pérdidas, daños, robo o comprometer los activos e interrupción de las actividades de la organización.		
A.9.2.1	Ubicación y protección del equipo	El equipo debe ubicarse o protegerse para reducir los riesgos de amenazas y peligros ambientales, y oportunidades para el acceso no autorizado.
A.9.2.2	Servicio de apoyo	El equipo debe protegerse contra falla de energía y otras interrupciones eléctricas causadas por fallas en los servicios de apoyo.
A.9.2.3	Seguridad del cableado	El cableado de energía eléctrica y de comunicaciones, que transporta datos o brinda apoyo a los servicios de información debe protegerse contra interceptación o daño.
A.9.2.4	Mantenimiento de equipos	Los equipos deben mantenerse adecuadamente para asegurar si continúa disponibilidad e integridad.
A.9.2.5	Seguridad de equipos fuera de las instalaciones de la organización	Debe aplicarse la seguridad a los equipos exteriores teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.9.2.6	Seguridad en la reutilización o eliminación de equipos.	Todos los elementos del equipo que contengan dispositivos de almacenamiento de datos deben controlarse, para asegurar que cualquier dato sensible y software bajo licencia ha sido removido o tachado antes de su disposición.
A.9.2.7	Retiro de la propiedad	No deben sacar de las instalaciones, sin autorización, los equipos, la información o el software.
A.10 GESTIÓN DE COMUNICACIÓN Y OPERACIONES		
A.10.1 Procedimientos y responsabilidades de operación Objetivo: Asegurar la operación correcta y segura de los recursos de tratamiento de información.		
A.10.1.1	Documentación de procedimientos operativos	Los procedimientos operativos deben documentarse mantenerse, y estar disponibles a todos los usuarios que los necesitan.
A.10.1.2	Gestión de cambio	Deben controlarse los cambios para los recursos y sistemas de procesamiento de la información.
A.10.1.3	Segregación de tareas	Las tareas o áreas de responsabilidad deben segregarse para reducir las oportunidades de modificación no autorizada o mal uso de los activos de la organización.
A.10.1.4	Separación de los recursos para el desarrollo, prueba/ensayo y operación.	Deben separase los recursos para el desarrollo, prueba/ensayo y operación para reducir los riesgos del acceso no autorizado o cambios al sistema operativo.
A.10.2 Gestión de entrega de servicio de tercera parte Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicio de tercera parte.		
A.10.2.1	Entrega de servicio	Debe asegurarse que los controles de seguridad, las definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio de tercera parte son implementados, operados, y mantenidos por la tercera

COD.	AGENTE A CONTROLAR	CONTROL
		parte
A.10.2.2	Seguimiento y revisión de los servicios de tercera parte.	Los servicios, informes y registros suministrados por la tercera parte deben ser seguidos y revisados regularmente, y deben ser llevados a cabo auditorías regularmente.
A.10.2.3	Gestión de cambios para los servicios de tercera parte	Los cambios para el suministro de servicios, incluyendo el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de información existentes, deben gestionarse, tomando en cuenta la criticidad del sistemas del negocio y los procesos involucrados y la revaluación de-los riesgos.
A.10.3 Planificación y aceptación del sistema **Objetivo: Minimizar el riesgo de fallas de los sistemas.**		
A.10.3.1	Gestión de la capacidad	Deben realizarse seguimiento, ajustes, y proyecciones de los requisitos de la capacidad futura de la utilización de los recursos, para asegurar el desempeño del sistema requerido
A.10.3.2	Aceptación del sistema	Deben establecerse los criterios de aceptación para los nuevos sistemas de información y versiones nuevas o mejoradas y deben desarrollarse pruebas adecuadas de los sistemas durante el desarrollo y antes de la aceptación.
A.10.4 Protección contra código malicioso y movible **Objetivo: Proteger la integridad del software y de la información.**		
A.10.4.1	Controles contra código malicioso	Deben implantarse los controles de detección, prevención y recuperación para la protección contra código malicioso, y procedimientos adecuados de toma de conciencia de los usuarios.
A.10.4.2	Control contra código movible	Donde la utilización de código movible está autorizada, la configuración debe asegurar que el código movible autorizado opera de acuerdo con una política de seguridad claramente definida, y debe prevenirse el ejecutar el código movible no autorizado.
A.10.5 Copia de seguridad **Objetivo: Mantener la integridad y la disponibilidad de la información y los recursos de procesamiento de la información.**		
A.10.5.1	Copia de seguridad de la información	Las copias de seguridad de la información y software deben ser tomadas y probadas con regularidad de acuerdo con la política de copia de seguridad acordada.
A.10.6 Gestión de seguridad de la red **Objetivo: Asegurar la protección de la información en las redes y la protección de su infraestructura de soporte.**		
A.10.6.1	Controles de red	Las redes deben gestionarse y controlarse adecuadamente a fin de estar protegidas de las amenaza, y mantener la seguridad para los sistemas y aplicaciones que utiliza la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de servicios de red	Las características de seguridad, los niveles del servicio, y los requisitos de gestión de todos los servicios en red deben identificarse e incluirse en cualquier acordado de servicio de red, ya sea que estos servicios sean proporcionados en la empresa o subcontratados.
A.10.7 Manejo de medios de Información **Objetivo: Prevenirla divulgación, modificación, eliminación o destrucción no autorizada de los activos, e interrupción de las actividades del negocio.**		

COD.	AGENTE A CONTROLAR	CONTROL
A.10.7.1	Gestión de medios removibles	Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2	Disposición de medios	Cuando ya no son requeridos, los medios de información deben eliminarse de forma segura y sin peligro, utilizando procedimientos formales.
A.10.7.3	Procedimientos de manejo de la información	Se deben establecer procedimientos para el manejo y almacenamiento de la información para protegerla contra si, uso inadecuado o divulgación no autorizada.
A.10.7.4	Seguridad de la documentación de sistemas	La documentación de sistema debería protegerse contra el acceso no autorizado.
A.10.8 Intercambio de información **Objetivo: Mantener la seguridad de la información y el software intercambiado dentro de una organización y con cualquier entidad externa.**		
A.10.8.1	Políticas y procedimientos de intercambio de información	Deben establecerse políticas, procedimientos de intercambio formales, y controles para proteger el intercambio de información a través de la utilización de toda clase de recursos de comunicación
A.10.8.2	Acuerdos de intercambio	Deben establecerse acuerdos, para el intercambio de información y software entre la organización y partes externas.
A.10.8.3	Medios de información físicos en tránsito	Los medios que contienen la información deben protegerse contra el acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensaje electrónico	Debe estar apropiadamente protegida la información involucrada en el mensaje electrónico
A.10.8.5	Sistemas de información del negocio	Deben desarrollarse e implementarse las políticas y procedimiento para proteger la información asociada con la interconexión de los sistemas de información del negocio.
A.10.9 Servicios de comercio electrónico **Objetivo: Asegurar la seguridad de servicios de comercio electrónico, y su utilización segura.**		
A.10.9.1	Comercio electrónico	La información involucrada en la transferencia de comercio electrónico en redes públicas debe protegerse de la actividad fraudulenta, autorizada litigios contractuales, y la divulgación o modificación no rizada.
A.10.9.2	Transacciones en línea	La información involucrada en las transacciones en línea debe protegerse para prevenir la transmisión incompleta, pérdida de rutas, alteración de mensaje no autorizado, divulgación no autorizada y duplicación o repetición de mensaje no autorizada.
A.10.9.3	Información disponible públicamente	La integridad de la información que está disponible sobre un sistema disponible públicamente debe protegerse para prevenir la modificación no autorizada.
A.10.10 Seguimiento **Objetivo: Detectar las actividades de procesamiento de la información no autorizadas.**		
A.10.10.1	Registro de auditoría	Deben producirse y mantenerse los registros de auditorías que registren actividades, excepciones y eventos de seguridad de la información del usuario, durante un periodo definido para ayudar en futuras

COD.	AGENTE A CONTROLAR	CONTROL
		investigaciones y seguimiento del control de accesos.
A.10.10.2	Seguimiento de la utilización	Deben establecerse los procedimientos para el seguimiento de la utilización de los recursos de procesamiento de la información, y los resultados de las actividades de seguimiento revisadas regularmente.
A.10.10.3	Protección de la información del registro	Deben protegerse los recursos de registro e información de registro contra el acceso manipulado y no autorizado.
A.10.10.4	Administrador y operador del registro	Deben registrarse las actividades del administrador y el operador del sistema.
A.10.10.5	Registro de fallas	Las fallas deben registrarse, analizarse y tomarse las acciones apropiadas.
A.10.10.6	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de la información pertinentes, dentro de una organización o dominio de seguridad, deben sincronizarse con una fuente de tiempo exacta acordada.
A.11 CONTROL DE ACCESOS		
A.11.1 Requisitos del negocio para el control de accesos Objetivo: Controlar los accesos a la información.		
A.11.1.1	Política de con control de accesos	Debe establecerse, documentarse y revisarse una política de control de accesos, basada en los requisitos del negocio y de seguridad para el acceso.
A.11.2 Gestión de acceso de usuarios Objetivo: Asegurar el acceso del usuario autorizado y prevenir el acceso no autorizado a los sistemas de información.		
A.11.2.1	Registro de usuarios	Debe existir un procedimiento formal de registro o y des-registro o de usuarios para conceder y revocar el acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Deben restringirse y controlarse la utilización y la asignación de privilegios.
A.11.2.3	Gestión de contraseñas de usuario	Debe controlarse la asignación de contraseñas a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso de usuario	La dirección debe revisar los derechos de acceso de los usuarios a intervalos regulares, utilizando un proceso formal.
A.11.3 Responsabilidades de usuarios Objetivo: Prevenir el acceso de usuarios no autorizados, y comprometer o robar la información y los recursos de procesamiento de información.		
A.11.3.1	Uso de contraseñas	Debe requerirse a los usuarios seguir la; buenas prácticas de que requerirse seguridad para la selección y uso de sus contraseñas.
A.11.3.2	Equipo desatendido	Los usuarios deben asegurar que los equipos desatendidos estén debidamente protegidos.
A.11.3.3	Políticas de escritorios y pantallas limpias	Para los recursos de procesamiento de información, debe adoptarse una política de escritorios limpios de papel y de dispositivos de almacenamiento removibles, y una política de pantallas limpias.
A.11.4 Control de acceso a la red. Objetivo: Prevenir el acceso no autorizado a los servicios de red.		
A.11.4.1	Política de utilización de los servicios de red.	Los usuarios sólo deben tener acceso a los servicios que han sido específicamente autorizados a utilizar.
A.11.4.2	Autenticación de	Deben utilizarse métodos de autentificación apropiados para controlar el

COD.	AGENTE A CONTROLAR	CONTROL
	usuarios para conexiones externas	acceso por usuarios remotos.
A.11.4.3	Identificación de equipo en redes	Debe considerarse la identificación de equipo automático como un medio de autentificar las conexiones de ubicaciones y equipos específicos.
A.11.4.4	Protección del diagnóstico remoto y de la configuración de puerto	Debe controlarse el acceso físico y lógico para el diagnóstico y configuración de los puertos.
A.11.4.5	Segregación en redes	Deben segregarse los grupos de los servicios de información, los usuarios, y los sistemas de información en las redes.
A.11.4.6	Control de conexión de redes	Para redes compartidas, especialmente aquellas que atraviesan las fronteras de la organización, la capacidad de usuarios a conectarse a la red debe restringirse, de acuerdo con la política de control de acceso y los requisitos de las aplicaciones del negocio (véase apartado 11.1).
A.11.4.7	Control de direccionamiento en la red	Deben implementarse los controles de direccionamiento a redes, para asegurar que las conexiones entre computadora y los flujos de información no violen la política de control de acceso de las aplicaciones del negocio.
A.11.5 Control de acceso al sistema operativo Objetivo: Prevenir el acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de conexión segura.	Debe controlarse el acceso a los sistemas operativos por un procedimiento de conexión segura.
A.11.5.2	Identificación y autenticación del usuario	Todos los usuarios deben disponer de un identificador único (ID de usuario) sólo para su uso personal, y debe seleccionarse una técnica de autenticación adecuada, para probar la identidad declarada de un usuario.
A.11.5.3	Sistema de gestión de contraseñas	Los sistemas para la gestión de contraseñas deben ser interactivos, y deben asegurar la calidad de las contraseñas.
A.11.5.4	Utilización de las prestaciones del sistema.	Debe restringirse y controlarse estrechamente la utilización de programas de servicio que podrían ser capaces de eludir las medidas de control del sistema y de las aplicaciones.
A. 11.5.5	Sesión inactiva	Las sesiones inactivas deben cerrarse después de un período de inactividad definido.
A.11.5.6	Limitación de tiempo de conexión	Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control de acceso a las aplicaciones e información Objetivo: Prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación.		
A.11.6.1	Restricción de acceso a la información	El acceso a la información y a las funciones del sistema de aplicación por usuarios y personal de soporte debe restringirse, de acuerdo con la política de control de acceso definida.
A.11.6.2	Aislamiento de sistemas sensibles	Los sistemas sensibles deben tener un entorno informática dedicada (aislada).
A.11.7 Computación móvil y trabajo a distancia Objetivo Asegurar la seguridad de la información cuando se utilizan recursos de computación móvil y de trabajo a distancia		
A.11.7.1	Computación móvil y comunicaciones	Debe implantarse una política formal, y deben adoptarse las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar recursos

COD.	AGENTE A CONTROLAR	CONTROL
		de computación móvil y de comunicación.
A.11.7.2	Trabajo a distancia	Deben desarrollarse e implementarse políticas, planes operacionales y procedimientos para las actividades de trabajo a distancia.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE INFORMACIÓN		
A.12.1 Requisitos de seguridad de los sistemas de información **Objetivo: Asegurar que la seguridad es una parte integral de los sistemas de información.**		
A.12.1.1	Análisis y especificación de los requisitos de seguridad	Las declaraciones de los requisitos del negocio para los nuevos sistemas de información o mejoras a los sistemas de información existentes deben especificar los requisitos de control de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones **Objetivo: Prevenirlos errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.**		
A.12.2.1	Validación de datos de entrada	Deben validarse los datos de entrada a las aplicaciones para asegurarse de que éstos son correctos y apropiados.
A.12.2.2	Control del procesamiento interno	Deben incorporarse a las aplicaciones las comprobaciones de validación para detectar cualquier corrupción de la información a través de los errores de procesamiento o actos deliberados.
A.12.2.3	Integridad de mensaje	Deben identificarse los requisitos para asegurar la autenticidad y proteger la integridad de mensajes en aplicaciones, e identificarse e implementarse los controles apropiados.
A.12.2.4	Validación de los datos de salida	Deben validarse los datos de salida de una aplicación para asegurarse de que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.
A.12.3 Controles criptográficos **Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información por los medios criptográficos.**		
A.12.3.1	Política sobre la utilización de controles criptográficos	Debe desarrollarse e implementarse una política obre la utilización de controles criptográficos para la protección de la información.
A.12.3.2	Gestión de claves	Debe establecerse la gestión de clave para dar apoyo a la utilización por la organización de técnicas criptográficas.
A.12.4 Seguridad de los archivos del sistema **Objetivo: Asegurar la seguridad de los archivos del sistema**		
A.12.4.1	Control del software operativo	Deben existir procedimientos establecidos para controlar la instalación del software en sistemas en funcionamiento.
A.12.4.2	Protección de los datos de prueba del sistema	Deben seleccionarse cuidadosa mente y protegerse y controlarse los datos de prueba.
A.12.4.3	Control de acceso al código fuente del programa	Debe restringirse el acceso al código fuente del programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte **Objetivo: Mantener la seguridad del software y la información del sistema de aplicación.**		
A.12.5.1	Procedimientos de control de cambios	La implementación de los cambios debe ser controlada por la utilización de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de aplicaciones después de	Cuando los sistemas operativos son cambiados, deben revisarse y probarse las aplicaciones criticas del negocio para asegurarse de que no

COD.	AGENTE A CONTROLAR	CONTROL
	los cambios de sistema operativo	hay impacto adverso sobre las operaciones, o la seguridad de la organización.
A.12.5.3	Restricciones en los cambios a los paquetes de software.	Las modificaciones a paquetes de software deben ser desalentadas, limitadas a los cambios necesarios, y todo cambio debe controlarse estrictamente.
A.12.5.4	Fuga de información	Deben prevenirse las oportunidades de fuga de información
A.12.5.5	Desarrollo de software contratado externamente	La organización debe supervisar y realizar seguimiento al desarrollo de software contratado externamente.
A.12.6 Gestión de vulnerabilidad técnica **Objetivo: Reducir los riesgos que resultan de la exposición de las vulnerabilidades técnicas publicadas.**		
A.12.6.1	Control de las vulnerabilidades técnicas	Debe obtenerse la información oportuna sobre las vulnerabilidades técnicas del sistema de información que está siendo utilizado, evaluarse la exposición de la organización a tales vulnerabilidades, y tomarse las medidas apropiadas para tratar el riesgo asociado.
A.13 GESTIÓN DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN		
A.13.1 Reportar los eventos y debilidades de seguridad de la información **Objetivo: Asegurar que los eventos y debilidades de seguridad de la información asociadas con los sistemas de información sean comunicados de una manera tal que permita que la acción correctiva sea tomada oportunamente.**		
A.13.1.1	Reporte de los eventos de seguridad de información	Deben reportarse los eventos de seguridad de la información a través de los canales de gestión apropiados tan rápidamente como sea posible.
A.13.1.2	Reporte de debilidades de seguridad	Debe requerirse a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información, detectar e informar cualquier debilidad en la seguridad de los sistemas o servicios, que haya sido observada o sospechada.
A.13.2 Gestión de los incidentes y mejoras de seguridad de la información **Objetivo: Asegurar que un enfoque coherente y eficaz es aplicado a la gestión de los incidentes de seguridad de la información.**		
A.13.2.1	Responsabilidades y procedimientos	Deben establecerse las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información.
A.13.2.2	Aprendizaje de los incidentes de seguridad de la información	Deben establecerse mecanismos que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos do los incidentes de seguridad de información.
A.13.2.3	Recolección de evidencias	Cuando una acción de seguimiento contra a una persona u organización, después de un incidente de seguridad de la información que involucra acciones legales (civiles o criminales) deben recolectarse, conservarse y presentarse evidencias conforme a las reglas establecidas por la legislación aplicable, o por el tribunal que sigue el caso.
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
A.14.1 Aspectos de seguridad de la información de la gestión de continuidad de¡ negocio **Objetivo: Contrarrestar las interrupciones de las actividades de] negocio y proteger los procesos críticos os del negocio de los efectos de fallas significativas o desastres de los sistemas de información, y asegurar su reanudación oportuna.**		

COD.	AGENTE A CONTROLAR	CONTROL
A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Un proceso dirigido debe ser cesar ollado y manteniendo para la continuidad del negocio, a través de la organización que trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.
A.14.1.2	Continuidad del negocio y evaluación del riesgo	Los eventos que pueden causar interrupciones a los procesos del negocio deben identificarse al mismo tiempo que la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollar e implementar planes de continuidad que incluyan la seguridad de la información.	Deben desarrollarse e implementarse planes para mantener y recuperar las operaciones y asegurar la disponibilidad de la información al nivel requerido y en los plazos requeridos, tras la interrupción o la falla en los procesos críticos del negocio.
A.14.1.4	Marco de planificación para la continuidad del negocio	Se debe mantener un esquema único de planes de continuidad del negocio, para asegurar que dichos planes son coherentes, para tratar coherentemente los requisitos de seguridad de la información y para identificar las prioridades de prueba y mantenimiento.
A.14.1.5	Prueba, mantenimiento y revaluación de los planes de continuidad del negocio.	Deben probarse y actualizar con regularidad los planes de continuidad del negocio, para asegurarse de su actualización y eficacia.
A.15 CUMPLIMIENTO		
A.15.1 Cumplimiento de requisitos legales **Objetivo: Evitar incumplimientos de cualquier ley, estatuto, obligación, reglamentarios o contractuales, y de cualquier requisito de seguridad.**		
A.15.1.1	Identificación de la legislación aplicable.	Deben definirse, documentarse y mantenerse actualizados todos los requisitos legales, reglamentarios y contractuales pertinentes y el enfoque de la organización que cumplan estos requisitos para cada sistema de información y de la organización.
A.15.1.2	Derechos de propiedad intelectual (DPI)	Cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material protegido por derechos de propiedad intelectual, y sobre el uso de productos de software reservados.
A.15.1.3	Protección de los registros de la organización.	Deben protegerse los registros importantes contra pérdida, destrucción y falsificación, de acuerdo con los requisitos legales, estatutarios, reglamentarios y contractuales y del negocio.
A.15.1.4	Protección de datos y de la privacidad de la información personal.	Deben asegurarse la protección de datos y la privacidad como sea requerido en la legislación, las reglamentaciones pertinentes, y, si es aplicable, en las cláusulas contractuales.
A.15.1.5	Prevención del mal uso de los recursos de procesamiento de la información	Debe disuadirse a los usuarios de utilizar los recursos de procesamiento de la información para propósitos no autorizados.
A.15.1.6	Regulación de controles criptográficos.	Deben utilizarse los controles criptográficos en cumplimiento con todos los acuerdos, leyes, y regulaciones pertinentes.
A.15.2 Cumplimiento con las políticas y normas de seguridad y el cumplimiento técnico **Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad de la organización.**		
A.15.2.1	Cumplimiento con las	Los gerentes deben asegurar que todos los procedimientos de seguridad

COD.	AGENTE A CONTROLAR	CONTROL
	políticas y normas de seguridad.	dentro de su área de responsabilidad son llevados a cabo correctamente, para alcanzar el cumplimiento con las normas y políticas de seguridad.
A.15.2.2	Comprobación del cumplimiento técnico.	Debe comprobarse regularmente la compatibilidad de los sistemas de información con las normas de implementación de seguridad.
A.15.3 Consideraciones de auditoría de los sistemas de información **Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema de la información.**		
A.15.3.1	Control de auditoría de los sistemas de información.	Deben planificarse cuidadosamente y acordarse los requisitos y actividades de auditoría que involucren comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Debe protegerse el acceso a las herramientas de auditoría del sistema de información para prevenir cualquier posible mal uso o compromiso.

Tabla 52: Listado de controles según ISO 27000.

ix. Preparación de la declaración de aplicabilidad.

La declaración de aplicabilidad es un documento importante que la clausula 4.2.1 (j) exige. Todos los objetivos de control y controles forman parte de la declaración de aplicabilidad y se debe de hacer una breve explicación de las razones para su selección (de acuerdo a los objetivos que se persiguen). También deben de incluirse los objetivos de control y controles existentes, si es que existiesen, y detallarse la exclusión de cualquier objetivo de control y controles con su respectiva explicación. La razón la declaración de aplicabilidad es proporcionar un chequeo a la empresa para que se cerciore de que no haya omitido ningún control. A continuación se presenta la declaración de aplicabilidad que se ha diseñado para La Comisión, cabe decir que en la actualidad CEL no cuanta con objetivos de control y controles por lo que se presenta solamente para los objetivos de control y controles expuestos en anterioridad.

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD		JUSTIFICACIÓN
		SI	NO	
A.5.1 Política de seguridad de la Información	A.5.1.1	x		Dar cumplimiento y brindar soporte a la gestión de la seguridad de la información, de acuerdo con los requisitos de CEL, las leyes y reglamentos pertinentes.
	A.5.1.2	X		
A.6.1 Organización interna	A.6.1.1	X		Al aplicar estos controles efectivamente lograremos gestionar la seguridad de la información dentro de la organización
	A.6.1.2	X		
	A.6.1.3	X		
	A.6.1.4	X		
	A.6.1.5	X		
	A.6.1.6	X		
	A.6.1.7	X		

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD		JUSTIFICACIÓN
		SI	NO	
	A.6.1.8	X		
A.6.2 Partes externas	A.6.2.1	X		Al aplicar estos controles efectivamente lograremos mantener la seguridad de la información y recursos de procesamiento de la información de la organización que son accesados, procesados, comunicados, o gestionados por entidades o partes externas.
	A.6.2.2	X		
	A.6.2.3	X		
A.7.1 Responsabilidad por los activos	A-7.1.1	X		Al aplicar estos controles efectivamente lograremos alcanzar y mantener la protección apropiada de los activos de la organización.
	A.7.1.2	X		
	A.7.1.3	X		
A.7.2 Clasificación de la información	A.7.2.1	X		Al aplicar estos controles efectivamente lograremos asegurar que la información reciba un nivel apropiado de protección.
	A.7.2.2	X		
A.8.1 Antes del empleo	A.8.1.1	X		Asegurar que los empleados, los contratistas y usuarios de terceras partes comprendan sus responsabilidades, y que sean apropiados para los roles considerados, y para reducir el riesgo del robo, fraude o mal uso de los, recursos.
	A.8.1.2	X		
	A.8.1.3	X		
A.8.2 Durante el empleo	A.8.2.1	X		Al aplicar estos controles efectivamente lograremos asegurar que todos los empleados, contratistas y usuarios de terceras partes son conscientes de las amenazas y aspectos relacionados con la seguridad de la información, sus responsabilidades y obligaciones, y que estén equipados para respaldar la política de seguridad de la organización en el curso normal de su trabajo, y reducir el riesgo de error humano
	A.8.2.2	X		
	A.8.2.3	X		
A.8.3 Terminación o cambio de empleo	A.8.3.1	X		Al aplicar estos controles efectivamente lograremos asegurar que los empleados, contratistas y usuarios de terceras partes se retiran de una organización o cambian el empleo de una manera ordenada.
	A.8.3.2	X		
	A.8.3.3	X		
A.9.1 Áreas seguras	A.9.1.1	X		Al aplicar estos controles efectivamente lograremos prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones e información de la organización.
	A.9.1.2	X		
	A.9.1.3	X		
	A.9.1.4	X		
	A.9.1.5	X		
	A.9.1.6	X		
A.9.2 Seguridad de los equipos	A.9.2.1	X		Al aplicar estos controles efectivamente lograremos prevenir pérdidas, daños, robo o comprometer los activos e interrupción de las actividades de la organización.
	A.9.2.2	X		
	A.9.2.3	X		
	A.9.2.4	X		
	A.9.2.5	X		
	A.9.2.6	X		
	A.9.2.7	X		
A.10.1 Procedimientos y responsabilidades de	A.10.1.1	X		Al aplicar estos controles efectivamente lograremos asegurar la operación correcta y segura de los recursos de tratamiento
	A.10.1.2	X		

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD		JUSTIFICACIÓN
		SI	NO	
operación	A.10.1.3	X		de información.
	A.10.1.4	X		
A.10.2 Gestión de entrega de servicio de tercera parte	A.10.2.1	X		Al aplicar estos controles efectivamente lograremos implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicio de tercera parte.
	A.10.2.2	X		
	A.10.2.3	X		
A.10.3 Planificación y aceptación del sistema	A.10.3.1	X		Al aplicar estos controles efectivamente lograremos minimizar el riesgo de fallas de los sistemas.
	A.10.3.2	X		
A.10.4 Protección contra código malicioso y movible	A.10.4.1	X		Al aplicar estos controles efectivamente lograremos proteger la integridad del software y de la información.
	A.10.4.2	X		
A.10.5 Copia de seguridad	A.10.5.1	X		Al aplicar estos controles efectivamente lograremos mantener la integridad y la disponibilidad de la información y los recursos de procesamiento de la información.
A.10.6 Gestión de seguridad de la red	A.10.6.1	X		Al aplicar estos controles efectivamente lograremos asegurar la protección de la información en las redes y la protección de su infraestructura de soporte.
	A.10.6.2	X		
A.10.7 Manejo de medios de Información	A.10.7.1	X		Al aplicar estos controles efectivamente lograremos prevenirla divulgación, modificación, eliminación o destrucción no autorizada de los activos, e interrupción de las actividades del negocio.
	A.10.7.2	X		
	A.10.7.3	X		
	A.10.7.4	X		
A.10.8 Intercambio de información	A.10.8.1	X		Al aplicar estos controles efectivamente lograremos mantener la seguridad de la información y el software intercambiado dentro de una organización y con cualquier entidad externa.
	A.10.8.2	X		
	A.10.8.3	X		
	A.10.8.4	X		
	A.10.8.5	X		
A.10.9 Servicios de comercio electrónico	A.10.9.1		X	Al aplicar estos controles efectivamente lograremos asegurar la seguridad de servicios de comercio electrónico, y su utilización segura. El control que no se aplicara se debe a que por el tipo de negocio de CEL el comercio no se realiza de forma electrónica.
	A.10.9.2	X		
	A.10.9.3	X		
A.10.10 Seguimiento	A.10.10.1	X		Al aplicar estos controles efectivamente lograremos detectar las actividades de procesamiento de la información no autorizadas.
	A.10.10.2	X		
	A.10.10.3	X		
	A.10.10.4	X		
	A.10.10.5	X		
	A.10.10.6	X		
A.11.1 Requisitos del negocio para el control de accesos	A.11.1.1	X		Al aplicar estos controles efectivamente lograremos controlar los accesos a la información.
A.11.2 Gestión de acceso de usuarios	A.11.2.1	X		Al aplicar estos controles efectivamente lograremos asegurar el acceso del usuario autorizado y prevenir el acceso no
	A.11.2.2	X		

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD		JUSTIFICACIÓN
		SI	NO	
	A.11.2.3	X		autorizado a los sistemas de información.
	A.11.2.4	X		
A.11.3 Responsabilidades de usuarios	A.11.3.1	X		Al aplicar estos controles efectivamente lograremos prevenir el acceso de usuarios no autorizados, y comprometer o robar la información y los recursos de procesamiento de información.
	A.11.3.2	X		
	A.11.3.3	X		
A.11.4 Control de acceso a la red.	A.11.4.1	X		Al aplicar estos controles efectivamente lograremos prevenir el acceso no autorizado a los servicios de red.
	A.11.4.2	X		
	A.11.4.3	X		
	A.11.4.4	X		
	A.11.4.5	X		
	A.11.4.6	X		
	A.11.4.7	X		
A.11.5 Control de acceso al sistema operativo	A.11.5.1	X		Al aplicar estos controles efectivamente lograremos prevenir el acceso no autorizado a los sistemas operativos.
	A.11.5.2	X		
	A.11.5.3	X		
	A.11.5.4	X		
	A. 11.5.5	X		
	A.11.5.6	X		
A.11.6 Control de acceso a las aplicaciones e información	A.11.6.1			Al aplicar estos controles efectivamente lograremos prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación.
	A.11.6.2	X		
A.11.7 Computación móvil y trabajo a distancia	A.11.7.1	X		Al aplicar estos controles efectivamente lograremos asegurar la seguridad de la información cuando se utilizan recursos de computación móvil y de trabajo a distancia, el control que no se toma es porque de acuerdo a la normativa de CEL, no se permite realizar trabajo a distancia, todo tiene que realizarse dentro de las instalaciones y oficinas
	A.11.7.2		X	
A.12.1 Requisitos de seguridad de los sistemas de información	A.12.1.1	X		Al aplicar estos controles efectivamente lograremos asegurar que la seguridad es una parte integral de los sistemas de información.
A.12.2 Procesamiento correcto en las aplicaciones	A.12.2.1	X		Al aplicar estos controles efectivamente lograremos prevenirlos errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.
	A.12.2.2	X		
	A.12.2.3	X		
	A.12.2.4	X		
A.12.3 Controles criptográficos	A.12.3.1	X		Al aplicar estos controles efectivamente lograremos proteger la confidencialidad, autenticidad o integridad de la información por los medios criptográficos.
	A.12.3.2	X		
A.12.4 Seguridad de los archivos del sistema	A.12.4.1	X		Al aplicar estos controles efectivamente lograremos asegurar la seguridad de los archivos del sistema
	A.12.4.2	X		
	A.12.4.3	X		
A.12.5 Seguridad en los procesos de desarrollo y	A.12.5.1	X		Al aplicar estos controles efectivamente lograremos mantener la seguridad del software y la información del sistema de
	A.12.5.2	X		

OBJETIVOS DE CONTROL	CONTROLES	APLICABILIDAD		JUSTIFICACIÓN
		SI	NO	
soporte	A.12.5.3	X		aplicación.
	A.12.5.4	X		
	A.12.5.5	X		
A.12.6 Gestión de vulnerabilidad técnica	A.12.6.1	X		Al aplicar estos controles efectivamente lograremos reducir los riesgos que resultan de la exposición de las vulnerabilidades técnicas publicadas.
A.13.1 Reportar los eventos y debilidades de seguridad de la información	A.13.1.1	X		Al aplicar estos controles efectivamente lograremos asegurar que los eventos y debilidades de seguridad de la información asociadas con los sistemas de información sean comunicados de una manera tal que permita que la acción correctiva sea tomada oportunamente.
	A.13.1.2	X		
A.13.2 Gestión de los incidentes y mejoras de seguridad de la información	A.13.2.1	X		Al aplicar estos controles efectivamente lograremos asegurar que un enfoque coherente y eficaz es aplicado a la gestión de los incidentes de seguridad de la información.
	A.13.2.2	X		
	A.13.2.3	X		
A.14.1 Aspectos de seguridad de la información de la gestión de continuidad de¡ negocio	A.14.1.1	X		Al aplicar estos controles efectivamente lograremos contrarrestar las interrupciones de las actividades de] negocio y proteger los procesos críticos os del negocio de los efectos de fallas significativas o desastres de los sistemas de información, y asegurar su reanudación oportuna.
	A.14.1.2	X		
	A.14.1.3	X		
	A.14.1.4	X		
	A.14.1.5	X		
A.15.1 Cumplimiento de requisitos legales	A.15.1.1	X		Al aplicar estos controles efectivamente lograremos evitar incumplimientos de cualquier ley, estatuto, obligación, reglamentarios o contractuales, y de cualquier requisito de seguridad
	A.15.1.2	X		
	A.15.1.3	X		
	A.15.1.4	X		
	A.15.1.5	X		
	A.15.1.6	X		
A.15.2 Cumplimiento con las políticas y normas de seguridad y el cumplimiento técnico	A.15.2.1	X		Al aplicar estos controles efectivamente lograremos asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad de la organización.
	A.15.2.2	X		
A.15.3 Consideraciones de auditoría de los sistemas de información	A.15.3.1	X		Al aplicar estos controles efectivamente lograremos maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema de la información.
	A.15.3.2			

Tabla 53: Declaración de aplicabilidad de los controles.

6. Declaración de documentación del SGSI

La documentación del sistema se basa en la pirámide documental descrita en la teoría de la ISO 27001:2005. A continuación se mencionan los documentos que dan soporte al SGSI.

- Manual de Seguridad de la Información.

- Metodología para la Continuidad y contingencia del negocio. }
- Procedimientos normativos
- Procedimientos operativos
- Formularios

En los apartados siguientes se presentan cada uno de ellos a excepción de los procedimientos normativos pues ellos quedaran a discreción de CEL cuando ya se este implementando el SGSI, en este apartado solo se presenta una lista de procedimientos operáticos PRS O recomendados para dar soporte a los PRS N.

a. Procedimientos Normativos

CÓDIGO	NOMBRE
PRSN-001	Procedimiento para la preparación de documentos del SGSI
PRSN-002	Procedimiento para el control de documentos del SGSI
PRSN-003	Procedimiento para la Preparación de Fichas de Proceso de Seguridad y Seguimiento de Puntos de Control
PRSN-004	Procedimiento para el mantenimiento de requisitos de seguridad de la información de documentos del SGSI
PRSN-005	Procedimiento de planificación de auditorías internas del SGSI
PRSN-006	Procedimiento para acciones preventivas y correctivas del SGSI
PRSN-008	Procedimiento de Gestión de Debilidades, Incidentes, Problemas y Violaciones de Seguridad de la Información
PRSN-009	Procedimiento para la Revisión del SGSI por la Dirección
PRSN-0010	Procedimiento para la clasificación y marcado de la información del SGSI

Tabla 54: Declaración Procedimientos Normativos.

b. Propuesta de Procedimientos Operativos

CÓDIGO	NOMBRE	OBJETIVO
PRSO 001	**ELIMINACION DE INFORMACION CONFIDENCIAL O SENSIBLE DE EQUIPOS CLIENTES O DISPOSITIVOS EXTERNOS DE ALMACENAMIENTO**	Describir los pasos a seguir para la eliminacion de información CONFIDENCIAL O SENSIBLE en los dispositivos de Almacenamiento, soportes magnéticos, ópticos u otros medios extraibles
PRSO 002	**ELIMINACION DE INFORMACION CONFIDENCIAL O SENSIBLE EN EQUIPOS SERVIDORES O DISPOSITIVOS DE ALMACENAMIENTO CENTRALES**	Describir los pasos a seguir para la eliminacion de información CONFIDENCIAL O SENSIBLE en los dispositivos de Almacenamiento, soportes magnéticos, ópticos u otros medios extraibles en los equipos servidores centrales
PRSO 03	**ELIMINACIÓN DE INFORMACIÓN CONFIDENCIAL O SENSIBLE EN LOS EQUIPOS DE COMUNICACIÓN Y CONEXOS**	Definir los pasos a seguir para la eliminación de la información confidencial o sensible residente en los equipos de comunicación
PRSO 04	**CONTROL DE SOFTWARE EN EQUIPOS CLIENTES ASIGNADOS A PERSONAL DE**	Describir los pasos a seguir para el control del software de la infraestructura cliente, que lleve a

	CEL	la estandarización del mismo, en cada una de las áreas que conforman CEL
PRSO 05	**ESCANEO DE VULNERABILIDADES EN SERVICIOS DE RED EN EQUIPOS CLIENTE Y SERVIDORES**	Definir los pasos a seguir para el escaneo de vulnerabilidades en servicios de red en equipos cliente y servidores, de tal forma que sean comunicados en una manera oportuna, permitiendo tomar las acciones correctivas para solventar las vulnerabilidades detectadas, eliminando las brechas de seguridad de la información en los mismos.
PRSO 06	**REVISION DE VULNERABILIDADES DE SISTEMAS OPERATIVOS WINDOWS, LINUX Y APLICATIVO DE BASE DE DATOS**	Definir los pasos a seguir para la revisión de vulnerabilidades de seguridad asociadas a los sistemas operativos Windows, Linux y aplicativo de base de datos, de tal forma que sean comunicados en una manera oportuna, permitiendo tomar las acciones correctivas para solventar las vulnerabilidades detectadas, eliminando las brechas de seguridad de la información en los mismos
PRSO 07	**REVISION DE VULNERABILIDADES DE SISTEMAS OPERATIVOS WINDOWS (CLIENTES), SOFTWARE DE ADMINISTRACION Y HELP DESK**	Definir las acciones a seguir para minimizar las vulnerabilidades de seguridad en los equipos clientes asociadas a los sistemas operativos Windows (cliente), Software de Oficina (MS Office) y Antivirus ejecutando tareas de remediación de manera oportuna
PRSO 08	**CAMBIO Y RESGUARDO DE CONTRASEÑAS DE SERVIDORES**	Ddocumentar y poseer en un lugar seguro las contraseñas del usuario administrador de los servidores o de las aplicaciones que administra el Área de Asistencia Tecnológica.
PRSO 09	**ELIMINACIÓN DE INFORMACIÓN CONFIDENCIAL O SENSIBLE EN LOS EQUIPOS DE COMUNICACIÓN Y CONEXOS**	Definir los pasos a seguir para la eliminación de la información confidencial o sensible residente en los equipos de comunicación y conexos administrados por el Área de Redes y Telecomunicaciones de

Tabla 55: Declaración de Procedimientos Operativos

NOTA: A continuación se presentan las generalidades de los documentos normativos diseñados en la propuesta del Sistema de Gestión del Manejo y Seguridad de la Información bajo las normas ISO 27000.
Para CEL dichos documentos son de carácter confidencial por lo que se recomienda que para usos didácticos se consulten en su formato completo en las Oficinas Centrales de CEL en la Unidad de Gestión Integrada, ubicado en la Alameda Juan Pablo II, Centro de Gobierno de El Salvador, Tel 2211 6000

B. OPERAR EL SGSI

La fase de operación se refiere a la actuación y funcionamiento permanente del SGSI para ello se recomienda revisar la Figura 44 de la página 272 donde se describe el proceso de operación permanente del SGSI y la tabal 69 de la pagina 274 que nos describe el proceso antes mencionado.

1. Elaboración del Plan de Tratamiento de Riesgos

Una vez que se han tomado las decisiones relacionadas con el tratamiento de riesgo, las actividades para poder implantar estas decisiones tienen que ejecutarse. Para este fin hay que identificar y plantear las actividades. Cada actividad de debe de ser identificada con claridad para poder distribuir las responsabilidades a las personas, estimar los requerimientos de recursos, el conjunto de entregables, las fechas críticas y la supervisión del mismo.

En esencia, la implantación del plan de tratamiento de riesgo se convierte en una fase del proyecto. La Comisión debe hacer hincapié en asignar a la persona idónea para responsabilizarla de esta fase, visualizar los recursos necesarios y manejar los reforzadores de conducta organizacional, que aseguren el correcto desempeño de la misma.

Las actividades consideradas vitales, cuando se formula un plan de tratamiento de riesgo, son las siguientes:

1. Identificar, con la precisión requerida, los factores limitadores del proyecto y establecer la estrategia para debilitarlos.

   Para este proyecto las limitantes son la falta de información de los empleados sobre los SGSI y las normas ISO 27001:2005 y la estrategia para debilitar esta limitante es desarrollar una serie de talleres para divulgar conocimiento sobre la Seguridad de la información.
2. Establecer las prioridades del proyecto

   La prioridad es desarrollar una evaluación del riego para determinar a partir del análisis del mismo los controles y objetivos de control a diseñar para su contrarresto
3. Identificar con claridad las fechas de entrega, lo mismo que los responsables del proyecto.

   Para ello se desarrollara a continuación el diagrama de Gantt, en el encontraremos las fechas y responsables de llevar a cabo cada actividad.
4. Estimar los requerimientos de recursos y a la vez identificar los recursos

   Para ello se requiere recursos humanos, el personal será el que actualmente posee la Unidad de Gestión integrada en CEL, utilizando las instalaciones y equipo que poseen en las oficinas.
5. Identificar el tiempo del proyecto.

   De a cuerdo a la duración del proyecto el tiempo estimado para su inicio sea la primera semana de mayo y finalice la primera semana de octubre. Esto con un total de 22 semanas la cual a la vez en la ruta critica del proyecto.

En el siguiente cuadro se muestran las actividades del plan de tratamiento de riesgo para La Comisión.

No.	Actividades	Fecha de inicio	Fecha de finalización	Duración	Responsable
1	Desarrollar una capacidad para localizar, evaluar y utilizar la información en todos	04/05/09	15/05/09	2 semanas	Unidad de Gestión Integrada

No.	Actividades	Fecha de inicio	Fecha de finalización	Duración	Responsable
	los procesos y sobre seguridad de información ISO 27001:2005				
2	Diseñar controles definidos para el manejo y seguridad de la información	18/05/09	22/05/09	1 semana	Unidad de Gestión Integrada
3	Dictaminar y diseñar políticas para resguardo de documentos	18/05/09	22/05/09	1 semana	Unidad de Gestión Integrada
4	Concientizar a los empleados sobre la importancia de la seguridad de la Información.	25/05/09	29/05/09	1 semana	Unidad de Gestión Integrada
5	Reunirse con los Jefes de los procesos críticos para determinar controles necesarios para atacar los riesgos	01/06/09	5/06/09	1 semanas	Unidad de Gestión Integrada
6	Diseñar Controles de y Objetivos de control	05/06/09	19/06/09	2 semanas	Unidad de Gestión Integrada
7	Implantar y socializar los controles y objetivos de control	05/06/09	19/06/09	2 semanas	Unidad de Gestión Integrada
8	Asignar recursos destinados para el manejo y seguridad de la información	22/06/09	26/06/09	1 semana	Unidad de Gestión Integrada
9	Elaborar mecanismos de monitoreo	29/06/09	17/07/09	3 semanas	Unidad de Gestión Integrada
10	Definir puntos de resguardo de la información	20/07/09	24/07/09	1 semana	Unidad de Gestión Integrada
11	Diseñar un manual para el manejo y seguridad de la información en todas las Unidades	27/07/09	14/08/09	3 semanas	Unidad de Gestión Integrada
12	Realizar auditorias que verifiquen el manejo y seguridad de la información	17/08/09	28/08/09	2 semanas	Unidad de Gestión Integrada
13	Elaborar mecanismos de mejora para el proyecto.	31/08/09	11/09/09	2 semanas	Unidad de Gestión Integrada
14	Aplicar mecanismos de mejora continua.	14/09/09	18/09/09	1 semana	Unidad de Gestión Integrada
15	Divulgar acciones y modificaciones hechas al SGSI	21/09/09	25/09/09	1 semana	Unidad de Gestión Integrada
16	Realizar simulacros para resguardo de información	28/09/09	2/10/09	1 semana	Unidad de Gestión Integrada

Tabla 56: Plan de tratamiento de riesgos

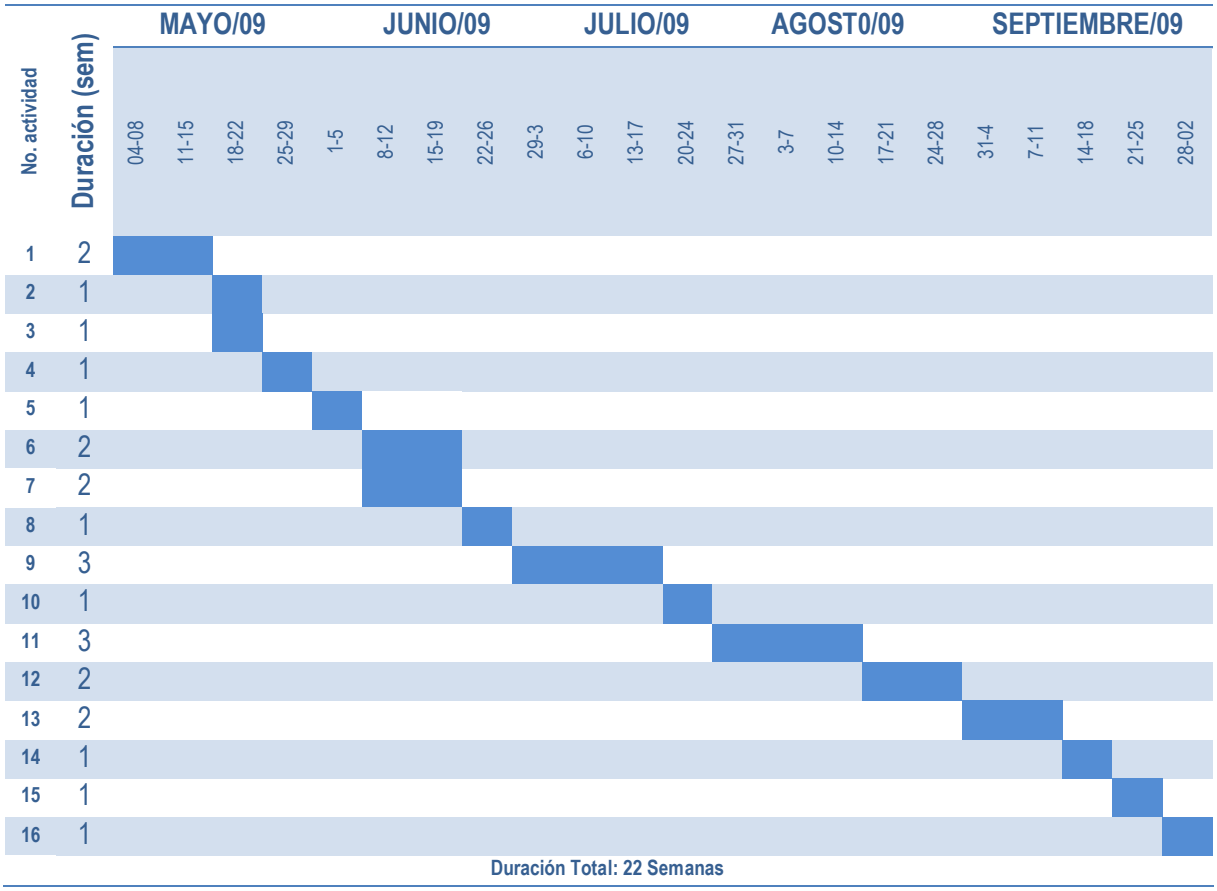


Grafico 9: Programación de actividades del plan de tratamiento de riesgos

Una vez se ha formulado el plan de tratamiento de riesgos, se deben de asignar los recursos y las acciones correspondientes para implementar las decisiones de la gestión del riesgo que deben iniciarse, este apartado queda a discreción de la gerencia pues nuestro trabajo se limito a formular hasta el punto de una programación de actividades, no obstante se recomienda que se cumplan las demás actividades que todo proyecto requiere para su puesta en marcha. En la clausula 4.2.2 (a), el ISO 27001:2005 plantea las exigencias para desarrollar el plan de tratamiento de riesgo.

2. **Elaboración del Manual de Seguridad de la Información**

Comisión Ejecutiva Hidroeléctrica Del Rio Lempa

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

HOJA DE AUTORIZACIÓN

Preparado por:

Nombre : Firma: Fecha:
Cargo :

Revisado por:

Nombre : Firma: Fecha:
Cargo :

Nombre : Firma: Fecha:
Cargo :

Aprobado por:

Nombre : Firma: Fecha:
Cargo :

CONTENIDO

1.1 INTRODUCCIÓN

"**La seguridad de la información** es la preservación de la confidencialidad, integridad y disponibilidad de la información; en adición, otras propiedades, como la autenticidad, responsabilidad, no-repudiación y fiabilidad pueden estar involucradas". Aunque se puede generar la tendencia que los controles asociados a la seguridad de la información solo están orientados a sistemas de "informática", es importante aclarar que se consideran todos los aspectos relacionados con la información, los medios y los sistemas que la manejan y la soportan.

Los sistemas de información y las redes de las Organizaciones están frente a amenazas de un gran número de fuentes, incluyendo fraudes por computadora, espionaje, sabotaje, vandalismo, incendios o inundaciones. Asimismo, causas de daño como códigos maliciosos, "hacking", ataques de denegación de servicios se hacen ahora más frecuentes y sofisticadas.

La seguridad que puede ser lograda a través de medios tecnológicos es limitada y debe estar soportada por procedimientos y una gestión apropiada. Identificar los controles que deben estar implementados requiere una cuidadosa planificación y detalle. La gestión de la seguridad de la información requiere la participación de las máximas autoridades, los empleados de la Institución, proveedores, terceras partes, contribuyentes, y otros.

Sistema de Gestión de Seguridad de la Información (SGSI)

Un sistema de gestión de seguridad de la información incluye la estructura organizacional, políticas, planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos; el cual, parte de un enfoque al riesgo del negocio, para establecer, implementar, operar, monitorear, revisar, mantener, y mejorar la seguridad de la información.

Fases del Sistema de Seguridad de la información

Las fases fundamentales del desarrollo y mantenimiento del sistema, basadas en el ciclo PHVA son:

- **Planificar (Establecimiento del SGSI):** Esta fase comprende la política de seguridad, objetivos, procesos y procedimientos relevantes a la gestión de riesgos y mejorar la seguridad de la información para obtener resultados de acuerdo a los objetivos y políticas de la Institución
- **Hacer (Implantación y operación):** En esta fase se Implanta y opera la política, controles, procesos y procedimientos del SGSI.
- **Verificación (Seguimiento y revisión del SGSI):** Esta fase considera la evaluación y donde sea aplicable, medir el desempeño de los procesos contra la política, objetivos y experiencia práctica del SGSI y reportar los resultados a la Dirección para su revisión.
- **Actuar (Mantenimiento y mejora el SGSI):** Comprende la realización acciones preventivas y correctivas, basadas en los resultados de las auditorias internas, la gestión y la revisión de la información relevante para alcanzar la mejora continua del SGSI.

1.2 OBJETIVOS

- Evaluar y gestionar constantemente los riesgos asociados a la información y los medios de tratamientos de ésta a través del cumplimiento de estos lineamientos y otra documentación del SGSI.
- Gestionar y dar continuidad a los servicios que presta CEL.
- Adoptar las mejores prácticas y estándares internacionales para proteger la información de los riesgos asociados.
- Evaluar, revisar y mejorar de forma continua las normas, procedimientos y demás herramientas para garantizar una seguridad razonable de la información de la Institución.
- Divulgar a los funcionarios y empleados la importancia del cumplimiento a las disposiciones contenidas en este manual y otros documentos del SGSI.
- Contribuir al cumplimiento de las normas y legislación vigente en materia de seguridad de la información.
- Proporcionar el detalle de los requisitos para establecer, implantar, operar, monitorear, revisar, mantener y mejorar el SGSI.
- Establecer las responsabilidades de las Dependencias y Unidades Organizativas involucradas en ciclo de desarrollo y mantenimiento del SGSI.
- Enunciar la documentación necesaria del SGSI.

3. Elaboración del procedimiento para la preparación de documentos del SGSI PRSN-001

Título:

PREPARACION DE DOCUMENTOS DEL SGSI

Preparado por :

Nombre: **Cargo :**	Firma:	Fecha:

Revisado por:

Nombre: **Cargo :**	Firma:	Fecha:
Nombre: **Cargo :**	Firma:	Fecha:

Aprobado por:

Nombre: **Cargo :**	Firma:	Fecha:

Contenido:

Observaciones:

Copia Controlada No._____

1. OBJETIVO

Establecer la metodología para la elaboración de los Documentos del Sistema de Gestión de Seguridad de la Información (SGSI) de CEL.

4. Elaboración del procedimiento para el control de documentos del SGSI PRSN-002

Titulo :

CONTROL DE DOCUMENTOS DEL SGSI

Preparado por :

Nombre : Firma: Fecha:
Cargo :

Revisado por:

Nombre: Firma: Fecha:
Cargo :

Nombre: Firma: Fecha:
Cargo :

Aprobado por:

Nombre: Firma: Fecha:
Cargo :

Contenido:

1. Objetivo
2. Ambito de aplicación
3. Base legal
4. Documentos relacionados
5. Definiciones
6. Responsabilidades
7. Procedimiento
8. Anexos
9. Modificaciones

Observaciones:

Copia Controlada No._____

1. OBJETIVOS

- Establecer la metodología para la revisión, actualización, aprobación, control y distribución (magnética y física) de los documentos del Sistema de Gestión de Seguridad de la Información (SGSI) de CEL.

- Definir los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y la disposición de los registros de seguridad, establecidos en el SGSI de CEL.

- Establecer los lineamientos para colocar los Documentos en los enlaces del SGSI.

5. **Elaboración de procedimiento para el mantenimiento de requisitos de seguridad de la información de documentos del SGSI PRSN-004**

Título:

MANTENIMIENTO DE REQUISITOS DE SEGURIDAD DE LA INFORMACION

Preparado por :

Nombre: **Cargo :**	Firma:	Fecha:

Revisado por:

Nombre: **Cargo :**	Firma:	Fecha:
Nombre: **Cargo :**	Firma:	Fecha:

Aprobado por:

Nombre: **Cargo :**	Firma:	Fecha:

Contenido:

Observaciones:

Copia Controlada No._____

2. OBJETIVO

Establecer el procedimiento que permita identificar y documentar las disposiciones legales y técnicas vigentes sobre la seguridad de la información, a fin de mantener el SGSI actualizado.

6. Elaboración del procedimiento para la clasificación y marcado de la información del SGSI PRSN-0010

Título:

CLASIFICACION Y MARCADO DE LA INFORMACION

Preparado por :

Nombre: Firma: Fecha:
Cargo :

Revisado por:

Nombre: Firma: Fecha:
Cargo :

Nombre: Firma: Fecha:
Cargo :

Aprobado por:

Nombre : Firma: Fecha:
Cargo :

Contenido:

Observaciones:

Copia Controlada No._____

1. OBJETIVOS

- Asegurar un nivel de protección adecuado para la información, clasificándola en términos de su valor, uso, requisitos legales y confidencialidad para CEL.
- Desarrollar e implementar un apropiado procedimiento para manejo y marcado de la información de acuerdo al esquema de clasificación adoptado en CEL.

COMISION EJECUTIVA HIDROELECTRICA DEL RIO LEMPA

METODOLOGÍA PARA LA GESTIÓN Y CONTINUIDAD DEL NEGOCIO

HOJA DE AUTORIZACIÓN

Preparado por:

Nombre : Firma: Fecha:

Cargo :

Revisado por:

Nombre : Firma: Fecha:

Cargo :

Aprobado por:

Nombre : Firma: Fecha:

Cargo :

Observaciones:

Copia Controlada No._____

CONTENIDO

1.1 INTRODUCCIÓN

Cada año cientos de negocios e instituciones son afectadas por inundaciones, incendios, vandalismos, etc. Aquellas que sobreviven a estas situaciones, son aquellas que han planificado estar preparadas para lo peor, estimando los posibles daños que pueden ocurrir, instalando los controles necesarios para protegerse. Esta metodología se ha preparado como una guía para elaborar el plan de continuidad del negocio de CEL y los planes de recuperación ante desastres de las dependencias de éste.

1.2 OBJETIVOS

1.2.1 Brindar los insumos a utilizar para elaborar el Plan de Continuidad del Negocio de CEL.
1.2.2 Garantizar la continuidad de las operaciones de los elementos considerados como críticos que componen los Sistemas de Información.
1.2.3 Apoyar en la definición de acciones y procedimientos a ejecutar en caso de falla de los elementos que componen un Sistema de Información.

C. MONITOREAR Y REVISAR EL SGSI

1. Diseño de indicadores de monitoreo y revisión del SGSI

Luego de haber realizado el análisis y evaluación de riesgo se prosiguió a diseñar una serie políticas, objetivos de seguridad y controles / objetivos de control que servirán para un adecuado tratamiento de riesgos, dichos controles deberán de cumplirse tal cual se han establecido para minimizar los efectos que pudieran causar en los activos de información al verse afectados por las amenazas y vulnerabilidades.

A continuación se presenta una serie de indicadores diseñados en conformidad con los controles, políticas y objetivos del SGSI anteriormente presentados, esto con el fin de monitorear y revisar el SGSI.

Dichos indicadores tienen la bondad de brindar información precisa sobre el cumplimiento de los controles, políticas y objetivos del SGSI, detectando cuáles de ellos necesita ser re implementados o reorientados para un mejor resultado y efectividad.

El índice de comparación para todos los indicadores será el siguiente el cual se ha basado en la escala de likert

Escala de cumplimiento	**1**	**2**	**3**	**4**	**5**
Significado	**Muy bajo** Menor o igual a 10%	**Bajo** Mayor del 10% y Menor o igual a 20%	**Medio.** Mayor del 20% y Menor o igual a 50%	**Alto** Mayor de 50% y Menor o igual a 80%	**Muy alto** Mayor de 80% y Menor o igual a 100%
Acción a tomar	El control debe de ser re implementado		El control debe de ser observador y re orientado para un mejor resultado posterior a la siguiente revisión.		El indicador denota que el control está dando muy buenos resultados.

Tabla 57: Criterios de: Indicadores de seguridad de información.

Indicadores de seguridad de la Información		
Indicador	Formula	Supuesta medición
Numero de virus o códigos maliciosos detectados	Total de activos infectados entre total de activos declarados en el sistema	Eficacia de los controles antivirus
Número de incidentes e investigaciones de seguridad	Número de incidentes ocurridos entre el total de incidentes detectados por el Sistema	Nivel de actividad de monitorización de eventos de seguridad.
Costes promedio de las brechas de Seguridad	Cantidad de dinero perdida por falla se Seguridad de Información entre el total de activos afectados.	Pérdidas económicas reales debidas a fallos de seguridad
Recursos asignados a las funciones de seguridad	Recursos económicos invertidos en el SGSI entre el total de los activos de información	Costo económico real de utilizar SGSI
Cumplimiento de los requisitos del SGSI	Total de requisitos Cumplidos entre en total de requisitos que establece el ISO 27001:2005	Nivel de cumplimiento de los requisitos del SGSI
Numero de ordenes de trabajo completadas	Numero de ordenes de trabajo terminadas entre el total de las	Eficacia del SGSI para atender las consultas y ordenes de trabajo

	órdenes recibidas a lo largo de un periodo establecido	encaminadas a erradicar riesgos

Tabla 58: Indicadores de seguridad de información.

La clave de los indicadores de seguridad está en obtener medidas que tengan las siguientes características ideales:

• Deberían medir cosas significativas para la organización.
• Deberían ser reproducibles.
• Deberían ser objetivas e imparciales.
• Deberían ser capaces de medir algún tipo de progresión a lo largo del tiempo.

2. Elaboración del plan de revisión y monitoreo del SGSI

Por tratarse de un sistema de Gestión, ese se someterá a auditorías internas (revisiones de efectividad del SGSI) como parte el monitoreo y revisión, dichas auditorias se desarrollaran en un periodo de dos semanas y serán una vez cada ano, las actividades que contendrán estas revisiones de efectividad son:

No.	Actividad	Duración	Fecha de Inicio	Fecha de finalización	Responsable.
1	Informar a los Jefes de las Unidades sobre el periodo de revisión	3 días	04/11/09	06/11/09	Unidad de gestión integrada.
2	Recabar información para aplicar los indicadores de seguridad	1 semana	09/11/09	13/11/09	Coordinador de Auditoría Interna
3	Procedimiento para la Preparación de Fichas de Proceso de Seguridad y Seguimiento de Puntos de Control PRSN-003	1 semana	16/11/09	20/11/09	Coordinador de Auditoría Interna
4	Procedimiento de planificación de auditorías internas del SGSI PRSN-005	1 semana	23/11/09	27/11/09	Coordinador de Auditoría Interna
5	Procedimiento de Gestión de Debilidades, Incidentes, Problemas y Violaciones de Seguridad de la Información PRSN-008	1 semana	30/11/09	04/12/09	Coordinador de Auditoría Interna
6	Procedimiento para la Revisión del SGSI por la Dirección PRSN-009	1 semana	07/12/09	11/12/09	Coordinador de Auditoría Interna
7	Elaborar informe con información, n recabada de los procedimientos PRSN-003, PRSN-005, PRSN-008 y PRSN-009	1 semana	14/12/09	18/12/09	Coordinador de Auditoría Interna
8	Presentar informe de auditoria	1 semanas	21/12/09	05/01/10	Coordinador de Auditoría Interna
9	Divulgar a las Unidades los resultados de la Auditoria.	1 semanas	8/01/10	13/01/10	Unidad de gestión integrada.
TOTAL		8 SEMANAS 3 DIAS			

Tabla 59: Plan de de revisión y monitoreo del SGSI.

Programación de actividades del plan de revisión y monitoreo del SGSI

No.	Actividad	NOVIEMBRE					DICIEMBRE			ENERO
		04 - 06	09 – 13	16 – 21	23 - 27	30 - 04	07 – 11	14 - 18	21 – 05	08 - 13
1	Informar a los Jefes de las Unidades sobre el periodo de revisión.									
2	Recabar información para aplicar los indicadores de seguridad.									
3	Procedimiento para la Preparación de Fichas de Proceso de Seguridad y Seguimiento de Puntos de Control PRSN-003.									
4	Procedimiento de planificación de auditorías internas del SGSI PRSN-005.									
5	Procedimiento de Gestión de Debilidades, Incidentes, Problemas y Violaciones de Seguridad de la Información PRSN-008.									
6	Procedimiento para la Revisión del SGSI por la Dirección PRSN-009.									
7	Elaborar informe con información, n recabada de los procedimientos PRSN-003, PRSN-005, PRSN-008 y PRSN-009.									
8	Presentar informe de auditoría.									
9	Divulgar a las Unidades los resultados de la Auditoria.									

Grafico 10: programación de actividades del plan de revisión y monitoreo del SGSI

3. Elaboración de Procedimiento para Preparación de Fichas de Proceso de Seguridad y Seguimiento de Puntos de Control, SGSI PRSN-003

PREPARACIÓN DE FICHAS DE PROCESO DE SEGURIDAD Y SEGUIMIENTO DE PUNTOS DE CONTROL

Preparado por :

Nombre: Firma: Fecha:
Cargo :

Revisado por:
Cargo :

Nombre: Firma: Fecha:
Cargo :

Aprobado por:

Nombre : Firma: Fecha:
Cargo :

Contenido:

Observaciones:

Copia Controlada No._____

1. OBJETIVO

Establecer una metodología para la preparación y ejecución de la inspección de Seguridad de la Información, a fin de definir las condiciones para el seguimiento de las características más significativas de los procesos claves y la medición del desempeño de los mismos; así como identificar el estado de los activos no conformes y determinar las acciones a seguir en las Unidades Organizativas de CEL, conforme con los requisitos de la Norma UNE-ISO/IEC 27001:2005 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

4. Elaboración de Procedimiento de planificación de auditorías internas del SGSI PRSN-005

Título:

PLANIFICACION Y EJECUCION DE AUDITORIAS INTERNAS DEL SGSI

Preparado por:

Nombre:	Firma:	Fecha:
Cargo :		

Revisado por:

Nombre:	Firma:	Fecha:
Cargo :		
Nombre:	Firma:	Fecha:
Cargo :		

Aprobado por:

Nombre:	Firma:	Fecha:
Cargo :		

Contenido:

Observaciones:

Copia Controlada No._____

1. OBJETIVO

Definir los pasos a seguir para planificar y realizar Auditorías de Seguridad de la Información y/o Seguimiento de Acciones Correctivas o Preventivas por No Conformidades de Auditorías anteriores, para evaluar la eficacia del Sistema de Gestión de Seguridad de la Información, conforme con los requisitos de la Norma ISO/IEC 27001:2005.

5. Elaboración de Procedimiento de Gestión de Debilidades, Incidentes, Problemas y Violaciones de Seguridad de la Información PRSN-008

Título:

GESTION DE DEBILIDADES, INCIDENTES, PROBLEMAS Y VIOLACIONES A LA SEGURIDAD DE LA INFORMACION

Preparado por :

Nombre: **Cargo :**	Firma:	Fecha: 00/00/00

Revisado por:

Nombre: **Cargo :**	Firma:	Fecha: 00/00/00
Nombre: **Cargo :**	Firma:	Fecha: 00/00/00

Aprobado por:

Nombre : **Cargo :**	Firma:	Fecha: 00/00/00

Contenido:

Observaciones:

Copia Controlada No._____

1. OBJETIVO

Establecer los mecanismos para la gestión de las debilidades, incidentes, problemas y violaciones a la seguridad de la información, asociados con los sistemas de información de La Comisión, para la toma de acciones correctivas en el menor tiempo posible.

6. Elaboración de Procedimiento para la Revisión del SGSI por la Dirección PRSN-009

Título:

REVISION DEL SGSI POR LA DIRECCION

Preparado por:

Nombre: **Cargo :**	Firma:	Fecha:

Revisado por:

Nombre: **Cargo :**	Firma:	Fecha:
Nombre: **Cargo :**	Firma:	Fecha:
Nombre: **Cargo :**	Firma:	Fecha:

Aprobado por:

Nombre : **Cargo :**	Firma:	Fecha:

Contenido:

10. Objetivo
11. Ámbito de aplicación
12. Base legal
13. Documentos relacionados
14. Definiciones
15. Responsabilidades
16. Procedimiento
17. Anexos
18. Modificaciones N/A

Observaciones:

Copia Controlada No._____

1. OBJETIVOS

- Asegurar la adecuación y efectividad del Sistema de Gestión de Seguridad de la Información en La Comisión.
- Describir la conformación y actuación de los involucrados de la revisión del SGSI.

D. MANTENER Y MEJORAR EL SGSI

1. Elaboración del procedimiento para acciones preventivas y correctivas del SGSI PRSN – 006

Titulo :

ACCIONES CORRECTIVAS O PREVENTIVAS DE SEGURIDAD DE LA INFORMACION

Preparado por :

Nombre: Firma: Fecha:
Cargo :

Revisado por:

Nombre: Firma: Fecha:
Cargo :

Nombre: Firma: Fecha:
Cargo :

Aprobado por:

Nombre : Firma: Fecha:
Cargo :

Contenido:

Observaciones:

Copia Controlada No._____

1. OBJETIVO

Establecer la forma de elaborar e implantar Acciones Correctivas o Preventivas eficaces, para eliminar las causas de No Conformidades reales o potenciales determinadas por auditorías o monitoreos; así como establecer la sistemática de identificación y tratamiento de oportunidades de mejora por parte de las Unidades Organizativas de los procesos claves y de apoyo de CEL.

2. **Elaboración de matriz de cumplimiento de objetivos del SGSI después de la aplicación de las mejoras.**

No.	OBJETIVOS DEL SGSI*	LIMITANTES ENCONTRADAS	ACCIONES A TOMAR PARA MEJORA	% CUMPLIMIENTO DE OBJETIVO ACTUAL
1	Contar con un Sistema de Gestión de Seguridad de la Información, con la finalidad de mitigar los riesgos operativos y de tecnología de información para el tercer trimestre del 2009.			
2	Fortalecer la cultura de administración del riesgo en función de los valores éticos y morales respecto a la seguridad de la información.			
3	Fomentar con los colaboradores la responsabilidad del manejo de la seguridad de la información, desde la perspectiva de la confiabilidad, integridad y la disponibilidad de la misma.			
4	Obtener la certificación bajo la Norma ISO 27001:2005 en el periodo de un año después de implementado y operado el SGSI			

Tabla 60: Matriz de cumplimiento de objetivos del SGSI.

NOTA: a medida de vayan desarrollando las mejoras al sistema se pueden ir incorporando nuevos objetivos.

CRITERIOS PARA ESTABLECER EL PORCENTAJE DE CUMPLIMIENTO DE LOS OBJETIVOS

COLOR		SIGNIFICADO
	VERDE CLARO	100% DE CUMPLIMIENTO
	VERDE OSCURO	75% DE CUMPLIMIENTO
	AMARILLO	50% DE CUMPLIMIENTO
	NARANJA	25% DE CUMPLIMIENTO
	ROJO	0% DE CUMPLIMIENTO

Tabla 61: Criterios de cumplimiento de objetivos del SGSI.

E. DISEÑO DE SISTEMA DE INFORMACIÓN

1. Diseño del sistema de información

El sistema de información que se implementara en la Comisión nos permitirá ordenar el flujo de la información que se maneja en cada uno de los procesos claves y de apoyo. Estará constituido por diferentes catálogos cuya función principal será la de registrar los datos, los cuales se almacenaran en una base de datos mediante tablas relacionadas, Sistema tendrá la capacidad de generar diferentes reportes e informes que reflejaran de una forma más clara la situación en que se encuentra la Comisión en cuanto a la Administración del SGSI.

El Sistema de Información será una herramienta muy importante que dará vida al SGSI diseñado bajo las normas internacionales ISO 27001, permitiéndole a la alta gerencia y todos aquellos interesados en la Gestión de la Seguridad de la Información ingresar a él y de primera mano obtener información confiable y segura en cuanto al cálculo de riesgos, la forma de gestionar la Seguridad de la Información, Estado y cálculo de los indicadores de seguridad, y sobre el estado de cumplimiento de los objetivos y políticas del SGSI.

Los beneficios que arrojara el Sistema serán:

- Mayor flujo de información entre los diferentes procesos, de una manera ordenada y rápida.
- Ahorro de tiempo en el manejo de información.
- Mecanización del SGSI

Componentes diseñados para el Sistema

- Desglose Funcional
- Sistema Entrada –Salida.
- Flujo de información.
- Modelo del sistema.
- Procedimientos.
- Medición de indicadores del SIG.
- Actas y Acuerdos.

2. Conceptualización del sistema de información

a) Desglose funcional.

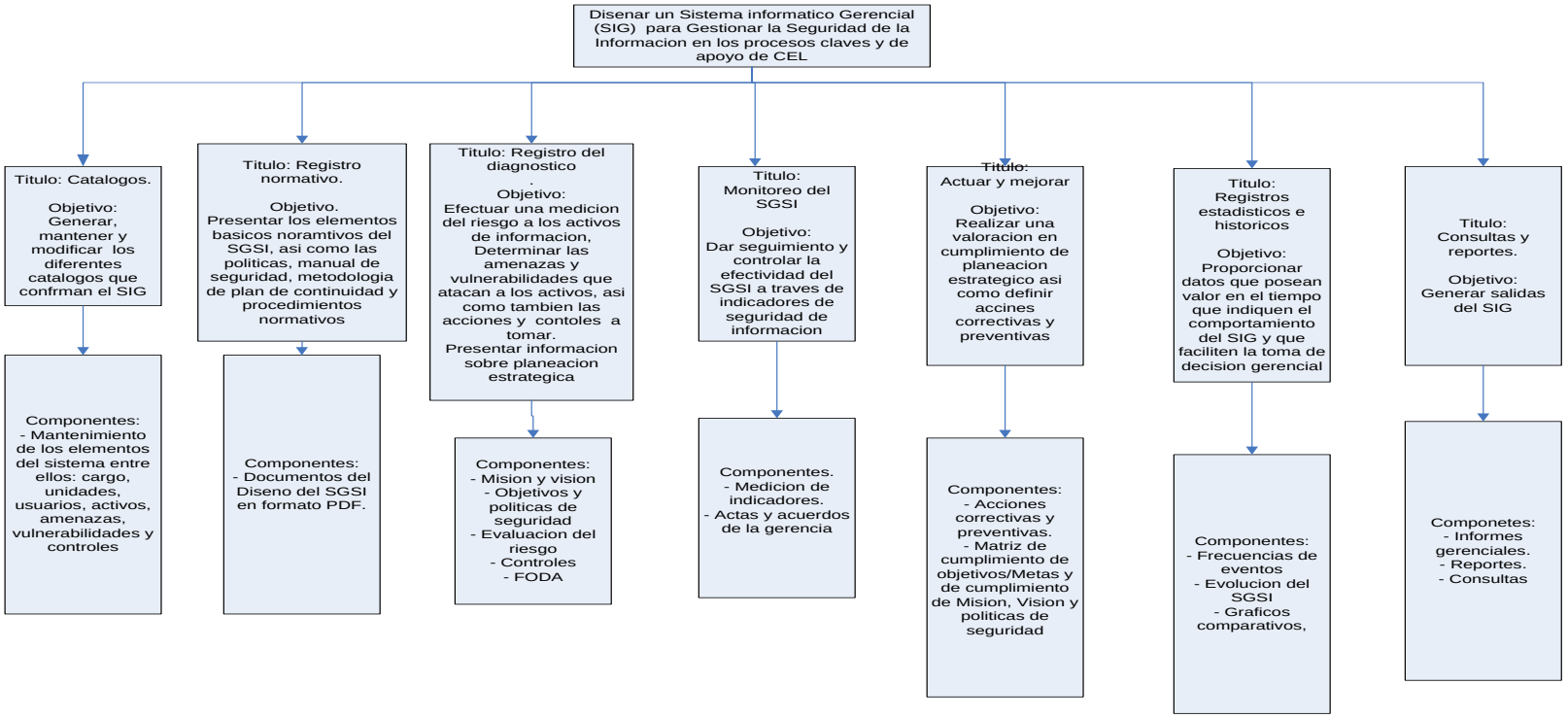


Figura 31: Desglose funcional de SIG

b) Sistema de entrada – salida

Las estradas y salidas serán las mismas para todo el sistema independientemente de la Unidad que se quiera estudiar. Por lo que a continuación se presenta la relación entradas – salidas del sistema.

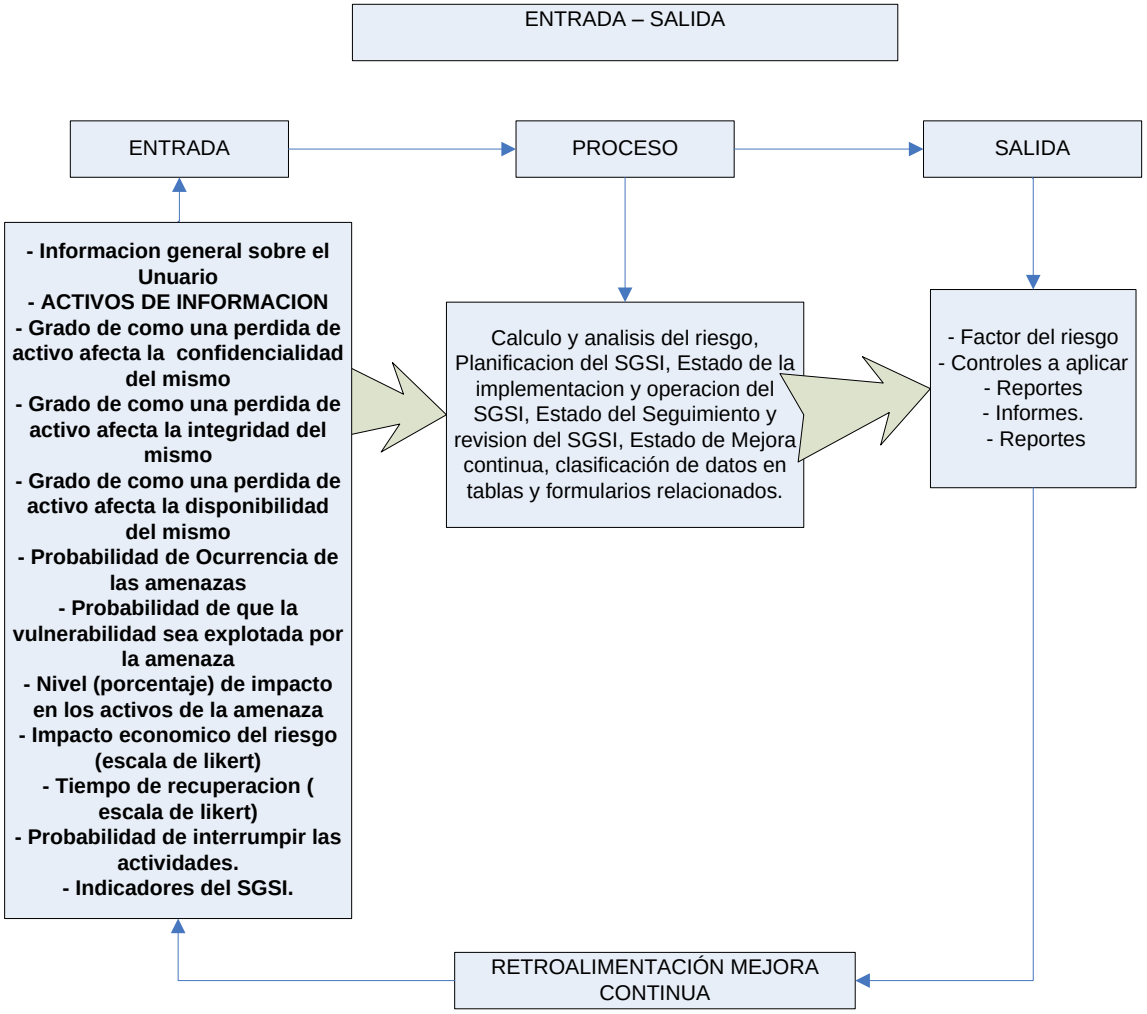


Figura 32: Sistema Entrada-Proceso-Salida.

c) Flujo de información.

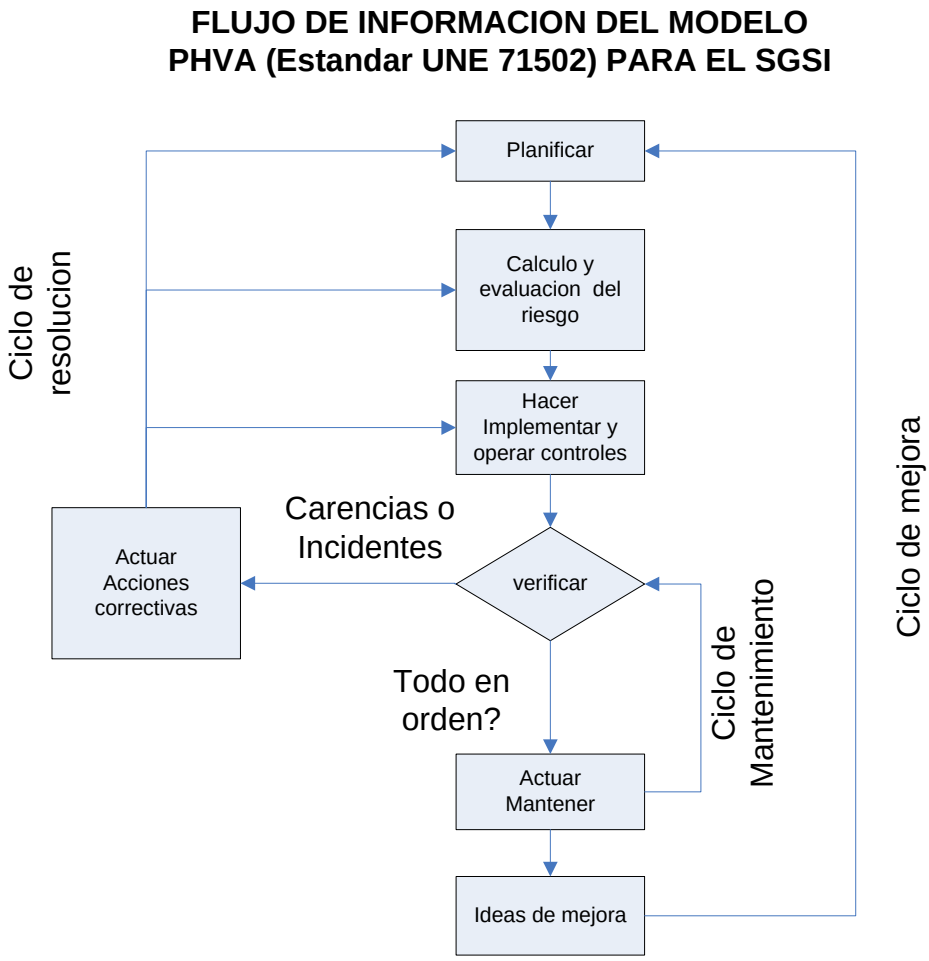


Figura 33: Flujo de Información del Sistema.

d) Modelo del sistema

El sistema se puede visualizar desde dos niveles, la idea principal está reflejada en el desglose analítico, luego en las entradas y salidas y su respectivo flujo de información.

EL NIVEL 1. Representa de forma genérica el proceso del sistema, el cual se basa en el Ciclo Planificar, Hacer, Verificar y actuar.

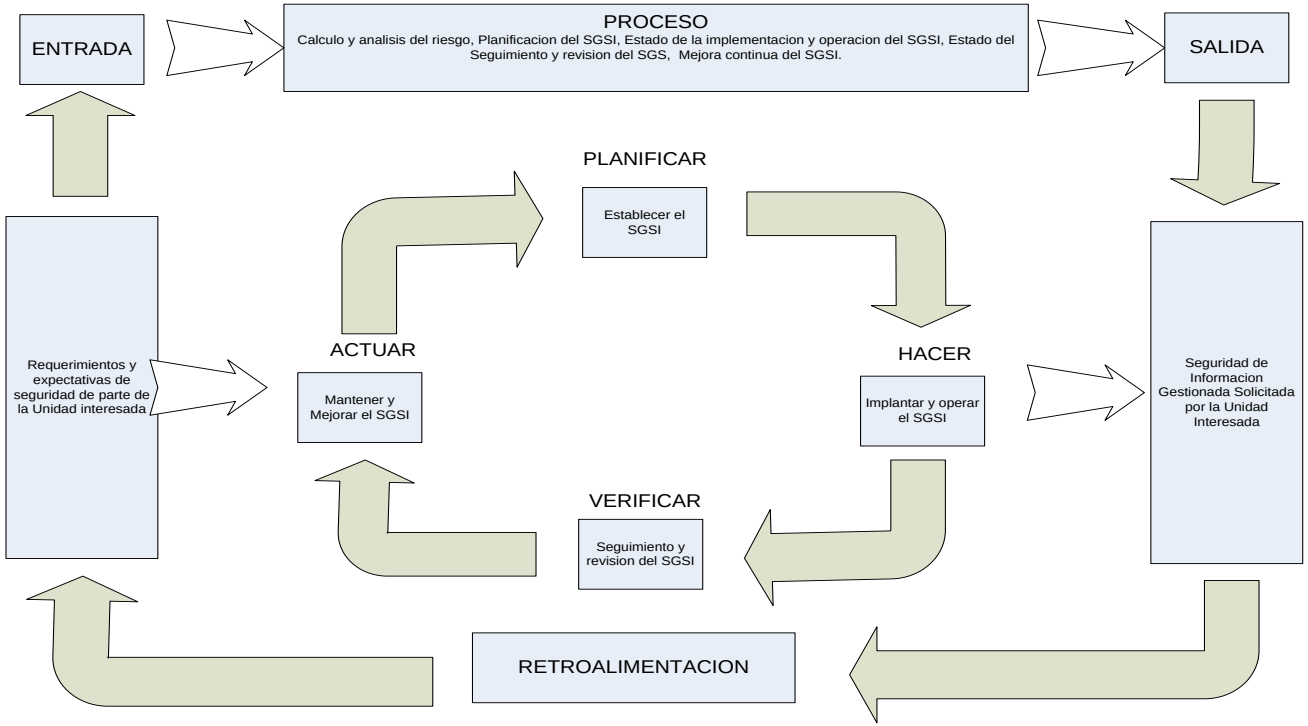


Figura 34: Modelo del Sistema.

El siguiente nivel (2) nos detalla en forma general como es que el sistema procesara las entradas, Cada fase corresponde al desglose funcional del sistema.

NIVEL 2

FASES DEL SISTEMA

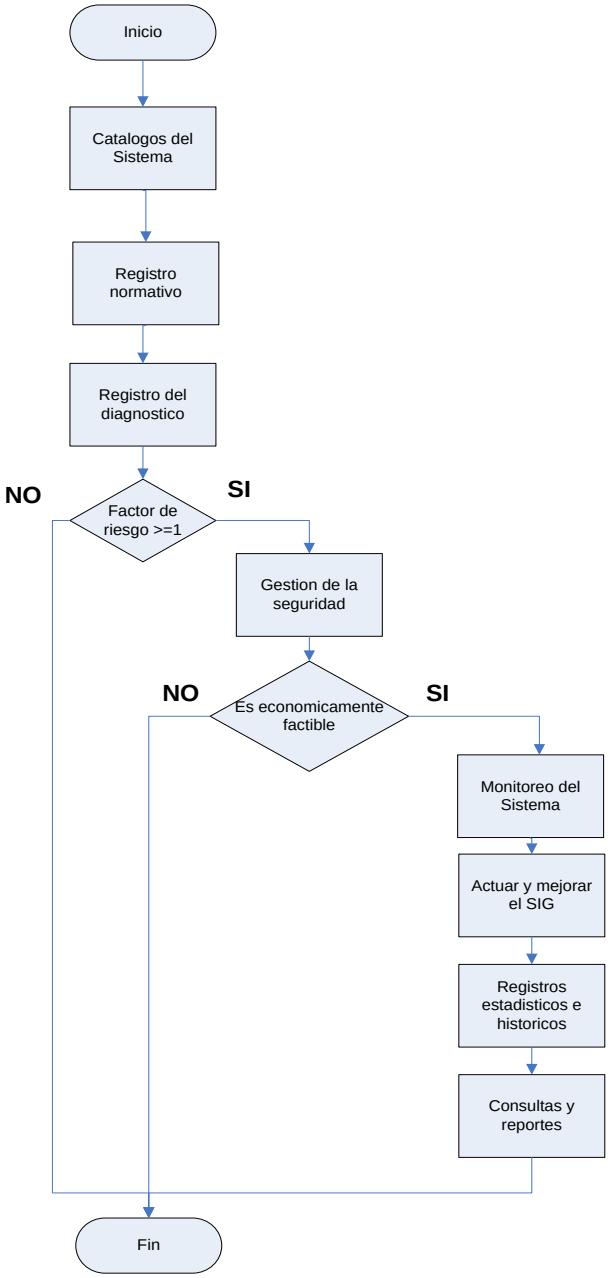


Figura 35: Fases del Sistema.

e) Procedimientos.

Luego de detallar el modelo del sistema a través de los diferentes niveles y fases que poseerá, proseguimos con la declaración y diseño de los procedimientos que darán vida de forma mecanizada a cada una de las fases del ciclo PHVA (El sistema de Información).

Al inicio deberá desarrollar un formulario que pida ingresar los siguientes datos generales del usuario del Sistema.

- Unidad a la que pertenece.
- Nombre completo
- Cargo Funcional
- Código del empleado
- Fecha actual

Estos datos serán almacenados en la base de datos del sistema para llevar un control de los usuarios del mismo.

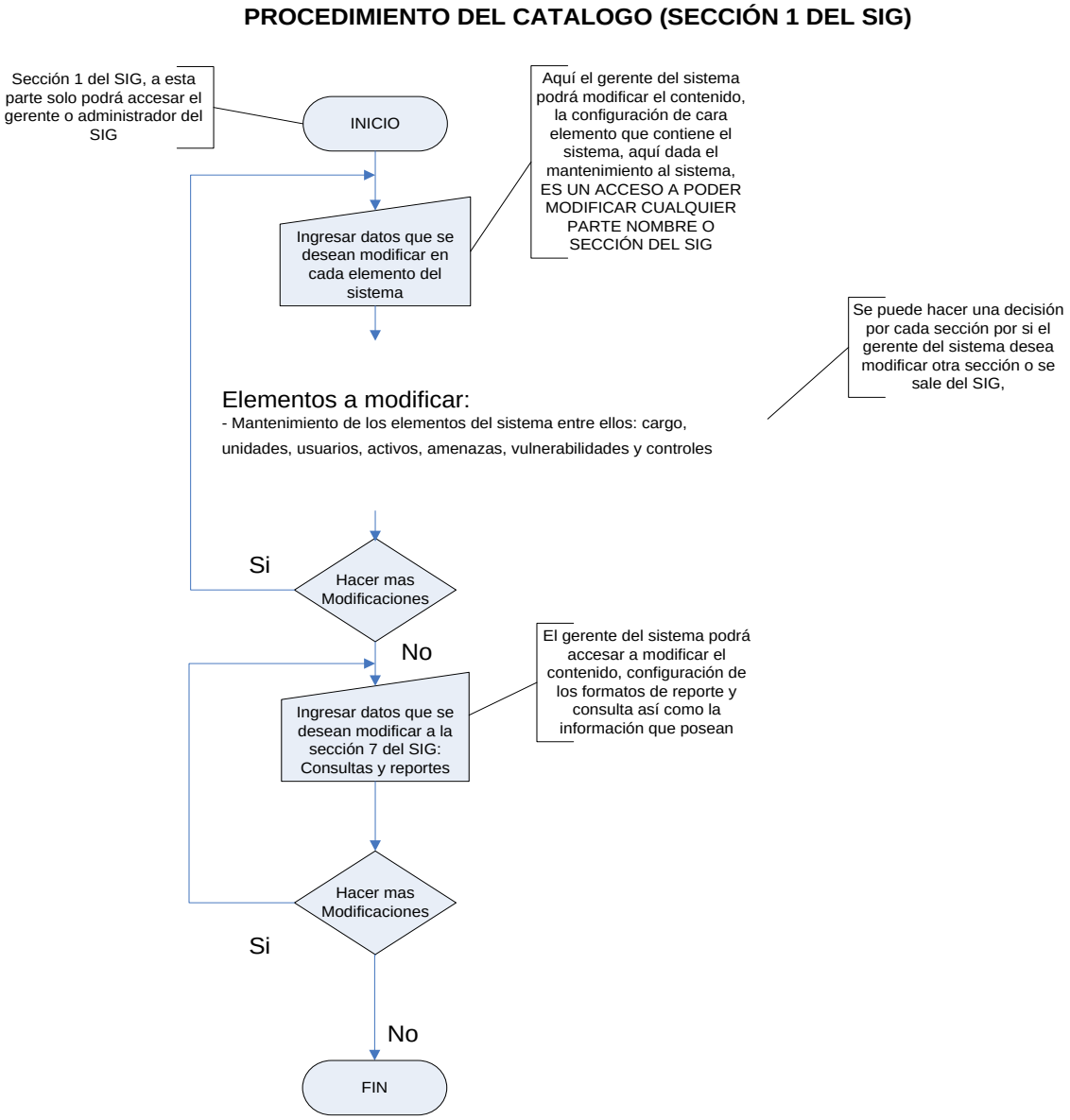


Figura 36: Procedimiento del Catalogo del Sistema.

PROCEDIMIENTO DEL REGISTRO NORMATIVO (SECCIÓN 2 DEL SIG)

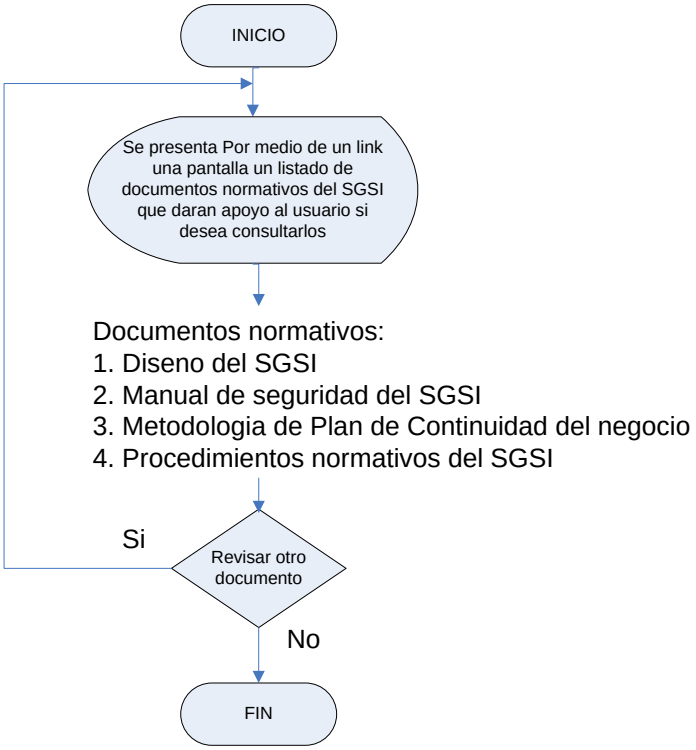
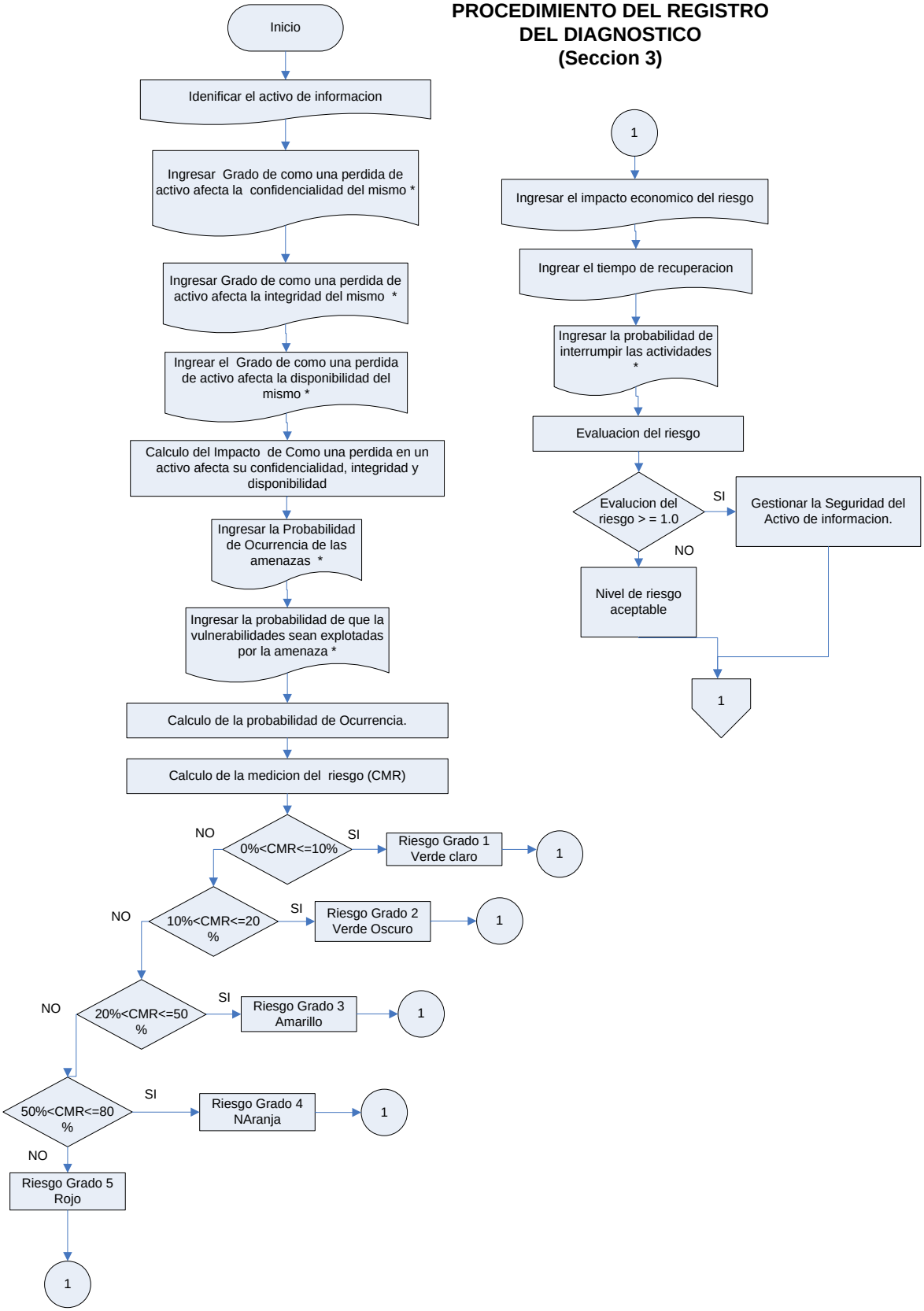


Figura 37: Procedimiento del Registro Normativo.

PROCEDIMIENTO DEL REGISTRO DEL DIAGNOSTICO (Seccion 3)



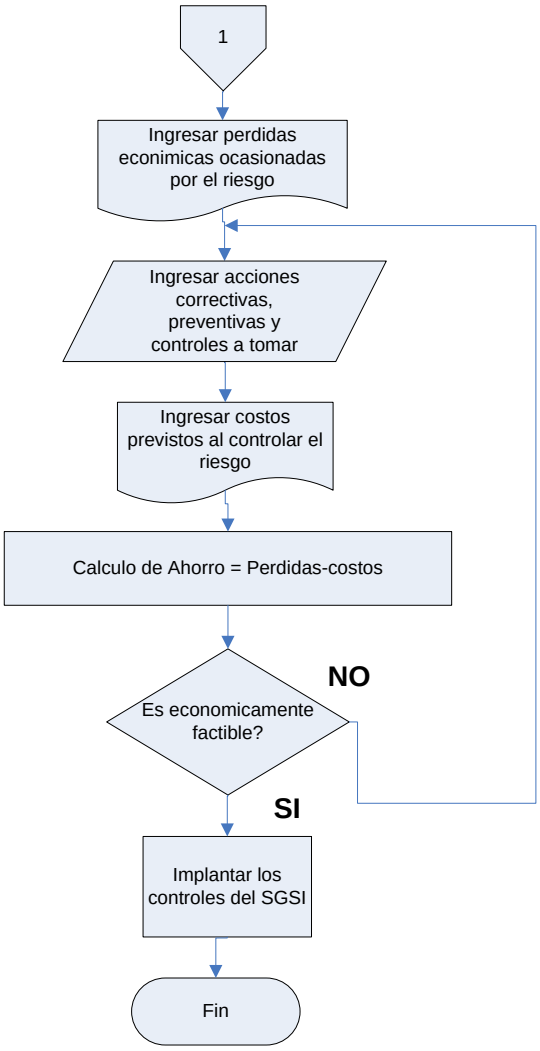


Figura 38: Procedimiento del Registro del Diagnostico.

* Los niveles y criterios para cada uno de las entradas del sistema se encuentran definidos en el documento del diseño del SGSI, en el apartado de elaboración de metodología para evaluación del riesgo

CONTROLES A APLICAR

Dependiendo de los niveles de riesgo así se aplicaran los controles necesarios
Cada activo tendrá asociado una cantidad de controles definidos.

#	Activos	Controles correspondientes
1	Base de datos de clientes	A.5.1 Política de seguridad de la Información A.6.1 Organización interna A.7.1 Responsabilidad por los activos A.7.2 Clasificación de la información
	Base de datos de empleados	
	Base de datos financieras	
	Base de datos de producción	

	Base de datos proveedores	A.9.1 Áreas seguras A.10.1 Procedimientos y responsabilidades de operación A.10.3 Planificación y aceptación del sistema A.10.4 Protección contra código malicioso y movible A.10.5 Copia de seguridad A.10.7 Manejo de medios de Información A.10.8 Intercambio de información A.11.1 Requisitos del negocio para el control de accesos A.11.2 Gestión de acceso de usuarios A.11.3 Responsabilidades de usuarios A.11.6 Control de acceso a las aplicaciones e información A.12.1 Requisitos de seguridad de los sistemas de información A.12.5 Seguridad en los procesos de desarrollo y soporte A.12.6 Gestión de vulnerabilidad técnica A.13.1 Reportar los eventos y debilidades de seguridad de la información A.13.2 Gestión de los incidentes y mejoras de seguridad de la información
	Equipo de computo	A.5.1 Política de seguridad de la Información A.6.1 Organización interna A.6.2 Partes externas A.7.1 Responsabilidad por los activos A.9.1 Áreas seguras A.9.2 Seguridad de los equipos A.10.3 Planificación y aceptación del sistema A.10.4 Protección contra código malicioso y movible A.10.6 Gestión de seguridad de la red A.10.7 Manejo de medios de Información A.10.8 Intercambio de información A.10.9 Servicios de comercio electrónico A.10.10 Seguimiento A.11.1 Requisitos del negocio para el control de accesos A.11.2 Gestión de acceso de usuarios A.11.3 Responsabilidades de usuarios A.11.4 Control de acceso a la red. A.11.5 Control de acceso al sistema operativo A.12.1 Requisitos de seguridad de los sistemas de información A.12.6 Gestión de vulnerabilidad técnica A.13.1 Reportar los eventos y debilidades de seguridad de la información
	Internet	
	Correos electrónicos	
	Intranet	
	Servicio de archivos	A.5.1 Política de seguridad de la Información A.6.1 Organización interna A.7.1 Responsabilidad por los activos A.7.2 Clasificación de la información
	Copias de respaldo	

		A.9.1 Áreas seguras A.10.2 Gestión de entrega de servicio de tercera parte A.10.3 Planificación y aceptación del sistema A.10.5 Copia de seguridad A.10.7 Manejo de medios de Información A.10.8 Intercambio de información A.11.1 Requisitos del negocio para el control de accesos A.11.2 Gestión de acceso de usuarios A.11.3 Responsabilidades de usuarios A.12.1 Requisitos de seguridad de los sistemas de información A.12.3 Controles criptográficos A.12.4 Seguridad de los archivos del sistema A.12.6 Gestión de vulnerabilidad técnica A.13.1 Reportar los eventos y debilidades de seguridad de la información
	Correspondencia interna	A.5.1 Política de seguridad de la Información A.6.1 Organización interna A.7.1 Responsabilidad por los activos A.7.2 Clasificación de la información A.9.1 Áreas seguras A.10.3 Planificación y aceptación del sistema A.10.5 Copia de seguridad A.10.7 Manejo de medios de Información A.11.1 Requisitos del negocio para el control de accesos A.11.2 Gestión de acceso de usuarios A.11.3 Responsabilidades de usuarios A.12.1 Requisitos de seguridad de los sistemas de información A.12.3 Controles criptográficos A.12.4 Seguridad de los archivos del sistema A.12.6 Gestión de vulnerabilidad técnica A.13.1 Reportar los eventos y debilidades de seguridad de la información
	Correspondencia externa	
	Documentos en papel impreso	
	Manuales de usuarios	
	Documentos legales	
	Línea dedicada	A.5.1 Política de seguridad de la Información A.6.1 Organización interna A.7.1 Responsabilidad por los activos A.9.1 Áreas seguras A.9.2 Seguridad de los equipos A.10.3 Planificación y aceptación del sistema A.10.6 Gestión de seguridad de la red A.10.7 Manejo de medios de Información A.11.1 Requisitos del negocio para el control de accesos A.11.2 Gestión de acceso de usuarios A.11.3 Responsabilidades de usuarios A.12.1 Requisitos de seguridad de los sistemas de información
	Líneas telefónicas	
	Cámaras	

		A.12.3 Controles criptográficos A.13.1 Reportar los eventos y debilidades de seguridad de la información
	Información intelectual Documentos en medio digital Software de sistemas	A.5.1 Política de seguridad de la Información A.6.1 Organización interna A.7.1 Responsabilidad por los activos A.7.2 Clasificación de la información A.8.1 Antes del empleo A.8.2 Durante el empleo A.8.3 Terminación o cambio de empleo A.10.3 Planificación y aceptación del sistema A.10.5 Copia de seguridad A.10.6 Gestión de seguridad de la red A.10.7 Manejo de medios de Información A.11.1 Requisitos del negocio para el control de accesos A.11.2 Gestión de acceso de usuarios A.11.3 Responsabilidades de usuarios A.12.1 Requisitos de seguridad de los sistemas de información A.12.3 Controles criptográficos A.12.4 Seguridad de los archivos del sistema A.13.1 Reportar los eventos y debilidades de seguridad de la información

Tabla 62: Controles de riesgos del Sistema de Información Gerencial.

FODA

Consistes en documentar las fortalezas, oportunidades, debilidades y amenazas del SIG para luego tomarlas como base para mejorar el sistema y ver su nivel de avance.

FORTALEZAS	OPORTUNIDADES	DEBILIDADES	AMENAZAS

Tabla 63: FODA del Sistema de Información Gerencial.

PROCEDIMIENTO DE MONITOREO (seccion 4)

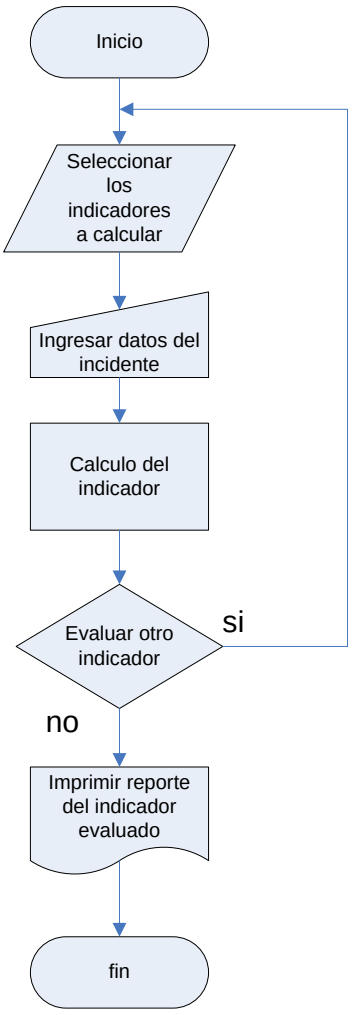


Figura 39: Procedimiento del Monitoreo.

f) Medición de indicadores del SIG

Indicadores de seguridad de la Información		
Indicador	Formula	Supuesta medición
Numero de virus o códigos maliciosos detectados	Total de activos infectados entre total de activos declarados en el sistema	Eficacia de los controles antivirus
Número de incidentes e investigaciones de seguridad	Número de incidentes ocurridos entre el total de incidentes detectados por el Sistema	Nivel de actividad de monitorización de eventos de seguridad.
Costes promedio de las brechas de Seguridad	Cantidad de dinero perdida por falla se Seguridad de Información entre el total de activos afectados.	Pérdidas económicas reales debidas a fallos de seguridad
Recursos asignados a las funciones de seguridad	Recursos económicos invertidos en el SGSI entre el total de los activos de información	Costo económico real de utilizar SGSI
Cumplimiento de los requisitos del SGSI	Total de requisitos Cumplidos entre en total de requisitos que establece el ISO 27001:2005	Nivel de cumplimiento de los requisitos del SGSI
Numero de ordenes de trabajo completadas	Numero de ordenes de trabajo terminadas entre el total de las órdenes recibidas a lo largo de un periodo establecido	Eficacia del SGSI para atender las consultas y ordenes de trabajo encaminadas a erradicar riesgos

Tabla 64: Indicadores del Sistema de Información Gerencial.

Criterios de los indicadores

Escala de cumplimiento	1	2	3	4	5
Significado	**Muy bajo** Menor o igual a 10%	**Bajo** Mayor del 10% y Menor o igual a 20%	**Medio.** Mayor del 20% y Menor o igual a 50%	**Alto** Mayor de 50% y Menor o igual a 80%	**Muy alto** Mayor de 80% y Menor o igual a 100%
Acción a tomar	El control debe de ser re implementado		El control debe de ser observador y re orientado para un mejor resultado posterior a la siguiente revisión.		El indicador denota que el control está dando muy buenos resultados.

Tabla 65: Criterios de Indicadores del Sistema de Información Gerencial.

g) Actas y acuerdos

Consiste en documentar los acuerdos que se dictaminen desde la gerencia luego de realizada una acciones de monitoreo.

ACTA No.	Fecha de Elaboración	No. de Acuerdo	Acuerdo	Cumplimiento		Acciones Ejecutadas
				SI	NO	

Tabla 66: Actas y acuerdos del Sistema de Información Gerencial.

PROCEDIMIENTO ACTUAR Y MEJORAR (seccion 5)

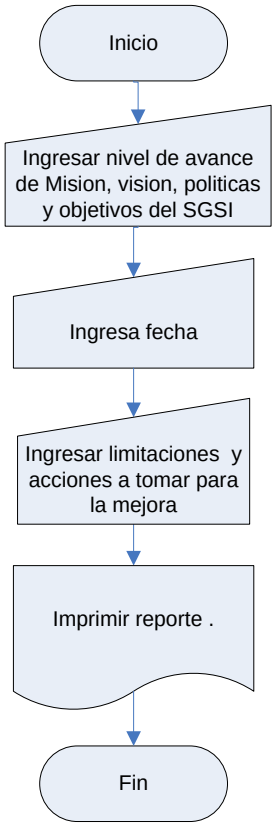


Figura 40: Procedimiento para Actuar y Mejorar.

ACCIONES CORRECTIVAS Y PREVENTIVAS

Consiste en documentar que acciones correctivas o preventivas estima realizar dependiendo de los resultados del monitoreo que previamente ha realizado. El podrá detectar que aéreas están deficientes o con posibilidad de mejora.

ACCIONES CORRECTIVAS A APLICAR	ACCIONES PREVENTIVAS A APLICAR

Tabla 67: Acciones correctivas y preventivas del Sistema de Información Gerencial.

REGISTRO ESTADISTICOS E HISTORICOS (SECCION 6)

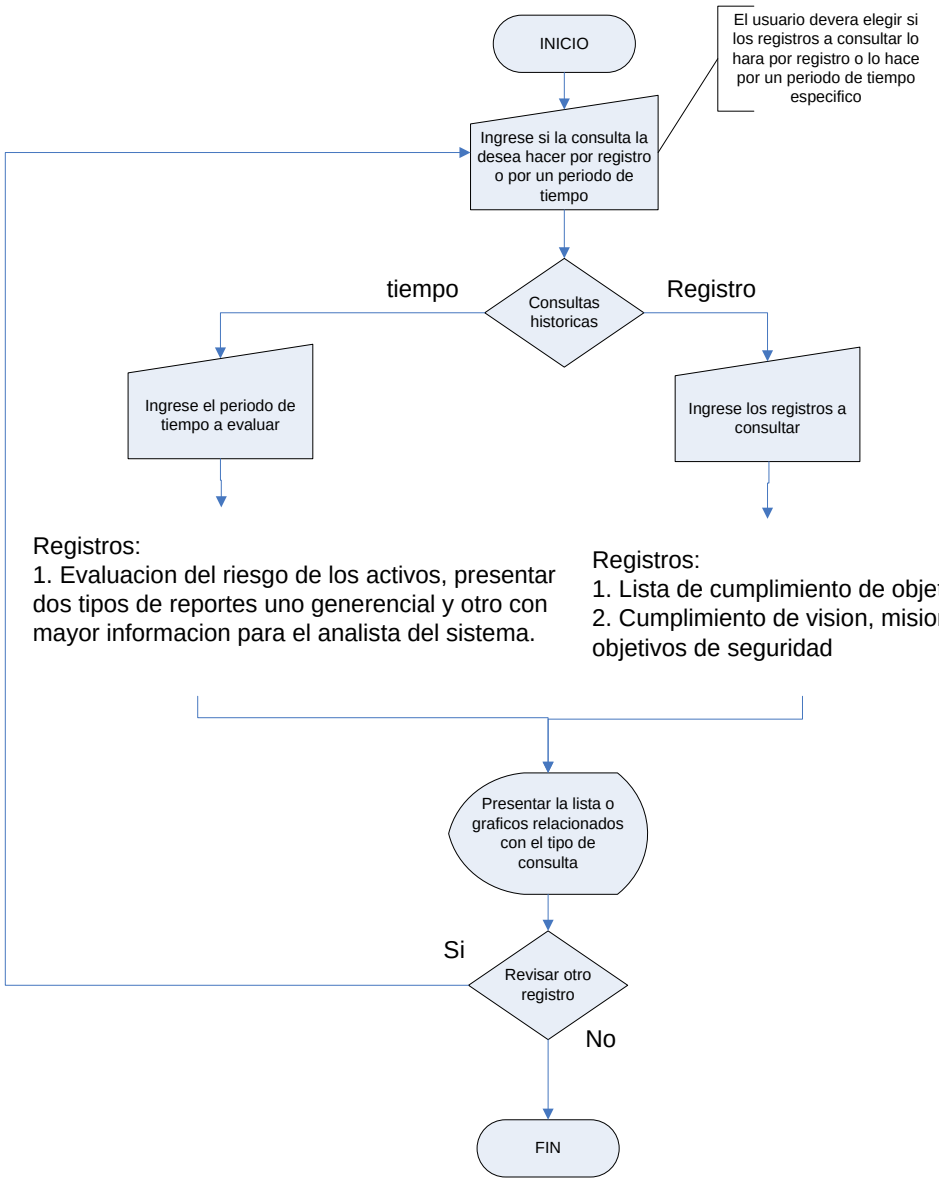


Figura 41: Procedimiento de Registro Estadístico e Histórico.

PROCEDIMIENTO DE REPORTES (SECCION 7)

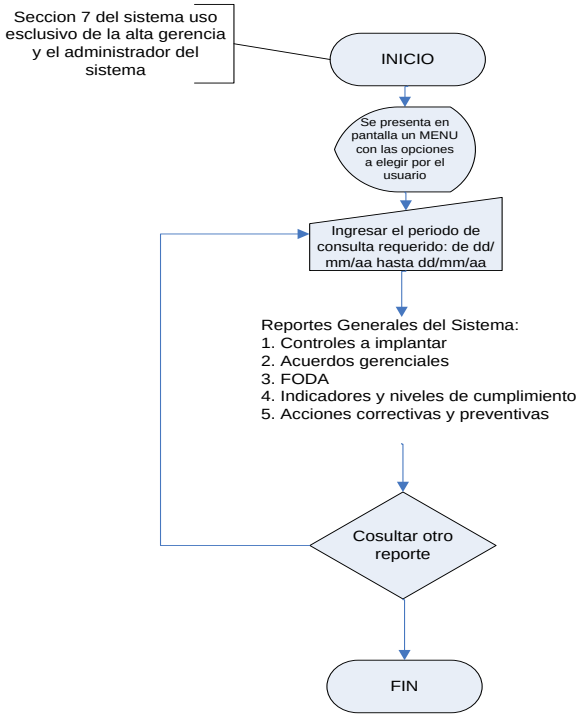


Figura 42: Procedimiento de Reportes.

F. METODOLOGIA DE APLICACIÓN DE LA ISO 27001:2005

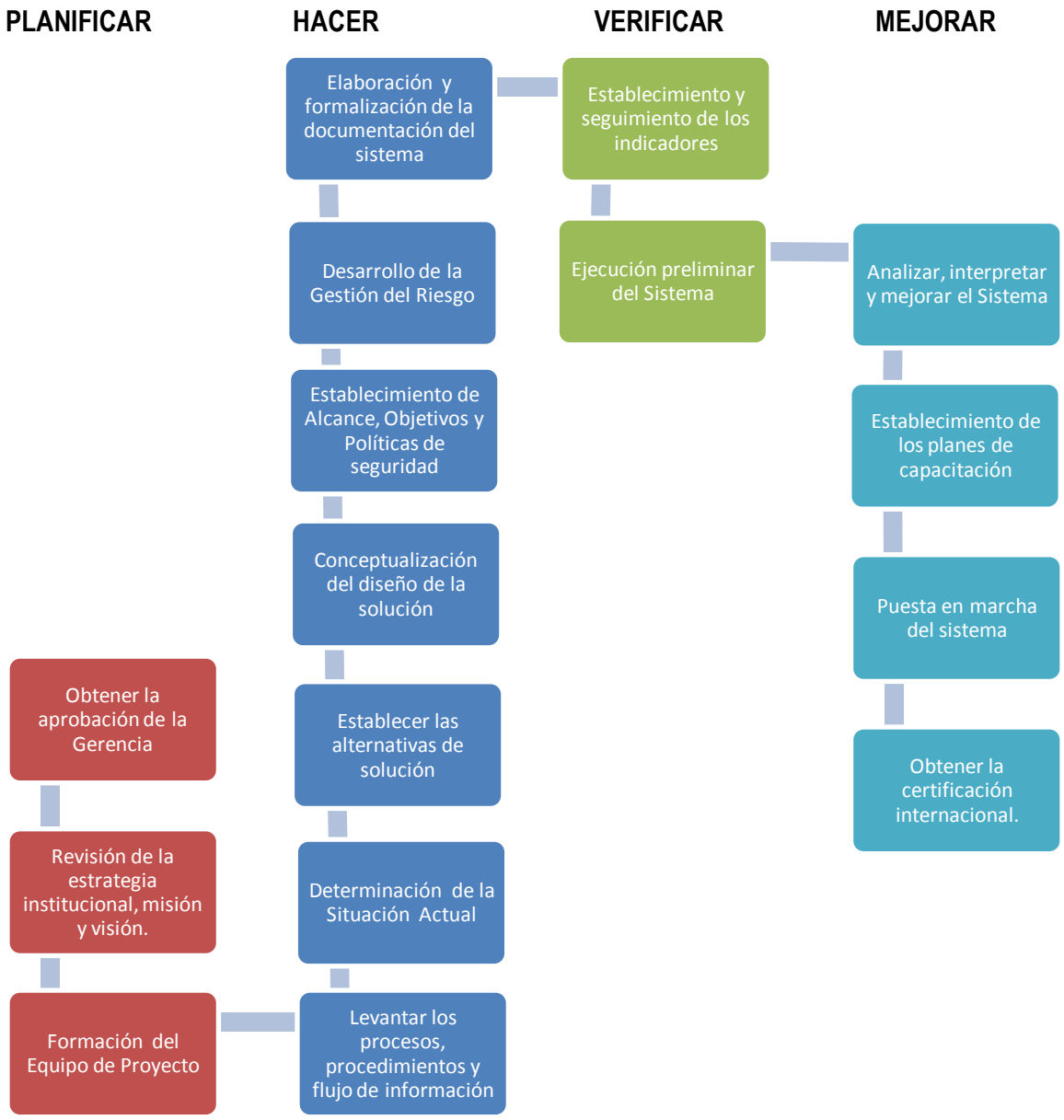


Figura 43: Metodología de aplicación de la norma ISO 27001.

Descripción de la implementación de la norma ISO 27001/PHVA

Ciclo	Fase	Descripción de la fase	Nivel de autorización	Responsable de ejecución
PLANIFICACION	Obtener la aprobación de la Gerencia	Esta fase consiste en hacer que la alta gerencia se comprometa, respalde e impulse la aplicación de la norma y que acompañe en todo el proceso de la misma.	Alta gerencia por medio de carta compromiso.	Alta gerencia
	Revisión de la estrategia institucional, misión y visión.	En esta fase se considera que las estrategias institucionales, la misión y la visión este acorde con los objetivos y lineamientos establecidos en la norma; si no es así, queda a discreción de la institución modificar o redefinir las estrategias y visión de la misma.	Alta gerencia	Alta gerencia y gerentes de procesos.
	Formación del Equipo de Proyecto	Aquí se conforma el equipo responsable directo de la implementación de la norma, se recomienda sea formado por un representante de cada proceso involucrado para comprometerlos y garantizar el éxito del proyecto, aquí se definen las funciones y roles de cada miembro del equipo, la estrategia a seguir para implementar y se calendarizan las macro actividades.	Alta gerencia	Alta gerencia y gerentes de procesos involucrados.
EJECUCION DE LO PLANIFICADO	Levantar los procesos, procedimientos y flujo de información	En esta fase se investigan y se recoge toda la información correspondiente al flujo de información de los procesos y procedimientos que serán gestionados bajo la norma, aquí se elabora el mapa de riesgos encontrados.	Gerentes de procesos	Equipo de proyecto (Analistas de procesos)
	Determinación de la Situación Actual	Aquí se presentan los resultados de la investigación y hallazgos encontrados, se dan a conocer las condiciones de seguridad y manejo de la información que poseen los procedimientos y procesos, así mismo se plantea la problemática encontrada.	Equipo de proyecto (Analistas de procesos)	Equipo de proyecto (Analistas de procesos)
	Establecer las alternativas de solución	En esta fase se determinan las posibles alternativas de solución que respondan a resolver la problemática planteada en la fase anterior, se evalúa la viabilidad y sostenibilidad de las	Alta gerencia	Equipo de proyecto

Ciclo	Fase	Descripción de la fase	Nivel de autorización	Responsable de ejecución
		alternativa y se selecciona la que cumpla con los criterios establecidos y garantice dar respuesta a las necesidades encontradas.		
	Conceptualización del diseño de la solución	Una vez seleccionada la mejor alternativa, en esta fase se precede a definirla, se presenta un panorama general y completo del contenido, fases, etapas y pasos a seguir para el desarrollo de las solución, aquí se debe estar completamente claro en la implementación de la norma, ya que será punto de partida para el diseño de la misma.	Alta gerencia	Equipo de proyecto
	Establecimiento de Alcance, Objetivos y Políticas de seguridad	Esta es la fase del diseño del Sistema que plantea la norma como parte de sus requisitos, aquí se elaborar los parámetro por los cuales se fundamenta la gestión de la información.	Alta gerencia	Equipo de proyecto
	Desarrollo de la Gestión del Riesgo	En esta fase se establece la metodología adecuada para la manejar y tratar el riesgo encontrado en la fase de levantamiento de los procesos, procedimientos, flujo de información y determinación de la Situación Actual.	Equipo de proyecto	Equipo de proyecto
	Elaboración y formalización de la documentación del sistema	Como parte del diseño del sistema, en esta fase se elabora toda la documentación requerida por la norma, manuales, procedimientos, instructivos, formularios, matrices de control y seguimiento, listas de verificación, etc.	Alta gerencia	Equipo de proyecto
VERIFICACION	Establecimiento y seguimiento de los indicadores	Aquí se establecen los mecanismos de seguimiento y verificación del sistema que permitan controlar los avances y cumplimiento de políticas y objetivos establecidos en la etapa preliminar.	Equipo de proyecto	Equipo de proyecto
	Ejecución preliminar del Sistema	En esta etapa el equipo de proyecto ejecuta preliminarmente el sistema para verificar su efectividad y puntos de mejora.	Alta gerencia	Equipo de proyecto
MEJORA R Y	Analizar, interpretar y mejorar el Sistema	Aquí se analizan los resultados obtenidos en la ejecución preliminar, se elaborar los planes de mejoras al sistema y ejecución de las mismas.	Equipo de proyecto	Equipo de proyecto

Ciclo	Fase	Descripción de la fase	Nivel de autorización	Responsable de ejecución
	Establecimiento de los planes de capacitación	Una vez mejorado el sistema, se establecen los planes de capacitación para el personal ejecutivo y operativo que será el responsable de manipular y alimentar el sistema una vez funcionando.	Equipo de proyecto	Equipo de proyecto
	Puesta en marcha del sistema	En esta fase se opera el sistema con todo el personal involucrado en los procesos, aplicando todo lo diseñado, esta ejecución puede ser desarrollada en un proceso específico o de manera paralela en todos los procesos requeridos.	Alta gerencia	Equipo de proyecto y alta gerencia
	Obtener la certificación internacional.	Aquí se realizaran las acciones requeridas con las instituciones certificadoras para iniciar el respectivo proceso de certificación.	Alta gerencia	Alta gerencia

Tabla 68: Descripción de la implementación de la norma ISO 27001/ PHVA

G. METODOLOGIA PARA LA OPERACIÓN DEL SGSI BAJO LA NORMA ISO 27001:2005

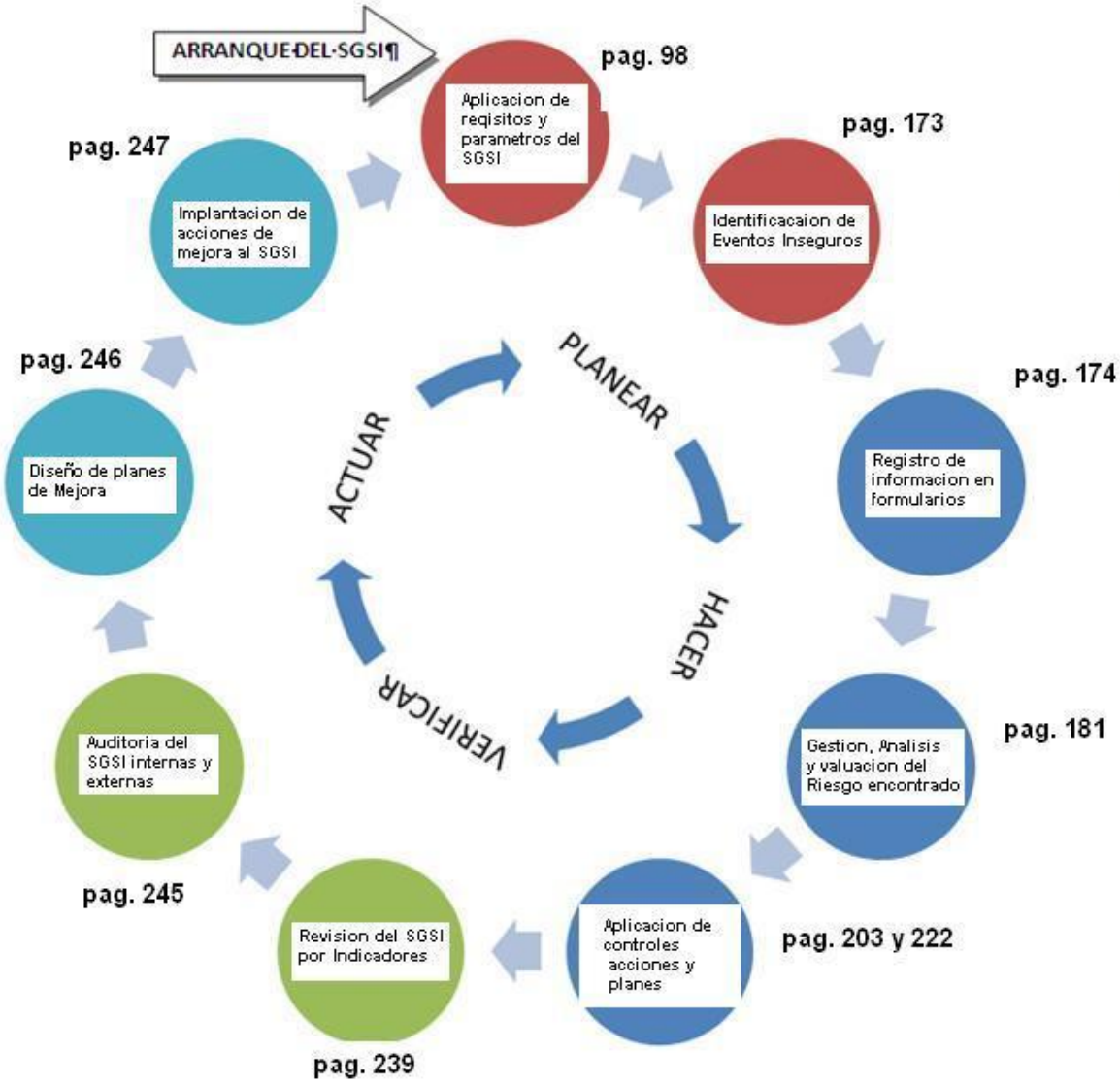


Figura 44: Metodología para la operación permanente del SGSI.

1. Diagrama de operación del SGSI por área responsable

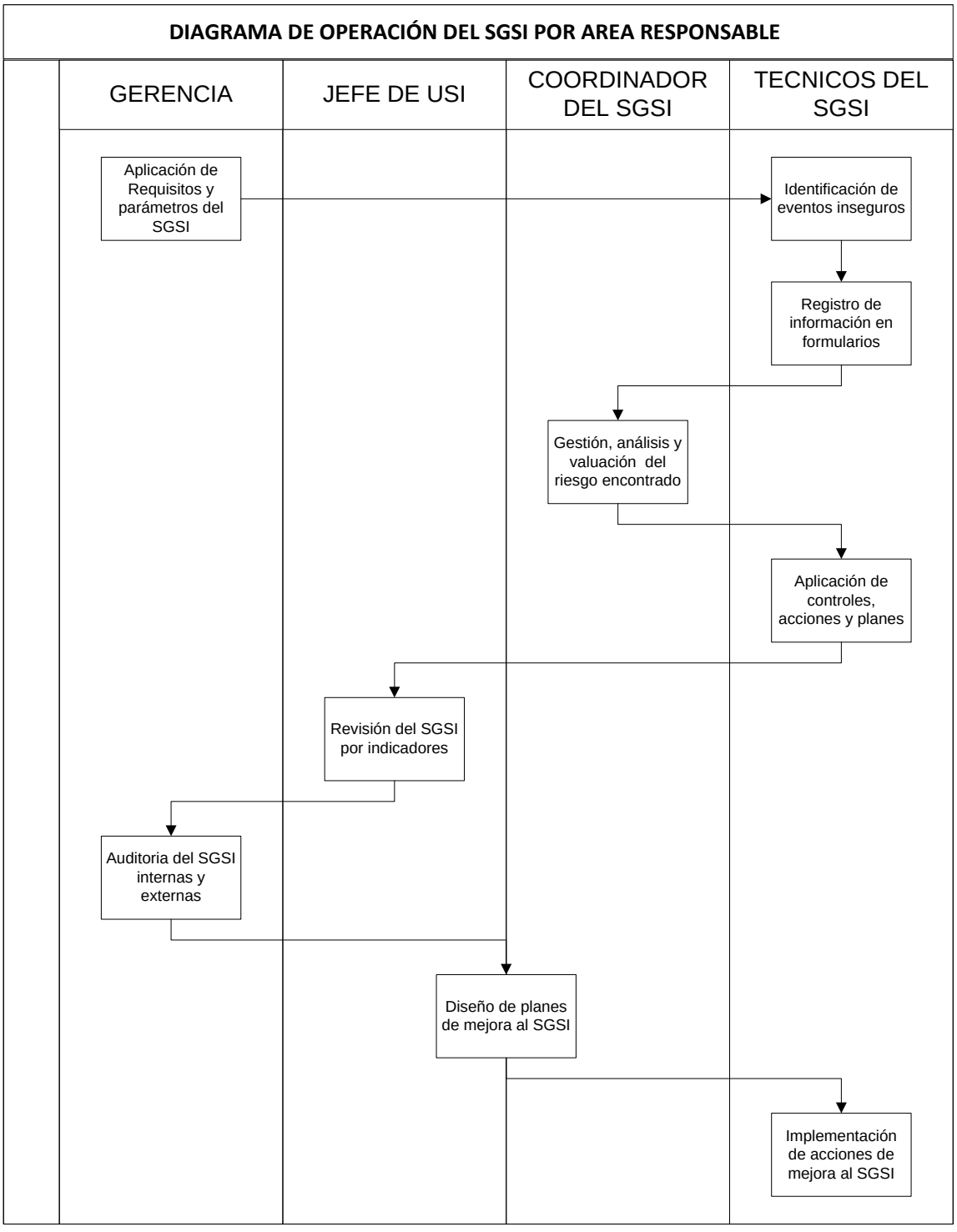


Figura 45: Diagrama de operación del SGSI por área responsable.

2. Descripción de funciones para operar el SGSI por etapas del ciclo PHVA

Ciclo	ETAPA	DESCRIPCIÓN DE LA ETAPA
PLANIFICACION	Aplicación de Requisitos y parámetros del SGSI	Para operar el sistema se deben tener como insumos todos los requisitos de la norma, parámetros de medición, estándares, referencias, planes, alcances, objetivo, etc.
	Identificación de eventos inseguros	En esta epata se identificaran todos aquellos eventos que representan una amenaza o riesgos potenciales que afecten directa o indirectamente a los activos de la organización, según los requerimiento y parámetros previamente establecidos.
EJECUCION DE LO PLANIFICADO	Registro de información en formularios	En esta etapa se documentara el evento riesgoso, registrándolo en los formularios diseñados para ese fin. Se registrara tanto en físico como en digital al sistema.
	Gestión, análisis y valuación del riesgo encontrado	Una vez registrada la información del evento riesgoso, en esta etapa se hará la gestión del riesgo, analizando y evaluándolo; aquí se determinara mediante el proceso de toma de decisión el manejo que se le dará al mismo y las acciones a tomar, los controles a implementar y los planes a implementar.
	Aplicación de controles, acciones y planes	En esta etapa se aplicaran los controles, acciones y planes propuestos en la etapa anterior, con el fin de corregir, disminuir o soportar el riesgo encontrado.
VERIFICACION	Revisión del SGSI por indicadores	Aquí se realizaran las revisiones del sistema, se verificara si los controles, acciones y planes aplicados causaron un impacto positivo frente al riesgo gestionado, estas revisiones se realizaran mediante los indicadores respectivos.
	Auditoria del SGSI internas y externas	En esta etapa la gerencia realizara las auditorias generales del sistema, evaluando el alcance el cumplimiento de los objetivos de seguridad planteados al inicio.
MEJORAR Y ACTUAR	Diseño de planes de mejora al SGSI	Aquí se diseñaran los planes y acciones de mejora al sistema en base a los hallazgos encontrados en las revisiones y las auditorias.
	Implementación de acciones de mejora al SGSI	Una vez diseñadas las acciones y planes a tomar para mejorar el sistema, se implementan estas acciones y planes con el fin de retroalimentar al sistema y mejorar la operación del mismo.

Tabla 69: Descripción de funciones para operar el SGSI por etapas del ciclo PHVA

CAPÍTULO V: EVALUACIÓN ECONOMICA Y FINACIERA DEL SGSI[21]

A. CLASIFICACION DE PROYECTOS

Existe una gran gama de autores y definiciones para la clasificación de un proyecto, a continuación se proporcionan las más completas y que mejor describen este trabajo de graduación:

1. Según el sector al cual están dirigidos

El Proyecto es:

De infraestructura económica. Se caracterizan por ser proyectos que proporcionan a la actividad económica ciertos insumos, bienes o servicios, de utilidad general, tales como: Energía eléctrica, Transporte y Comunicaciones. Incluyen los proyectos de construcción, ampliación y mantenimiento de carreteras, Ferrocarriles, Aeropuertos, Puertos y Navegación; Centrales eléctricas y sus líneas y redes de transmisión y distribución; Sistemas de telecomunicaciones y sistemas de información.

2. Según su carácter

El Proyecto es:

Social. Cuando la decisión de realizarlo no depende de que los consumidores o usuarios potenciales del producto, puedan pagar íntegramente o individualmente los precios de los bienes o servicios ofrecidos, que cubrirá a la comunidad parcialmente o en su conjunto, a través del presupuesto público, de subsidios directos o de sistemas diferenciales de tarifas.

En el caso del presente proyecto los únicos beneficios monetarios que se perciben son en términos de ahorro por de pérdidas incurridas por el mal manejo y falta de seguridad en la información, además el costo de funcionamiento administrativo de CEL está contemplado dentro del presupuesto general de la república por lo que el costo del proyecto no se carga directamente a los usuarios o clientes

En resumen el presente trabajo de graduación se Clasifica en:

Según El Sector Al Cual Está Dirigido en:

De infraestructura económica

Según Su Carácter en:

Social.

Es por ello que para la Decisión de la puesta en marcha de este proyecto es necesario para su evaluación lo siguiente:

- ✓ Investigar cuanto es el costo de su puesta en marcha y su funcionamiento posterior.

[21] Ver Anexo 14: Resumen ejecutivo de la Evaluación Económica – Financiera del SGSI

- ✓ Realizar una evaluación social de los beneficios que percibirá la población consumidora de energía hidroeléctrica que produce CEL, y que ahora contara con un SGSI.

Para evaluar Propuesta de un Sistema de Gestión del Manejo y Seguridad de la información bajo la norma internacional ISO 27001:2005 para La Comisión Ejecutiva Hidroeléctrica del Rio Lempa, CEL, en primer lugar se ha realizado el Análisis de los Beneficios que se tendrán al mantener el sistema en operación, los cuales vendrán dados por los ahorros en las pérdidas económicas incurridas por los diferentes problemas de seguridad de la información presentado en el Diagnostico; así como también los costos que implica tener activo el Sistema, para el cual se ha obtenido la siguiente información:

- ✓ Costos de Inversión del Proyecto
- ✓ Costos de Operación
- ✓ Beneficios económicos del SGSI

Posteriormente se elaborará una Evaluación Social, que tendrá por objeto medir los Beneficios Sociales que se obtendrán con la propuesta, identificados en los resultados esperados a partir de la puesta en marcha del SGSI

B. COSTOS DE INVERSIÓN DEL PROYECTO

Los principales rubros que constituyen los costos de inversión del SGSI son:

1. Costos de Diseño del Sistema de Gestión
2. Costo de Capacitación
3. Costo de Equipo y Material de Seguridad
4. Costo de Documentación
5. Costo del Sistema de Información Gerencial
6. Costos de la estructura organizativa de la Administración del proyecto
7. Costos de la Certificación

A continuación se detallan cada uno de ellos:

1. Costos de diseño del SGSI

Este rubro se refiere al costo de ingeniería, que lo constituye el pago a consultores por el Diseño del SGSI, esto incluye:

- Análisis general de los procesos claves y de apoyo.
- Caracterización de cada una de las áreas (personal, usuarios, maquinaria y equipo, materiales, actividades de trabajo y condiciones actuales de trabajo)
- Evaluación y valoración de riesgos de los activos
- Diseño del Manual del Seguridad del SGSI
- Diseño de la Metodología para la Continuidad y Contingencia del Negocio
- Diseño de Procedimientos Normativos del Sistema de Gestión
- Diseño de Formularios del Sistema de Gestión

- Diseño de Planes y Programas del Sistema
- Diseño del Sistema de Información Gerencial

Todas estas actividades han sido desarrolladas en el presente Trabajo de Graduación, por lo que no representan un costo en el que deba incurrir CEL, pero se incluirá para propósitos de conocer los costos que comprenden el Proyecto.

El costo de Diseño se refiere al pago de Honorarios a 3 consultores por el Diseño del SGSI, el cual es calculado en base al pago de un Consultor en Sistemas de Gestión de Calidad. (Consejo Nacional de Ciencia y Tecnología, CONACYT[22]).

ACTIVIDADES	DURACIÓN	COSTO DIARIO INDIVIDUAL ($)	COSTO TOTAL ($) 3 CONSULTORES
▪ Análisis general de los procesos claves y de apoyo.	10 Días	$ 60 x 10 = 600.00	$ 1,800.00
▪ Caracterización de cada una de las Áreas (personal, usuarios, maquinaria y equipo, materiales, actividades de trabajo y condiciones actuales de trabajo)	15 Días	$ 60 x 15 = 900.00	$ 2,700.00
▪ Evaluación y Valoración de Riesgos de los activos	20 Días	$ 60 x 20 = 1,200.00	$ 3,600.00
▪ Diseño del Manual del Seguridad del SGSI ▪ Diseño de Metodología para la Continuidad y Contingencia del Negocio	20 Días	$ 60 x 20 = 1,200.00	$ 3,600.00
▪ Diseño de Procedimientos Normativos del Sistema de Gestión ▪ Diseño de Formularios del Sistema de Gestión ▪ Diseño de Planes y Programas del Sistema ▪ Diseño del Sistema de Información Gerencial	60 Días	$ 60 x 60 = 3,600.00	$ 10,800.00
		TOTALES	**$ 22,500.00**

.

Tabla 70: Costos del diseño del SGSI.

Como se observa en la Tabla el Costo del Diseño del SGSI es de **$ 22,500.00** , pero CEL no incurrirá en estos costos puesto que los tres consultores que han desarrollado este diseño son los estudiantes integrantes de este Trabajo de Graduación.

2. Costos de capacitación

Los Costos de Capacitación se dividen de la siguiente manera:

- Costos de Capacitación a las Autoridades de CEL
- Costos de Capacitación a las áreas involucradas en el proyecto

Los cursos de capacitación serán gestionados con apoyo de INSAFORP, esta institución ofrece dos tipos de cursos:

[22] Fuente: CONACYT

- ✓ Cursos de capacitación Abierta: son aquellos solicitados por empresas externas en los que pueden participar personas que pertenezcan o no a la empresa misma. .
- ✓ Cursos de capacitación Cerrada: son aquellos solicitados por empresas externas en los que solo participa personal propio de la empresa, en los que se tratarán temas o problemas específicos de la misma.

CUADRO RESUMEN DE POLÍTICAS DE APOYO DE INSAFORP

TIPO DE CURSO	**POLÍTICAS DE APOYO (CURSOS ABIERTO)**	
I. CURSOS ABIERTOS	CURSOS ADMINISTRATIVOS	CURSOS TÉCNICOS
A) EN EL PAÍS	De 8 hasta 24 horas	De 8 hasta 40 horas
Número de horas		
% de apoyo sobre el costo de participación	Hasta 60%	Hasta 60%
	(Independientemente del nivel organizativo)	(Independientemente del nivel organizativo)
Número de personas propuestas a apoyar	HASTA 2 NIVEL DIRECTIVO Y HASTA 5 NIVEL OPERATIVO	HASTA 2 NIVEL DIRECTIVO Y HASTA 5 NIVEL OPERATIVO
B) EN EL EXTRANJERO	De 8 hasta 24 horas	De 8 hasta 40 horas
Número de horas		
% de apoyo sobre el costo de participación	Hasta 30%	Hasta 50%
	(Independientemente del nivel organizativo)	(Independientemente del nivel organizativo)
Número de personas de acuerdo a nivel	HASTA 2 NIVEL DIRECTIVO Y HASTA 2 NIVEL OPERATIVO	HASTA 2 NIVEL DIRECTIVO Y HASTA 2 NIVEL OPERATIVO
II. CURSOS CERRADOS	**POLÍTICAS DE APOYO (CURSOS CERRADOS)**	
Número de horas	De 8 hasta 120 Horas	De 8 hasta 180 Horas
Número de grupos a apoyar	Sujeto a análisis	Sujeto a análisis
Número de personas por grupo	Sujeto a análisis	Sujeto a análisis
% de apoyo		
■ Proveedor Nacional	Hasta 85% de honorarios y material didáctico	Hasta 85% de honorarios y material didáctico
■ Proveedor Extranjero	Hasta 85% de honorarios y material didáctico	Hasta 85% de honorarios y material didáctico

Tabla 71: Políticas de apoyo de Insaforp.

Según la clasificación anterior las capacitaciones solicitadas por CEL para la implementación del SGSI serán cerradas, participando personal de la empresa únicamente.
Dentro de las políticas de capacitación y los acuerdos entre INSAFORP y CEL el monto a cubrir por parte de INSAFORP[23] es del 70%[24], por lo que CEL solo desembolsara el 30% de las mismas.
Cabe decir que este apoyo es indiferente cuando se refiere capacitaciones para mandos altos, medios u operativos. Solo se necesita especificar en el formulario de acción formativa[25] el nivel organizacional de los participantes.

a) Costos de Capacitación a las Autoridades de CEL[26]

i. Costo de capacitación.

El Costo de Capacitación se calculará a partir de la siguiente fórmula:
Costo de Capacitación = Costo de Consultor/ hr Capacitac. Por persona + Costo de Oportun. Hr Hombre por Capacitación + Costo de papelería y refrigerio.

TITULO DEL CURSO	DIAS	TIEMPO DIARIO	TIEMPO TOTAL
Capacitación y Taller con niveles estratégicos en Gestión y Manejo de la seguridad de la información	4	60 min	4 h

Tabla 72: Curso de capacitación para las autoridades de CEL.

A continuación se presenta el contenido temático de cada uno de los cursos a impartir.

1. Sensibilización sobre las Norma ISO 27000

Nº	Contenido
1	• Propósito y ámbito de aplicación de la Norma ISO
2	• Elementos del sistema de gestión en base a la Norma ISO

Tabla 73: Contenido del curso de capacitación No1 para las autoridades de CEL.

[23] Fuente: Area de capacitaciones de CEL. Lic. Azucena tel 2211 6000

[24] Ver Anexo 15: Cotización de capacitaciones y el monto que Insaforp absorbe de la misma.

[25] Ver Anexo 16: Formulario de Accion Formativa F-8 INSAFORP

[26] Ver Anexo 17: Programa de Capacitaciones del personal de CEL

2. Definición General del SGSI

Nº	Contenido
1	• Manual general del sistema de Gestión
2	• Procedimientos del sistemas de gestión
3	• Planes y programas del sistema de Gestión
4	• Metodología para la continuidad y contingencia del negocio
5	• Diseño del Sistema Información Gerencial

Tabla 74: Contenido del curso de capacitación No2 para las autoridades de CEL.

3. Implementación del Sistema de Gestión

Nº	Contenido
1	• Evaluaciones del Proyecto
2	• Actividades de implantación (Duración y responsabilidades)
3	• Control de la implantación y cronograma de actividades

Tabla 75: Contenido del curso de capacitación No3 para las autoridades de CEL.

Cu**adro Resumen**

Nº	TÍTULO DEL CURSO
1	Sensibilización sobre las Normas ISO 27000
3	Definición General del SGI
3	Implementación del Sistema de Gestión

Tabla 76: Resumen de cursos de capacitación para las autoridades de CEL.

A continuación se presenta el costo por la capacitación, el cual se determina en base al contenido y tiempo invertido, el pago al consultor se calcula a partir de información proporcionada por INSAFORP, siendo de $ 90 dólares por hora y por capacitado.

Cantidad de personas	Horas por persona	Total de horas	Pago de consultor por hora	Total del costo del curso	Costo a pagar por CEL (30% del total)
5	4 hr	20 hr	$ 90	$ 1,800.0	$540.0

Tabla 77: Costo de cursos de capacitación para las autoridades de CEL.

El Costo Total por la Capacitación a Autoridades de CEL de acuerdo a las Políticas de INSAFORP es de $270.

ii. Costo de Papelería y Refrigerio

Nº	TÍTULO DEL CURSO	N. de Copias
1	Sensibilización sobre las Normas ISO 27000	100
2	Definición General del SGSI	120
3	Implementación del Sistema de Gestión	150
	TOTAL DE COPIAS	**370**
	COSTO DE COPIAS ($0.02)	**$7.4**

Tabla 78: Costo de papelería de cursos de capacitación para las autoridades de CEL.

N. de Cursos	N. de personas por curso	N. de sesiones por curso	N. de Refrigerios
3	5	1	15
COSTO DE REFRIGERIOS ($2.0 C/U)			**$30.0**

Tabla 79: Costo de refrigerios de cursos de capacitación para las autoridades de CEL.

Costo de Capacitación = Costo de Consultor/ hr Capacitac. por persona + Costo de papelería y refrigerios

COSTO DE CAPACITACIÓN A AUTORIDADES Y REPRESENTANTES DE LAS UNIDADES	
RUBRO	**DESEMBOLSO**
COSTO (DESEMBOLSO) DE LA CAPACITACIÓN	**$ 540**
COSTO DE PAPELERIA Y REFRIGERIOS	**$37.4**
TOTAL	**$ 577.4**

Tabla 80: Costo total de cursos de capacitación para las autoridades de CEL.

b) Costos de Capacitación a las áreas involucradas en el proyecto[27]

i. Costos de Capacitación

El Costo de Capacitación se calculará a partir de la siguiente fórmula:
Costo de Capacitación = Costo de Consultor/ hr Capacitac. Por persona + Costo de Oportun. Hr Hombre por Capacitación + Costo de papelería y refrigerio.

A continuación se presenta en resumen la temática de las capacitaciones, así como también la duración de cada uno de ellos:

[27] Ver Anexo 17: Programa de Capacitaciones para el personal de CEL

Titulo del curso	Dias	Tiempo diario	Tiempo total
Capacitación: analizáis y evaluación del riesgo.	5	45 min	5 h
Capacitación: Políticas de seguridad de la información y objetivos	5	30 min	2.5 h
Capacitación y Taller: Evaluación de las opciones para el tratamiento de riesgo	7	30 min	3.5 h
Capacitación y Taller: Selección de controles y objetivos de control	7	30 min	3.5 h
Capacitacion: Declaracion de Aplicabilidad	5	30 min	2.5 h
Capacitación y taller: Análisis de riesgo y escenarios de amenazas	7	30 min	3.5 h
Capacitación y Taller: Estrategias de continuidad.	5	30 min	2.5 h
Capacitación y taller: Plan de reanudación de operaciones	5	30 min	2.5 h
Capacitación :Plan de tratamiento de riesgos	6	30 min	3 h
Capacitación y taller : efectividad de controles y métricas	5	30 min	2.5 h
Capacitación y Taller: Incidentes y eventos de seguridad	5	30 min	2.5 h
Capacitación y taller: revisiones periódicas del SGSI	5	30 min	2.5 h
Capacitación: Como Implementar Las Acciones Correctivas y Preventivas	5	30 min	2.5 h
Capacitación: Manual de seguridad de la información.	5	30 min	2.5 h
TOTAL			40 h

Tabla 81: Curso de capacitación para las áreas involucradas en el proyecto.

El contenido temático de los cursos a impartir es el siguiente:

1. Evaluación y Valoración de Riesgos

Nº	Contenido
1	• Descripción de la metodología

Tabla 82: Contenido del curso de capacitación No1 para las áreas involucradas en el proyecto.

2. Requisitos de las Normas ISO 27000

Nº	Contenido
1	• Requerimientos generales del sistema
2	• Política de seguridad

3	• Planificación del sistema de Gestión
4	• Puesta en práctica y funcionamiento del Sistema
5	• Comprobación y acción correctora del sistema

Tabla 83: Contenido del curso de capacitación No2 para las áreas involucradas en el proyecto.

3. Documentación del Sistema de Gestión

Nº	Contenido
1	• Elaboración y codificación de documentos del sistema
2	• Control de documentación
3	• Actualización de documentación
4	• Uso de procedimientos del sistema
5	• Uso de Formularios del sistema
6	• Uso de planes y programas

Tabla 84: Contenido del curso de capacitación No3 para las áreas involucradas en el proyecto.

Resumen de cursos

Nº	MÓDULO
1	▪ Evaluación y Valoración de Riesgos.
2	▪ Requisitos de las Norma ISO 27000
3	▪ Documentación del Sistema de Gestión

Tabla 85: Resumen de cursos de capacitación para las áreas involucradas en el proyecto.

A continuación se presenta el costo por la capacitación, el cual se determina en base al contenido y tiempo invertido, el pago al consultor se calcula de acuerdo a la información proporcionada por INSAFORP, el cual es de $ 90 dólares por hora y por capacitado.

Cantidad de personas	Horas por persona	Total de horas	Pago de consultor por hora	Total del costo del curso	Costo a pagar por CEL (30% del total)
6	40 hr	240 hr	$ 90	$ 21,600.0	$6480

Tabla 86: Costo de cursos de capacitación para las áreas involucradas en el proyecto

El Costo Total por la Capacitación del personal de las áreas involucradas en el proyecto de acuerdo a las Políticas de INSAFORP es de $3,240.0

ii. Costo de Papelería y Refrigerio

Nº	TÍTULO DEL CURSO	N. de Copias
1	Evaluación y Valoración de Riesgos	150
2	Requisitos de las Normas ISO 27000	200
3	Documentación del Sistema de Gestión	350
	TOTAL DE COPIAS	**600**
	COSTO DE COPIAS ($0.02)	**$ 12.0**

Tabla 87: Costo de papelería de cursos de capacitación para las áreas involucradas en el proyecto

N. de Cursos	N. de personas por curso	N. de sesiones por curso	N. de Refrigerios
3	20	1	60
COSTO DE REFRIGERIOS ($3.0 C/U)			**$180**

Tabla 88: Costo de papelería de cursos de capacitación para las áreas involucradas en el proyecto.

Costo de Capacitación = Costo de Consultor/ hr Capacitac. por persona + Costo de papelería y refrigerios

COSTOS DE CAPACITACIÓN A LAS ÁREAS INVOLUCRADAS EN EL PROYECTO	
RUBRO	**DESEMBOLSO**
Costo (desembolso) de la capacitación	**$ 6,480.0**
Costo de papelería y refrigerios	**$ 192.0**
TOTAL	**$ 6,672.0**

Tabla 89: Costo total de cursos de capacitación para las áreas involucradas en el proyecto.

El Costo Total por la capacitación dirigida al personal de las áreas involucradas en el proyecto es de $ 3,432.0

En la siguiente tabla se resume el Desembolso a realizar por Capacitaciones:

TIPO DE CAPACITACIÓN	DESEMBOLSO
Capacitación a Autoridades de CEL	$ 577.4
Capacitación al personal de las aéreas involucradas	$6,672.0
TOTAL COSTO CAPACITACIÓN	**$ 7,249.40**

Tabla 90: Costo total de cursos de capacitación para CEL.

3. Costo de equipo, materiales, servicios e instalaciones

Se refiere al equipamiento de de cada una de las áreas.

COSTO (DESEMBOLSO)			
OBRA CIVIL			
OFICINA	**CANTIDAD**	**COSTO UNITARIO ($)**	**COSTO TOTAL ANUAL ($)**
Oficina con sistema eléctrico y servicios básicos	1	1,200	14,400.0
		SUB-TOTAL	**14,000.0**
SERVICIOS BASICOS			
SERVICIOS	**CANTIDAD**	**COSTO UNITARIO ($)**	**COSTO TOTAL ANUAL ($)**
Energía Eléctrica	1	55	660
Agua potable	1	15	180
Servicio de telefonía	1	50	600
Servicio de internet	1	45	540
Licencia antivirus	6	200	1200
Licencia de Windows	6	150	900
		SUB-TOTAL	**$ 4,080.0**
EQUIPO Y MOBILIARIO			
EQUIPO Y MOBILIARIO	**CANTIDAD**	**COSTO UNITARIO ($)**	**COSTO TOTAL ($)**
Computadoras de escritorio	6	$ 500	$3,000
Computadora portátil	1	$800	$800
Escritorios	6	$125	$750
Sillas	6	$30	$180
Aparatos telefónicos	**6**	**$15**	**$90**
Servidor	1	$6000	$6000
Impresor	1	$80	$80
Fotocopiadora	1	$200	$200
Escáner	1	$125	$125
Aire acondicionado	**1**	**$400**	**$400**
Archiveros con llave	3	$150	$450
Estante	1	$50	$50
Mesa de reunión	1	$250	$250
		SUB-TOTAL	**$12,125.0**
		TOTAL	**$30,205**

Tabla 91: Costo Total de equipo, materiales, servicios e instalaciones.

De la Tabla anterior obtenemos un Total de costos de $30,205.0

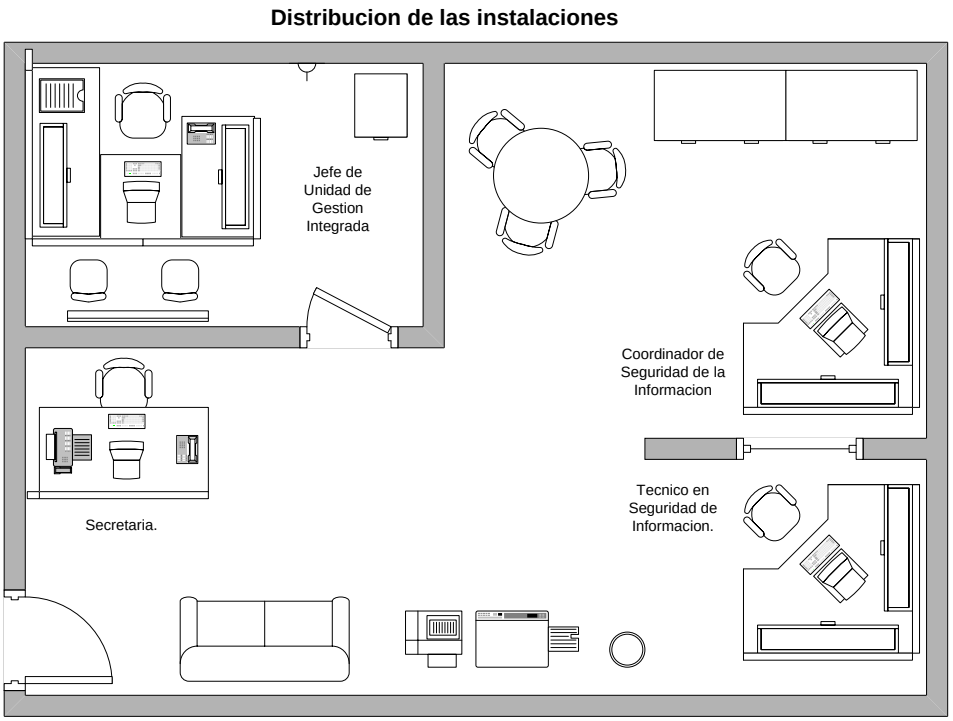


Figura 46: Distribución de la Instalaciones.

4. Costo de documentación

Este costo se refiere a la impresión y fotocopias necesarias de los documentos que componen el Sistema de Gestión, para ponerlo en Operación.
Los documentos serán entregados a la Unidad de Gestión Integrada de CEL.

COSTO (DESEMBOLSO) DE DOCUMENTACIÓN				
TIPO DE GASTO	CANTIDAD	Nº PÁG.	COSTO UNITARIO	COSTO TOTAL
Documento Diseño del SGSI	2	200	$ 0.06	$ 24.0
Manual de Seguridad - CEL	2	50	$ 0.06	$ 6.0
Metodología para la Continuidad y Contingencia del Negocio	2	52	$ 0.06	$ 6.24
Procedimientos normativos	18	250	$ 1.50	$ 540.0
			TOTAL	**$ 560.24**

Tabla 92: Costo total de documentación.

El Desembolso en Documentación del Sistema de Gestión que debe hacerse para la implantación, como se observa en la Tabla V.19 es de **$ 560.24**

5. Costos del sistema de información gerencial

Este costo se refiere al pago del programador que se encargo de desarrollar y l llevar el sistema de Información en lenguaje Visual Fox pro.

COSTO DE PROGRAMADOR VISUL FOX			
Producto	Cantidad	Costo unitario	Costo total
Menú	1	$ 10.0	$ 10.0
Base de datos	1	$ 150.0	$ 150.0
Formularios	30	$ 8.0	$ 240.0
Consultas y reportes	10	$ 8.0	$ 80.0
TOTAL			$ 480.0

Tabla 93: Costo total del Sistema de Información Gerencial.

En total el costo por programar el Sistema de Información Gerencial fue de **$ 480.0**

6. Costos de la estructura organizativa de la Administración del proyecto:

La estructura propuesta es la siguiente y se contratara durante un periodo de 10 meses, a tiempo completo realizando estrictamente actividades de implantación:

PUESTO	SALARIO MENSUAL (Incluye prestaciones)	SALARIO ANUAL
Jefe de Unidad de Gestión Integrada	$1,733.92	**$17,339.2**
Gerente del proyecto	$1,173.08	**$11,730.8**
Asesor Externo	$948.75	**$9,487.5**
	TOTAL	**$38,557.5**

Tabla 94: Costo total de planilla de la administración del Proyecto.

7. Costos de la Certificación

De acuerdo a datos proporcionados por la UACI de CEL el costo por contratar a una empresa certificadora en este caso a AENOR para realizar todas las auditorias, y obtención de la certificación bajo ISO 27000 asciende a un total de **$ 27,830.00**

8. Resumen de costos de inversión

La siguiente tabla presenta el total de los Costos de Inversión para implementar el SGSI

COSTO (DESEMBOLSO) DE INVERSIÓN	
RUBRO	COSTO
Costos de Capacitación a las Autoridades de CEL	$ 577.4
Costos de Capacitación al personal de las aéreas involucradas	$6,672.0
Costo de Equipo, materiales, servicios e instalaciones	$30,205

Costo de Documentación	$560.24
Costos del Sistema de Información Gerencial	$ 480.0
Costos de la estructura organizativa de la Administración del proyecto	$ 38,557.5
Costos de la Certificación	$ 27,830
TOTAL	**$ 104,882.14**

Tabla 95: Costo total de inversión del proyecto.

Por lo tanto, CEL tendría que efectuar un **desembolso** de **$ 104,882.14**, para implantar el Sistema de Gestión en términos de inversión inicial

C. COSTOS DE OPERACIÓN

Los Costos de Operación del SGSI en son los que año con año CEL incurrirá en el funcionamiento permanente del Sistema de Gestión, están constituidos por los Costos por la utilización permanente de los Formularios generados en el Sistema, los Costos de Planilla.

1. Costo de papelería/documentos del sistema

Este Costo lo constituyen las Fotocopias necesarias de los diversos Formularios utilizados por el Sistema, para un año.

Cantidad de formularios	Cantidad total de copias	Costo unitario de copias	Costo total anual
22	2500	$ 0.02	$ 50

Tabla 96: Costo de papelería y documentación del sistema.

Como se observa se CEL tendrá un **desembolso** anual de **$50** en Copias de los Formularios, las cuales serán utilizadas por las Unidades para llevar a cabo los diferentes procedimientos del SGSI

2. Costos de salarios de la estructura organizativa de operación[28] del SGSI

Para determinar los costos de la planilla se ha tomado como referencia los salarios promedio que tienen los trabajadores del sector industrial.
Cabe destacar que es necesario crear toda una estructura que soporte el SGSI para no sobre cargar de tareas de las personas que actualmente se desempeñan en los otros Sistemas de Gestión que CEL posee.
Estas personas serán contratadas a tiempo completo con jornadas laborales de acuerdo a las políticas de contratación de personal del Área de reclutamiento de personal de CEL.
Cabe decir que CEL ya cuenta con Alta Gerencia y no será tomada en la estructura de costos, solo se tomo en el organigrama para efectos de representar mandos jerárquicos.

[28] Ver Anexo 18: Manual de funciones para la operación del SGSI

PUESTO	SALARIO	ISSS (7.5%)	AFP (6.75%)	Aguinaldo (15 días de salario/12)	Vacaciones (30% de salario quincenal/12)	SALARIO MENSUAL (Incluye prestaciones)	SALARIO ANUAL
Jefe de Unidad de Seguridad de la Información	$1,500.00	$51.42	$101.25	$62.50	$18.75	$1,733.92	$ 20,807.04
Coordinador del SGSI	$1,000.00	$51.42	$67.50	$41.66	$12.50	$1,173.08	$ 14,076.96
Técnico de SGSI de producción	$800.00	$51.42	$54.00	$33.33	$10.00	$948.75	$ 11,385.00
Técnico de SGSI de comercialización	$800.00	$51.42	$54.00	$33.33	$10.00	$948.75	$ 11,385.00
Técnico de SGSI de Gestión de la Información	$800.00	$51.42	$54.00	$33.33	$10.00	$948.75	$ 11,385.00
Técnico de SGSI de RRHH	$800.00	$51.42	$54.00	$33.33	$10.00	$948.75	$ 11,385.00
TOTAL							**$ 80,424.00**

Tabla 97: Costo total de planilla de operación del Proyecto.

Para determinar el Costo Real de Pago de Planilla del personal que se asignara al Sistema, se han tomado en cuenta las prestaciones siguientes:

- ✓ ISSS (7.5 % que aporta el Patrono), es de aclarar que se cotiza y se recibe prestaciones sobre un límite de $ 685.71 según la Ley del Seguro Social (Reglamento para la Aplicación del Régimen del Seguro Social Decreto No 37 Capítulo II)
- ✓ AFP (6.75% que aporta el Patrono)
- ✓ Aguinaldo (10 días del salario mensual según Art. 198 del código de trabajo)
- ✓ Vacaciones (30% del salario quincenal según Art. 177 del código de trabajo)

Al agregar las prestaciones al salario se tendrá los costos reales de Planilla, los cuales se calculan en base a la siguiente Fórmula:

Costo Real de M. O. = Salario + ISSS (7.5%) + AFP (6.75%) + Aguinaldo + Vacaciones

Como se observa en la Tabla el desembolso que se habrá de efectuar para el pago de la planilla es de **$ 80,424.00** para un año de operación del sistema.

3. Resumen de costos de operación

En la Tabla se muestra el Costo de Operación al Implementar el SGSI en CEL

COSTOS (DESEMBOLSOS) DE OPERACIÓN	
RUBRO	COSTO ANUAL
Costo de Formularios del Sistema	$ 50.0
Costo de Equipo de Protección Personal	$80,424.00
TOTAL	**$80,474.0**

Tabla 98: Costo total operativos del SGSI.

Los Costos de Operación representan la inversión para el primer año de funcionamiento del Sistema de Gestión, siendo un total de **$80,474.0**

D. BENEFICIOS ECONÓMICOS DEL SISTEMA DE GESTIÓN

Los beneficios que se obtendrán con la implantación del SGSI se verán reflejados en la Disminución de las pérdidas económicas ocasionadas por el mal manejo y falta de seguridad de la información, para ello se utilizaron de referencia las perdidas reales ocasionadas por mal manejo de la información descritas en la pagina 133, que ascendieron a $ 1, 479,000.00. Pero para efectos analíticos se han suavizado los datos despreciando aquellos que se clasifican en costos de oportunidad, los cuales son los datos #: 2, 4 y 5. Totalizando un promedio de perdidas para el periodo 2007-2008 de $153,250.00

En base a la experiencia de las certificaciones anteriores se puede encontrar que, al cuantificar el cumplimiento de los objetivos globales durante los primeros tres anos se obtuvieron los siguientes índices:*

CERTIFICACIONES	% DE CUMPLIMIENTO DE OBJETIVOS AL PRIMER ANO	% DE CUMPLIMIENTO DE OBJETIVOS AL SEGUNDO ANO	% DE CUMPLIMIENTO DE OBJETIVOS AL TERCER ANO
ISO 9000	78	90	100
ISO 14000	86	95	100
ISO 18000	85	95	100
PROMEDIOS	**83**	**93**	**100**

(Fuente: Documentos de auditoría interna de la unidad de gestión Integrada)

Tabla 99: Porcentaje de cumplimiento de objetivos en la Implantación de Sistemas de Gestión de CEL

*Las conclusiones del porque de la diferencia de los índices se debieron a la variabilidad de la curva de aprendizaje así como la experiencia del personal por tener certificaciones anteriores; con relación a la ISO 18000 por lo diferente de la norma se obtuvo al primer ano un punto porcentual debajo de la certificación anterior (ISO 14000).

Factores a los que se debe el cambio de porcentaje de cumplimiento de metas y objetivos.

- ISO 9000 fue el primer sistema que la comisión obtuvo certificación, fue un campo nuevo parar mucho del personal de la comisión.
- La resistencia al cambio se dio más en la primera certificación que en las segundas obtenidas
- El mejoramiento de los índices que podemos observar en la segunda y tercera certificaciones se da gracias a la familiarización que el personal tiene ya con los sistemas integrados de calidad y la base de una norma ISO

Al implementar el SGSI se considerará una Disminución del 83% para el primer año de Gestión como resultado de una proyección generada en base al promedio de certificaciones anteriores considerando que una debida aplicación e implantación del SGSI reduciría los incidentes de seguridad de información.

En el siguiente cuadro de han proyectado los ahorros que se obtendrán al implementar el SGSI en base al cumplimiento de los objetivos que la institución posee por promedio de estadísticas anteriores

Año	% esperado de Reducción de perdidas	Pérdidas promedio ocasionadas por el mal manejo y falta de seguridad de la información.	Pérdidas proyectadas ocasionadas por el mal manejo y falta de seguridad de la información.	Ahorro Anual estimado	Beneficios Esperados del SGSI
2010	83%	$153,250.00	$26,052.50	$127,197.50	$101,145.00
2011	93%	$153,250.00	$10,727.50	$142,522.50	$131,795.00
2012	100%	$153,250.00	$0.00	$153,250.00	$153,250.00

Tabla 100: Beneficios esperados del SGSI

Los Beneficios Económicos en el primer año de implementación del SGSI en los procesos claves y de apoyo son de **$ 101,145.00**

9. Comparación entre los beneficios y los costos de operación anuales

AÑO	BENEFICIO	COSTO
2010	$101,145.00	$80,474.00
2011	$131,795.00	$80,474.00
2012	$153,250.00	$80,474.00
TOTALES	$386,190.00	$241,422.00

Tabla 101: Beneficios y Costos del SGSI

Como los beneficios económicos están dados a lo largo de tres años de operación del sistema, se tendrán que traer al presente para calcular el valor del Beneficio – Costo, para lo cual es necesario calcular una TMAR (Tasa Mínima Atractiva de Retorno)

10. Cálculo de la TMAR

La TMAR utilizada en el proyecto está basada en la tasa aplicada a los empréstitos autorizados por el Ministerio de Hacienda en materia de apoyo a instituciones públicas con el plazo de tres años. Esta tasa es del 7.5% anual. El valor de la TMAR no tiene adicionada una tasa de premio al riesgo, debido a que CEL es una institución con suficiente estabilidad para poder asumir riesgos de inversión.

La fórmula de Beneficio – Costo viene dada por la siguiente fórmula:

$$B/C = \frac{Ingresos\_Actualizados}{Egresos\_Actualizados} = \frac{\sum_{1}^{n} \frac{ING}{(1+Tmar)^n}}{\sum_{1}^{n} \frac{EGR}{(1+Tmar)^n}}$$

TMAR= 7.50%

AÑO	BENEFICIO	COSTO	Ingresos Actualizados	Egresos Actualizados
2010	$101,145.00	$80,474.00	$94,088.37	$74,859.53
2011	$131,795.00	$80,474.00	$114,046.51	$69,636.78
2012	$153,250.00	$80,474.00	$123,360.21	$64,778.40
		∑	$331,495.09	$209,274.71

Tabla 102: Beneficios y costos actualizados del SGSI

B/C= $331,495.00/$209,274.71= 1.58

Luego el Beneficio Costo es de B/C: 1.58, por lo cual bajo este análisis se ACEPTA el Proyecto.

11. Tiempo de Recuperación de la Inversión (TRI)

Es el tiempo en el cual se espera se recupere la inversión hecha en el proyecto, dicho valor se calcula mediante la siguiente fórmula:

$$TRI = \frac{InversionInicial}{BeneficiosActualizados} = \frac{InversionInicial}{\frac{BeneficiosActualizadosTotales}{3anos}} = \frac{\$101{,}679.54}{\frac{\$331.495.09}{3}} = 0.92anos$$

Aplicando la formula anterior se tiene que la TRI para el proyecto es de 0.92 anos, traducido en meses nos da un aproximado de 11.04 meses, lo cual indica que el tiempo de recuperación es menor que un año, con lo que concluimos que es proyecto es factible.

E. ESCENARIOS ECONÓMICOS PARA CEL

A lo largo del capítulo se ha abordado el enfoque de costo que genera la implantación del SGSI
Pero resultaría muy interesante realizar un análisis de sensibilidad sobre como los beneficios del SGSI contrarrestaran las pérdidas económicas por falta de seguridad de información, desde el punto de vista positivo y negativo.

12. Análisis de escenarios económicos

Escenario 1

Escenario: Al implementar el SGSI se considerará una Disminución del 78% para el primera año de Gestión, y 90 % para el segundo año, lo que representa según las estadísticas el porcentaje más bajo y que se dio con la primera acreditación donde el personal comienza a adaptarse a las normas ISO.
En el siguiente cuadro de han proyectado los ahorros que se obtendrán al implementar el SGSI

Año	% esperado de Reducción de perdidas	Pérdidas promedio ocasionadas por el mal manejo y falta de seguridad de la información.	Pérdidas proyectadas ocasionadas por el mal manejo y falta de seguridad de la información.	Ahorro Anual estimado	Beneficios Esperados del SGSI
2010	78%	$153,250.00	$33,715.00	$119,535.00	$85,820.00
2011	90%	$153,250.00	$15,325.00	$137,925.00	$122,600.00
2012	100%	$153,250.00	$0.00	$153,250.00	$153,250.00

Tabla 103: Beneficios esperados del SGSI del escenario No1.

c) Comparación entre los Beneficio y los Costos de Operación anuales

AÑO	BENEFICIO	COSTO
2010	$85,820.00	$80,474.00
2011	$122,600.00	$80,474.00
2012	$153,250.00	$80,474.00
TOTALES	$361,670.00	$241,422.00

Tabla 104: Beneficios y Costos del SGSI del escenario No 1.

Como los beneficios económicos están dados a lo largo de tres años de operación del sistema, se tendrán que traer al presente para calcular el valor del Beneficio – Costo, para lo cual es necesario calcular una TMAR (Tasa Mínima Atractiva de Retorno)

d) Cálculo de la TMAR

La TMAR utilizada en el proyecto está basada en la tasa aplicada a los empréstitos autorizados por el Ministerio de Hacienda en materia de apoyo a instituciones públicas con el plazo de tres años. Esta tasa es del 7.5% anual. El valor de la TMAR no tiene adicionada una tasa de premio al riesgo, debido a que CEL es una institución con suficiente estabilidad para poder asumir riesgos de inversión.

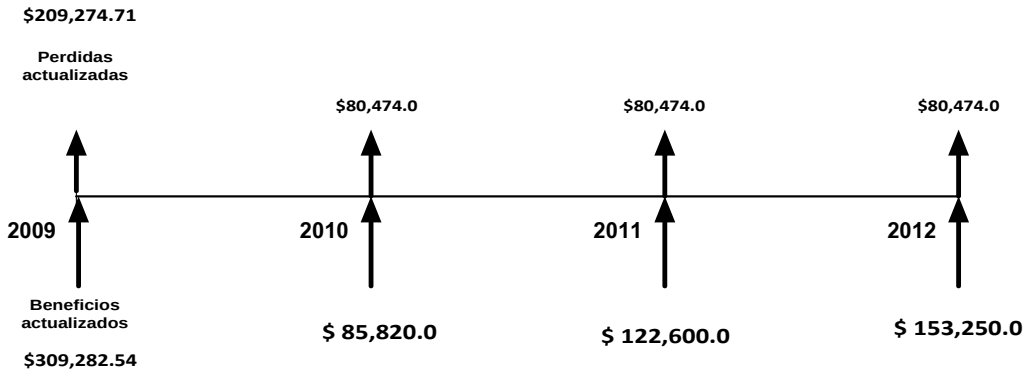
La fórmula de Beneficio – Costo viene dada por la siguiente fórmula:

$$B/C = \frac{Ingresos\_Actualizados}{Egresos\_Actualizados} = \frac{\sum_{1}^{n} \frac{ING}{(1+Tmar)^n}}{\sum_{1}^{n} \frac{EGR}{(1+Tmar)^n}}$$

TMAR= 7.50%

AÑO	BENEFICIO	COSTO	Ingresos Actualizados	Egresos Actualizados
2010	$85,820.00	$80,474.00	$79,832.56	$74,859.53
2011	$122,600.00	$80,474.00	$106,089.78	$69,636.78
2012	$153,250.00	$80,474.00	$123,360.21	$64,778.40
		∑	$309,282.54	$209,274.71

Tabla 105: Beneficios y costos actualizados del SGSI del escenario No. 1



B/C= $309,282.54/$209,274.71= 1.48

Luego el Beneficio Costo es de B/C: 1.48, por lo cual bajo este análisis se ACEPTA el Proyecto.

e) Tiempo de Recuperación de la Inversión (TRI)

Es el tiempo en el cual se espera se recupere la inversión hecha en el proyecto, dicho valor se calcula mediante la siguiente fórmula:

$$TRI = \frac{InversionInicial}{BeneficiosActualizados} = \frac{InversionInicial}{\frac{BeneficiosActualizadosTotales}{3anos}} = \frac{\$101{,}679.54}{\frac{\$309{,}282.00}{3}} = 0.99anos$$

Aplicando la formula anterior se tiene que la TRI para el proyecto es de 0.99 anos, traducido en meses nos da un aproximado de 11.88 meses, lo cual indica que el tiempo de recuperación es menor que un ano, con lo que concluimos que es proyecto es factible.

Escenario 2

Escenario: Al implementar el SGSI se considerará un porcentaje similar al de la ultimo estándar ISO 18000 del 85% para el primera año de Gestión, 95% para el segundo año y 100% para el tercer año, lo que para CEL es un escenario moderno
En el siguiente cuadro de han proyectado los ahorros que se obtendrán al implementar el SGSI

Año	% esperado de Reducción de perdidas	Pérdidas promedio ocasionadas por el mal manejo y falta de seguridad de la información.	Pérdidas proyectadas ocasionadas por el mal manejo y falta de seguridad de la información.	Ahorro Anual estimado	Beneficios Esperados del SGSI
2010	85%	$153,250.00	$22,987.50	$130,262.50	$107,275.00
2011	95%	$153,250.00	$7,662.50	$145,587.50	$137,925.00
2012	100%	$153,250.00	$0.00	$153,250.00	$153,250.00

Tabla 106: Beneficios esperados del SGSI del escenario No 2.

f) Comparación entre los Beneficio y los Costos de Operación anuales

AÑO	BENEFICIO	COSTO
2010	$107,275.00	$80,474.00
2011	$137,925.00	$80,474.00
2012	$153,250.00	$80,474.00
TOTALES	$398,450.00	$241,422.00

Tabla 107: Beneficios y Costos del SGSI del escenario No 2.

Como los beneficios económicos están dados a lo largo de tres años de operación del sistema, se tendrán que traer al presente para calcular el valor del Beneficio – Costo, para lo cual es necesario calcular una TMAR (Tasa Mínima Atractiva de Retorno)

g) Cálculo de la TMAR

La TMAR utilizada en el proyecto está basada en la tasa aplicada a los empréstitos autorizados por el Ministerio de Hacienda en materia de apoyo a instituciones públicas con el plazo de tres años. Esta tasa es del 7.5% anual. El valor de la TMAR no tiene adicionada una tasa de premio al riesgo, debido a que CEL es una institución con suficiente estabilidad para poder asumir riesgos de inversión.

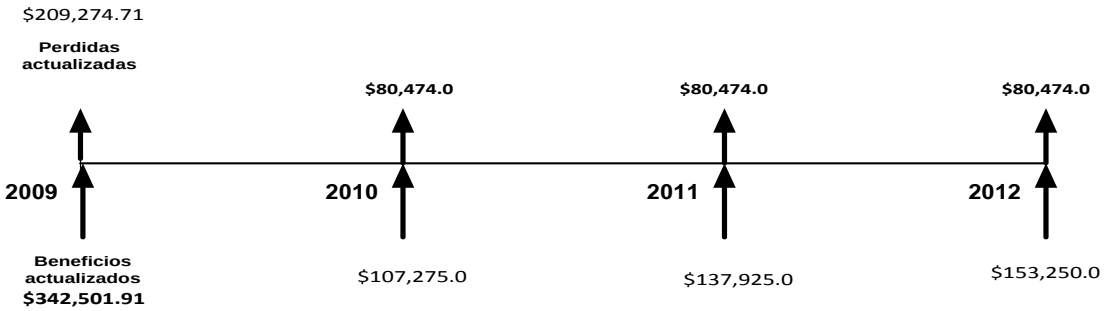
La fórmula de Beneficio – Costo viene dada por la siguiente fórmula:

$$B/C = \frac{Ingresos\_Actualizados}{Egresos\_Actualizados} = \frac{\sum_{1}^{n} \frac{ING}{(1+Tmar)^n}}{\sum_{1}^{n} \frac{EGR}{(1+Tmar)^n}}$$

TMAR= 7.50%

AÑO	BENEFICIO	COSTO	Ingresos Actualizados	Egresos Actualizados
2010	$107,275.00	$80,474.00	$99,790.70	$74,859.53
2011	$137,925.00	$80,474.00	$119,351.00	$69,636.78
2012	$153,250.00	$80,474.00	$123,360.21	$64,778.40
		∑	$342,501.91	$209,274.71

Tabla 108: Beneficios y costos actualizados del SGSI del escenario No. 2



B/C= $342,501.91/$209,274.71= 1.64

Luego el Beneficio Costo es de B/C: 1.64, por lo cual bajo este análisis se acepta el proyecto, en los primeros tres años de funcionamiento se logran contrarrestar las pérdidas económicas,

h) Tiempo de Recuperación de la Inversión (TRI)

Es el tiempo en el cual se espera se recupere la inversión hecha en el proyecto, dicho valor se calcula mediante la siguiente fórmula:

$$TRI = \frac{InversionInicial}{BeneficiosActualizados} = \frac{InversionInicial}{\frac{BeneficiosActualizadosTotales}{3anos}} = \frac{\$101679.54}{\frac{\$342,501.91}{3}} = 0.89$$

Aplicando la formula anterior se tiene que la TRI para el proyecto posee un TRI de 0.89 años, por lo que el proyecto es factible.

Resumen de escenarios

ESCENARIO	Año	% esperado de Reducción de perdidas	TMAR	B/C	TRI	FACTIBLE?
	2010	78%				
	2011	90%				
1	2012	100%	7.50%	1.48	0.99	SI
	2010	85%				
	2011	95%				
2	2012	100%	7.50%	1.64	0.89	SI

Tabla 109: Resumen de escenarios

Como se observa en la tabla 109 para CEL el escenario factible son el escenario base o promedio y los datos pesimistas y optimistas basados en experiencias anteriores de tal manera que el beneficio costo y la TRI son aceptadas con buen margen en cada uno de los tres escenarios.

13. Análisis Probabilístico

Evaluación de alternativas ¿Cuál será la más acertada?
Considerando:

anos/ Escenarios	2010 P (X)	2011 P (X)	2012 P (X)	Valor Esperado
1	83.00	93.00	100.00	92.0000
2	78.00	90.00	100.00	89.3333
3	85.00	95.00	100.00	93.3333

Tabla 110: Porcentaje de cumplimiento de objetivos esperado para el SGSI.

P(x) = **% esperado de cumplimiento de objetivos**

Varianza = [$\sum x_i \cdot x_i \cdot P(x_i)$] - (Valor esperado)^2

La varianza es una medida del riesgo; por lo tanto, cuanto mayor la varianza, mayor el riesgo. La varianza no se expresa en las mismas unidades que el valor esperado. En otras palabras, la varianza es difícil de entender y explicar porque es el término al cuadrado de su cálculo. Este problema puede resolverse trabajando con la raíz cuadrada de la varianza, llamada desviación estándar.

Desviación estándar = (Varianza) $^{1/2}$

Ambas, la varianza y la desviación estándar, proporcionan la misma información; siempre se puede obtener una de la otra. En otras palabras, el proceso de calcular una desviación estándar siempre involucra el cálculo de una varianza. Como la desviación estándar es la raíz cuadrada de la varianza, siempre se expresa en las mismas unidades que el valor esperado.

Ahora, la pregunta es ¿qué escenario es el que me proporciona mayor seguridad de implantación en cuanto a los porcentajes de reducción de pérdidas? Para tomar una decisión acertada en estos casos, se puede usar otra medida de riesgo, conocida como el Coeficiente de Variación. El Coeficiente de Variación (C.V.) es el riesgo relativo con respecto al Valor Esperado, que se define como:

El Coeficiente de Variación (C.V.) = (Desviación estándar / Valor esperado)100 %

Observe que el C.V. es independiente de la medida de unidad de valor esperado. El coeficiente de variación se usa para representar la relación entre la desviación estándar y el valor esperado; expresa el riesgo como porcentaje del valor esperado.

La siguiente tabla muestra los resultados de las evaluaciones:

Anos/ Escenarios	2010	2011	2012	Valor esperado	Varianza	Desviación estándar	Coeficiente de variación
1	83.00	93.00	100.00	92.0000	73.000	8.5440	9.286960593
2	78.00	90.00	100.00	89.3333	121.333	11.0151	12.33038182
3	85.00	95.00	100.00	93.3333	58.3333	7.6376	8.183170884

Tabla 111: Coeficiente de variación de los escenarios.

De la columna de coeficiente de variación se llega a la conclusión de que el escenario que representa menor coeficiente es el numero 3, con una variación del 8.18% es decir que representa menos riesgo y un mayor cumplimiento de objetivos. Es claro que en la práctica cualquiera de ellos pudiera presentarse, para ello se presenta a continuación un análisis más profundo haciendo uso de las probabilidades para establecer cuál de los tres es el más probable tomando en cuanta una serie de variables y criterios de decisión:

CRITERIOS DE EVALUACION:		NO EXITOSO	INDIFERENTE	EXITOSO			
		1	3	5			
ESCENARIO	EVALUADOR	CRITERIOS PARA EL EXITO O FRACASO DE LOS ESCENARIOS					
		EXPERIENCIAS ANTERIORES	NOVEDOSO DEL PROYECTO	APOYO DE LA GERENCIA	ESTRUCTURA ADMINISTRATIVA	AMBIENTE DE ESTABILIDAD	INTERES DEL PERSONAL	TOTAL
1	1	3	5	5	3	3	3	38.55%
	2	5	1	5	3	5	3	
	3	5	5	1	1	3	5	
Prom		4.33	3.67	3.67	2.33	3.67	3.67	3.56
2	1	5	3	3	5	1	3	31.33%
	2	3	3	1	3	5	1	
	3	1	1	3	3	5	3	
Prom		3.00	2.33	2.33	3.67	3.67	2.33	2.89
3	1	5	1	1	3	1	3	30.12%
	2	1	5	5	1	5	1	
	3	1	1	3	5	3	5	
Prom		2.33	2.33	3.00	3.00	3.00	3.00	2.78

Tabla 112: Probabilidad de ocurrencia de los escenarios.

De lo anterior en base a los criterios y puntuaciones se puede concluir que el escenario Numero 1 es el que cuenta con mayor probabilidad de ocurrencia.

Escenario	Análisis del coeficiente de variación	Análisis de probabilidad de ocurrencia
1	9.28%	38.55%
2	12.33%	31.33%
3	8.18%	30.12%

Tabla 113: Resumen de análisis probabilístico.

De lo anterior el escenario que resulta más factible es el numero 1 pues es el que posee mayor probabilidad de ocurrencia y el que posee un coeficiente de variación promedio, es decir se encuentra entre los límites del mismo.

F. EVALUACIÓN SOCIAL

Evaluación Social se define como la Contribución o Aporte que un Proyecto hará a la sociedad al implementarse, dando elementos suficientes para establecer una Decisión; la de Aceptar o Rechazar el proyecto.
Los Beneficios Sociales están orientados principalmente a mejorar el servicio demandado de electricidad tanto para las distribuidoras como para los consumidores finales

OBJETIVO GENERAL DE LA EVALUACION SOCIAL:

- Determinar de una manera real, en términos cuantitativos el impacto social que tendrá la implementación de un sistema de gestión para el manejo y seguridad de la información bajo la norma ISO 27001:2005

OBJETIVOS ESPECIFICOS DE LA EVALUACION SOCIAL:

- Medir el impacto social en términos de :
    - Beneficios a los consumidores finales, clientes internos y externo
    - Educación
    - Desarrollo económico
        - Empleos directos

✓ Beneficios a los consumidores finales, clientes internos y externo.

A los clientes internos:
Con la implementación de este sistema CEL traducirá en ahorro las perdidas promedio obtenidas durante los años 2007 y 2008 que hacienden a $818,250 ya que los usuarios internos del sistema gozaran de las ventajas del mismo, y así reducir la ocurrencia de eventos que generen inseguridad y mal manejo de la información ya que harán uso de información confiable, autentica, integra y controlada.

A los clientes externos:
Los Beneficiarios Directos de la implantación del SGSI serán las empresas distribuidoras de energía eléctrica del país, inscritas en AESS y Del Sur, a través de la Unidad de Transacciones UT, ya que ellas recibirán información segura, integra, confiable y real sobre los niveles de producción de energía Hidroeléctrica, esto hará que por ningún motivo se fugue o pierda información, evitando multas o algún otro tipo de inconveniente por falta de servicio.

A los consumidores finales:
Los Beneficiarios Indirectos de la implantación del Sistema de Gestión son que las Familias salvadoreñas las cuales reciben día a día energía eléctrica en sus casas, establecimientos e

industrias, con ello se asegura que la energía producida por CEL como resultado de un buen manejo de la información, cumpla la demanda de las operadoras y así también de las miles de familias salvadoreñas.

Beneficios indirectos:

- Obtener un servicio eficiente y de calidad libre de cortes por falta de oferta de electricidad, ya que la información para la generación de electricidad estará segura, será autentica, y estará en el tiempo adecuado.

- Disminución el riesgo de inundaciones en el bajo Lempa, y demás comunidades ubicadas en la línea de flujo, ocasionado por errores en la apertura de las represas.

- Una posible reducción en el pago mensual de electricidad ya que CEL, ya no estará cargando los costos ocasionados por el mal manejo y falta de seguridad en la información a la factura emitida a las distribuidoras, por tanto las distribuidoras comprar la electricidad más barata y por ende estarán en posibilidad de bajar la tarifa de cobro mensual cargado a las y los consumidores.

- Más familias podrán contar con el servicio de energía eléctrica ya que se tendrá más certeza en el cálculo de la generación de la misma y así satisfacer la demanda creciente y potencial.

✓ Educación.

Con la implementación de este sistema se pretende fortalecer los conocimientos técnicos sobre seguridad de la información a los usuarios directos e indirectos del sistema, con el objetivo de mejorar la manipulación de la información, así como también concientizar a los usuarios que la información es un activo vital de la Comisión y que por lo tanto debe manipularse y resguardarse utilizando los mejores mecanismos y sistemas de seguridad.

✓ Desarrollo económico.

Empleos directos:
Con la puesta en marcha del sistema se pretende brinda empleo directo a 9 personas que posean el perfil adecuado para el echar a andar el proyecto, 3 de los empleos directos se generar en la etapa de implementación del sistema y 6 más de manera permanente en la etapa de operación del sistema, esto aportara significativamente a la economía familiar, aumentando la posibilidad de mejorar sus condiciones de vida y así inyectar capital al mercado comercial del país.

CAPÍTULO VI: PLAN DE IMPLANTACIÓN DEL SISTEMA DE GESTIÓN Y MANEJO DE LA SEGURIDAD DE LA INFORMACION (ISO 27000:2005)

En el Plan de Implantación se definirán todas las actividades a ser ejecutadas para poner en práctica el Diseño del Sistema de Gestión y seguridad de la información basada en las normas ISO 27000. Queda a criterio de la Junta Directiva, la modificación del Plan de Implantación en cuanto a su tiempo de ejecución, en caso de enfrentar dificultades.

El Plan de Implantación requerirá que los involucrados deben poner en práctica los principios básicos de la norma para lo cual deberán recibir en primer lugar, la capacitación necesaria, debiendo considerarse todos los factores que permitirán que la misma sea realizada con éxito.

DESGLOSE ANALITICO

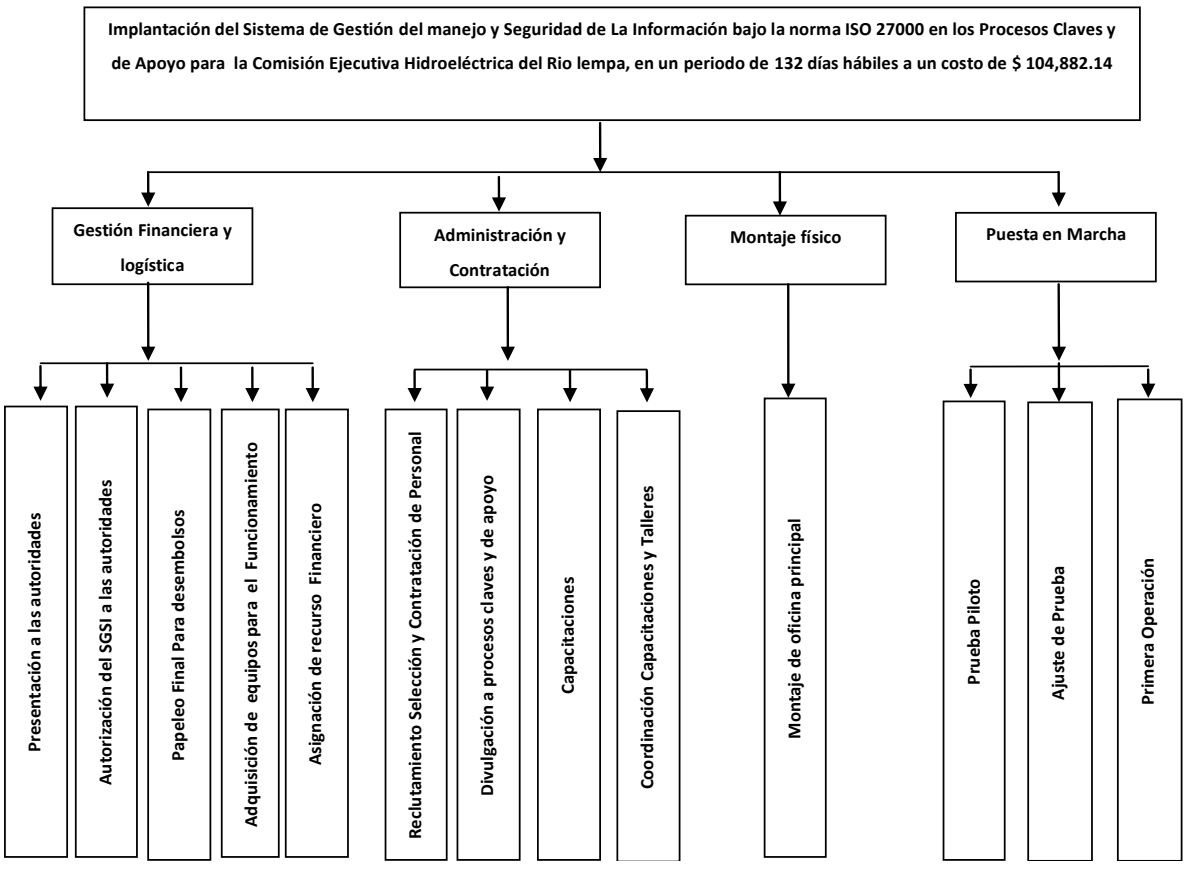


Figura 47: Desglose analítico de la implantación del proyecto.

A. ORGANIZACIÓN PARA LA IMPLANTACIÓN DEL SISTEMA.

El objetivo primordial para lo cual se propone la siguiente organización, es facilitar la programación de cada una de las actividades que componen la implantación del sistema y establecer cualquier tipo de acción correctiva antes que este comience a funcionar, en caso que los resultados obtenidos no sean los que se esperen.

La organización se refiere a la asignación del personal que estará a cargo de la implementación del proyecto que será llamada "Unidad ejecutora del Proyecto".

1. Estructura organizativa de la implantación del proyecto

Para poner en marcha la propuesta es necesario establecer una organización que permita poder generar cualquier cambio pertinente en el plan de implantación además de una mejor realización de sus actividades.

En el diseño de la organización de la unidad ejecutora, se ha tomado en cuenta que sea lo más sencilla posible, quedando el organigrama de la siguiente manera:

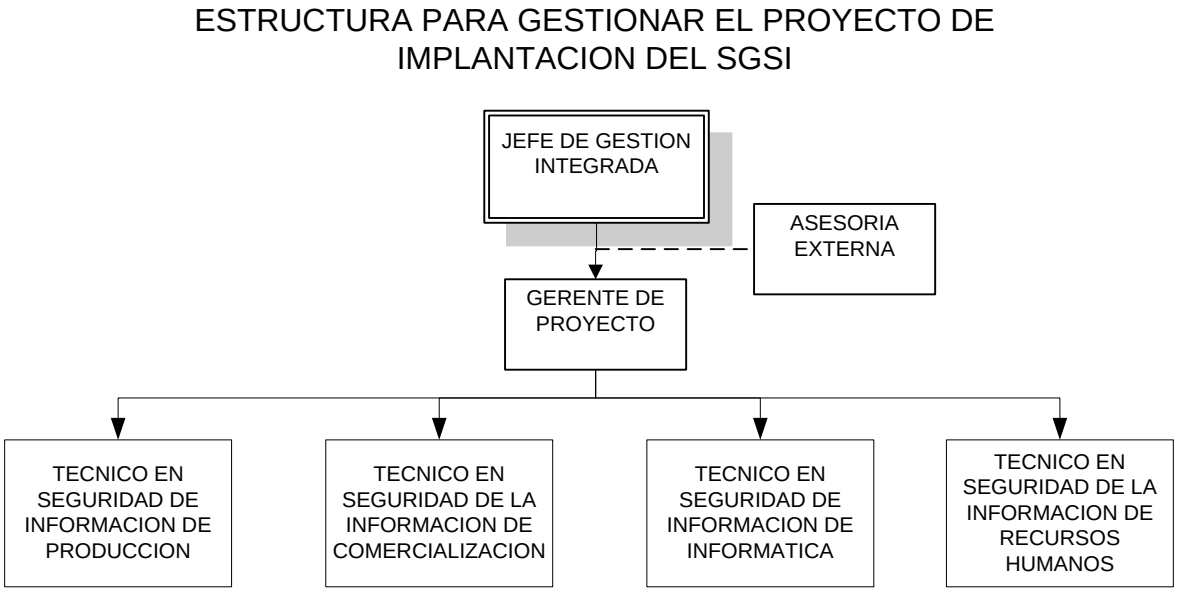


Figura 48: Estructura organizativa para la implantación del proyecto.

2. Manual de organización.

A continuación se presentan los manuales que contienen la descripción de las funciones específicas de cada unidad que conformaran la organización para la implementación del proyecto así como el perfil de cada puesto de la misma.

NOTA: De acuerdo al organigrama anterior las plazas de técnicos en seguridad de la información serán cubiertas por personal que actualmente labora en CEL por lo que no se tomaran en cuanta para la evaluación económica financiera (Costos de Mano de obra), de esta forma estaremos garantizando el involucramiento del personal de la Comisión, ya que serán ellos mismos los responsables de implementar el proyecto.

MANUAL DE ORGANIZACIÓN PARA LA PUESTA EN MARCHA DEL SGSI	
NOMBRE DE LA UNIDAD: Gestión Integrada (Director del Comité de Implantación)	**PAG 1 DE 1**
DEPENDE DE: Dirección Ejecutiva	**UNIDAD SUBORDINADA:** Coordinador del Área Técnico – Administrativa
OBJETIVO: Planificar, organizar, dirigir y controlar todas las actividades necesarias para la realización del proyecto.	
FUNCIONES ✓ Planificar, organizar, dirigir y controlar el desarrollo de cada actividad de la ejecución del proyecto. ✓ Promocionar el proyecto. ✓ Formular políticas y estrategias para la administración del proyecto. ✓ Dar seguimiento y evaluar cada objetivo propuesto para la implantación del proyecto. ✓ Establecer planes de asignación de recursos para cada unidad y controlar el cumplimiento de los mismos. ✓ Coordinar las funciones de las otras unidades que conforman el proyecto. ✓ Controlar los avances del plan de implantación de acuerdo a lo presupuestado. ✓ Tomar decisiones en situaciones críticas que se presenten durante la implementación del proyecto.	

Tabla 114: Manual de organización de la Unidad de Gestión Integrada.

MANUAL DE ORGANIZACIÓN PARA LA PUESTA EN MARCHA DEL SGSI	
NOMBRE DE LA UNIDAD: Coordinador del Área Técnico – Administrativa	**PAG 1 DE 1**
DEPENDE DE: Gestión Integrada (Director del Comité de Implantación)	**UNIDAD SUBORDINADA:** Asesoría externa
OBJETIVO: Realizar actividades para suministrar la investigación y el desarrollo técnico necesarios para la implantación del proyecto.	
FUNCIONES: ✓ Seleccionar, negociar y comprar equipos Necesarios. ✓ Seleccionar, negociar y comprar el mobiliario de oficina Necesario ✓ Determinar el presupuesto y la planificación de compras. ✓ Establecer formas de pago a proveedores y definir condiciones de servicio post-venta. ✓ Realizar el programa de distribución y control de fondos. ✓ Elaborar informes del avance del proyecto ✓ Elaborar el plan general de trabajo ✓ Informar al director del proyecto los avances sobre equipamiento y puesta en marcha del sistema. ✓ Gestionar capacitaciones, entrenamiento y talleres	

Tabla 115: Manual de organización de la Coordinación Técnica.

MANUAL DE ORGANIZACIÓN PARA LA PUESTA EN MARCHA DEL SGSI	
NOMBRE DE LA UNIDAD: Asesoría interna	**PAG 1 DE 1**
DEPENDE DE: Coordinador del Área Técnico – Administrativa	**UNIDAD SUBORDINADA**: Ninguna
OBJETIVO: Definir el personal adecuado, gestionar la obtención de recursos financieros en instituciones respectivas y establecer los aspectos legales necesarios para la implementación del proyecto.	
FUNCIONES: ✓ Informar al director del proyecto los avances en las actividades de gestión y recursos humanos. ✓ Establecer paquetes de prestaciones a ofrecer al personal de implantación. ✓ Controlar los resultados de las capacitaciones. ✓ Colaborar con el establecimiento de políticas para el proyecto en cuanto al área de personal. ✓ Realizar e impartir capacitaciones, entrenamientos y talleres ✓ Elaborar reportes técnicos	

Tabla 116: Manual de organización de la asesoría externa.

3. Manual de puestos

MANUAL DE PUESTOS PARA LA PUESTA EN MARCHA DEL SGSI	
Nombre del puesto: Jefe De Gestión Integrada	**Página:** 1 de 1
Dependencia jerárquica: Dirección Ejecutiva	**Fecha:** Septiembre de 2009
Vigencia: Septiembre de 2009	**Revisión:** Septiembre de 2009

FUNCIONES:

- ✓ Planificar las actividades necesarias para la realización del proyecto
- ✓ Organizar y asignar los recursos para la ejecución del proyecto.
- ✓ Dirigir y controlar las operaciones de ejecución para que el conjunto de acciones a realizar se junten en tiempo, costo y calidad.
- ✓ Mantener contacto con los interesados en el proyecto.
- ✓ Tomar decisiones sobre cambios relevantes en situaciones especiales durante la ejecución de los subsistemas a su responsabilidad
- ✓ Tomar acciones de contingencia ante las desviaciones que surjan.

REQUISITOS MINIMOS DEL PUESTO

EDUCACION: Ingeniero Industrial o Administrador de empresas

EXPERIENCIA: 3 años en puestos similares

PERFIL DE CONTRATACION:

EDAD: Mayor de 25 años SEXO: Masculino o Femenino

APTITUDES

- ✓ Capacidad de liderazgo.
- ✓ Conocimientos técnicos en implementación y operación de sistemas de gestión
- ✓ Capacidad de toma de decisiones.
- ✓ Conocimientos del proceso administrativo.
- ✓ Integridad en su actuación.
- ✓ Habilidad en el manejo de conflictos.
- ✓ Capacidad en dirección de personal.
- ✓ Capacidad de comunicación

Tabla 117: Manual de puestos del Jefe de Gestión Integrada.

MANUAL DE PUESTOS PARA LA PUESTA EN MARCHA DEL SGSI	
Nombre del puesto: Gerente del Proyecto	**Página:** 1 de 1
Dependencia jerárquica: Jefe De Gestión Integrada	**Fecha:** Septiembre de 2009
Vigencia: Septiembre de 2009	**Revisión:** Septiembre de 2009

FUNCIONES

- ✓ Gestionar el financiamiento del proyecto apoyando al director en los trámites legales necesarios para su aprobación.
- ✓ Programar y coordinar los desembolsos necesarios para la ejecución del proyecto.
- ✓ Elaborar las gestiones para el suministro de maquinaria, equipo y vehículos, aprobados para el SGSI
- ✓ Reportar resultados al Director del proyecto.
- ✓ Elaborar instrumentos de selección de personal.
- ✓ Seleccionar y contratación, o traslado de empleados de otra unidad, además de su respectiva inducción.

REQUISITOS MINIMOS DEL PUESTO

EDUCACION: Ingeniero Industrial o Administrador de empresas

EXPERIENCIA: 2 año en puestos similares

PERFIL DE CONTRATACION:

EDAD: más de 25 anos SEXO: Femenino o Masculino

APTITUDES

- ✓ Capacidad de liderazgo.
- ✓ Conocimientos financieros y contables.
- ✓ Integridad en su actuación.
- ✓ Habilidad en el manejo de conflictos.
- ✓ Capacidad de comunicación.
- ✓ Habilidad en realizar negociaciones

Tabla 118: Manual de puestos del Gerente del proyecto.

MANUAL DE PUESTOS PARA LA PUESTA EN MARCHA DEL SGSI	
Nombre del puesto: Asesor externo	**Página:** 1 de 1
Dependencia jerárquica: Gerente del Proyecto	**Fecha:** Septiembre de 2009
Vigencia: Septiembre de 2009	**Revisión:** Septiembre de 2009

FUNCIONES

- ✓ Desarrollar talleres sobre liderazgo
- ✓ Realizar capacitaciones sobre SGSI
- ✓ Realizar inspecciones y auditorias de SGSI
- ✓ Recibir y revisar las instalaciones físicas del nuevo departamento.
- ✓ Presentar informes al director del proyecto sobre los avances realizados en su área.
- ✓ Coordinar actividades en la Auditoría Interna inicial del Sistema.
- ✓ Informar al coordinador sobre las actividades y resultados de la auditoria inicial.

REQUISITOS MINIMOS DEL PUESTO

EDUCACION: Ingeniero Industrial.

EXPERIENCIA: 2 años en puestos similares

PERFIL DE CONTRATACION:

EDAD: Más de 25 anos **SEXO:** Masculino o Femenino

APTITUDES

- ✓ Capacidad de liderazgo.
- ✓ Habilidad en el manejo de conflictos.
- ✓ Capacidad de comunicación.
- ✓ Habilidad en realizar negociaciones.
- ✓ Experiencia práctica en las funciones de un auditor de seguridad de información.

Tabla 119: Manual de puestos del Asesor externo.

B. PLANIFICACIÓN

1. Objetivos de la planificación

a) Objetivo General

Determinar las actividades necesarias para poner en práctica las Políticas, Planes, Programas, y Procedimientos del Sistema de Gestión y Seguridad de la información, para que en los procesos que intervenga el sistema, existan condiciones de seguridad de información se identifiquen las amenazas y vulnerabilidades así como también se minimicen las posibles fuentes de riesgo.

b) Objetivos Específicos

- Determinar las actividades necesarias para que se lleve a cabo la Implantación del Sistema de Gestión y Seguridad de la Información.
- Determinar el orden cronológico de cada una de las actividades de implantación, con el propósito de alcanzar los objetivos de Seguridad de la Información.
- Establecer la estructura transitoria que será responsable de la implantación del Sistema de Gestión y seguridad de la información.
- Definir los lineamientos funcionales generales dentro de la Estructura Organizativa.
- Establecer Mecanismos de Control para el avance del proceso de Implantación del SGSI.

2. Políticas de implantación

- La Comisión ejecutiva hidroeléctrica del rio Lempa debe considerar a la Organización del Sistema de Gestión y Seguridad de la información como el medio más importante para reducirlos riesgos y minimizar los impactos ocasionados por las vulnerabilidades y amenazas relacionados con la información, por lo que su política principal será dar todo el apoyo a fin de que los objetivos de seguridad y manejo de la información sean alcanzados.

3. Estrategias de implantación

a) Concientización

Se debe convencer a la junta directiva de la Comisión Ejecutiva Hidroeléctrica del Rio Lempa sobre los beneficios de contar con un Sistema de Gestión de Seguridad de la Información, explicándoles las consecuencias que conlleva la materialización de los riesgos con los que se vive y opera

actualmente, las condiciones en que funcionará el sistema, el personal involucrado y la importancia de las responsabilidades asignadas.
Las personas deben conocer las nuevas condiciones de seguridad de la información bajo las cuales operará cada uno de los procesos planos, deben de comprender la importancia de cumplir con las normas de seguridad y manejo, el beneficio que representa para los usuarios de las unidades.
La concientización se realizará a través de capacitaciones, en las cuales inicialmente se darán a conocer elementos básicos del Sistema, como la Misión, Visión, Objetivos de Seguridad, etc.; posteriormente se introducirá a aspectos más específicos sobre las condiciones en que se encuentran los procesos claves que son la expresión de la razón de CEL, así como la forma y medios de protección para prevenir riesgos.
Algunos mecanismos a utilizar para la concientización serán:

a. Realizar charlas expositivas de los temas a los jefes de Departamento, Unidades y Secciones para que éstos transmitan a sus empleados los temas tratados.
b. Realizar charlas a nivel institucional, para explicar la problemática, sus soluciones y los beneficios que se lograrán.
c. Diseñar y repartir documentos conteniendo artículos sobre manejo y seguridad de la información, comparándolos con las condiciones bajo las cuales opera actualmente La Comisión.
d. Desarrollar capacitaciones para los empleados de las diferentes unidades, así como para las autoridades involucradas en el funcionamiento del sistema, con el objeto de que conozcan el funcionamiento del sistema, la interrelación de sus elementos, los riesgos identificados, la importancia de controlar y gestionar dichos riesgos y los medios de control y medidas de seguridad a adoptar.
e. Los Jefes o encargados de las unidades conocerán la utilización y uso de formatos para el análisis de incidentes y procedimientos relacionados con la seguridad de la información.

Se propone que para realizar las capacitaciones y charlas expositivas de concientización, se busque apoyo en entidades tales como:

- Ministerio de Hacienda.
- Instituto Salvadoreño De Formación Profesional (INSAFORP)

También se puede gestionar a través de entidades privadas o personas particulares que tengan los conocimientos en materia de Gestión y Manejo De La Seguridad de la información.

b) Formación del Comité de Implantación del Sistema de Gestión y manejo de la seguridad de la información

Se debe formar un Comité, el cual estará encargado de la Implantación del Sistema de Gestión.
La persona que funja como jefe del Comité, éste se encargará de conformar los demás puestos, de acuerdo a los perfiles requeridos para los mismos. Se considera que para el buen funcionamiento

del SGSI, la continuidad de sus miembros es fundamental, por lo que las personas elegidas deberán llenar los perfiles definidos en el SGSI.

c) Unificación del esfuerzo

Para lograr la colaboración del personal para la puesta en práctica de las medidas de control, gestión y seguridad, se instruye en el momento de realizar su trabajo y corrigiendo con paciencia y de buenas maneras en caso de cometer errores o actos que generen riesgos, esta instrucción estará a cargo del gerente del proyecto y la asesoría externa, en cada una de las unidades y coordinadas por los encargados de las mismas.
Para conseguir lo anterior, los equipos de seguridad pueden apoyarse en entidades externas como:

a. INSAFORP.

Este apoyo lo pueden lograr mediante:

- La búsqueda continua y en forma planificada de la cooperación de instituciones externas para el apoyo técnico, legal, y con experiencias anteriores en esta rama, como por ejemplo el Ministerio de Hacienda.
- La solicitud de ayuda a través de instituciones del gobierno para la preparación y capacitación tal como el INSAFORP.
- Envío de personal a capacitaciones para la especialización en técnicas y mecanismos de Manejo y seguridad de la información.

d) Equipamiento

La adquisición de equipo y material, se realizará dependiendo de la magnitud de los riesgos que se presentan en las unidades de acuerdo a los resultados del Diagnóstico y de lo dictaminado por el equipo de implementación.

e) Infraestructura

Al desarrollar cambios en la infraestructura de las unidades deben considerarse las medidas preventivas expuestas en los manuales de prevención de riesgos de las normas de OSHAS, dependiendo de los riesgos identificados en la unidad en la cual se efectuará la remodelación.

f) Priorización

Comenzar la implantación del SGSI de acuerdo a los riesgos y vulnerabilidades identificados basándose en aquellos que necesiten corrección urgente e inmediata y que representen grave impacto tanto económico como a los intereses de la institución.

C. RESULTADOS ESPERADOS DE LA IMPLANTACION

Con el SGSI se espera proporcionar información gestionada de manera eficaz y que cumpla con los requisitos de seguridad de los estándares internacionales en las diferentes Unidades de la comisión ejecutiva hidroeléctrica del rio lempa, mediante identificación y tratamiento de los riesgos encontrados con el fin de minimizar el impacto que estos podrían ocasionar.

D. ACTIVIDADES DE IMPLANTACIÓN DEL SGSI

Para poner en marcha el Plan de Implantación del SGSI, se requiere la ejecución de una serie de fases subdivididas en actividades, las cuales se describen a continuación, estableciendo para las mismas el Tiempo promedio de Ejecución y la Secuencia.

FASES		ACTIVIDAD	DESCRIPCIÓN DE ACTIVIDAD
0	Preparativos	A	Creación del presupuesto para la implantación y Operación del SGSI
		B	Evaluación y aprobación del Plan de Implantación
		C	Creación del Comité de Implantación del SGSI
		D	Contratación del personal de Capacitación en GSI
I	Entendimiento de los requerimientos del modelo	E	Capacitación y Taller con niveles estratégicos y tácticos en Gestión y Manejo de la seguridad de la información
II	Determination del Alcance	F	Capacitación Estratégica y Capacitación Táctica
III	Análisis y evaluación del riesgo	G	Capacitación: análisis y evaluación del riesgo.
		H	Capacitación: Políticas de seguridad de la información y objetivos
		I	Capacitación y Taller: Evaluación de las opciones para el tratamiento de riesgo
		J	Capacitación y Taller: Selección de controles y objetivos de control
		K	Capacitacion: Declaracion de Aplicabilidad
iV	Plan de continuidad del negocio	L	Capacitación y taller: Análisis de riesgo y escenarios de amenazas
		M	Capacitación y Taller: Estrategias de continuidad.
		N	Capacitación y taller: Plan de reanudación de operaciones
V	Inplementar y Operar	O	Capacitación :Plan de tratamiento de riesgos
		P	Capacitación y taller : efectividad de controles y métricas
VI	Monitorial y Revisar	Q	Capacitación y Taller: Incidentes y eventos de seguridad
		R	Capacitación y taller: revisiones periódicas del SGSI
VII	Mantener y Mejorar	S	Capacitación: Como Implementar Las Acciones Correctivas y Preventivas
VIII	Desarrollo de	T	Entrenamiento en Documentación del SGSI

	Competencias Organizacionales	U	Entrenamiento en manejo de la acción Correctiva y Preventiva
		V	Entrenamiento en manejo de la auditoría interna.
		W	Entrenamiento en el manejo del sistema de información
IX	Manual de Seguridad de la información	X	Capacitación: Manual de seguridad de la información.
X	Montage Fisico	Y	Montaje del Espacio físico de la Oficina de Manejo y seguridad de la información
XI	Puesta en marcha	Z	Prueba Piloto del Sistema de manejo y seguridad de la información
		AA	Evaluación de la Implantación y Retroalimentación
		AB	Puesta en Operación del Sistema de manejo y seguridad de la información
XII	Auditorias Internas	AC	Ejecucion de auditorias Internas
XIV	Obtencion de Certificacion Internacional	AD	Búsqueda de la Empresa certificadora.
		AE	Realización de la auditoria por parte de la certificadora
		AF	Obtencion de la certificacion.

Tabla 120: Actividades de la implantación del proyecto.

E. DESCRIPCIÓN DE ACTIVIDADES DE IMPLANTACIÓN DEL SGSI

A continuación se describe cada una de las actividades que se llevarán a cabo para desarrollar el Plan de Implantación del Sistema de gestión y manejo de información, basado en las Normas ISO 27001:2005. Estas Actividades se presentan de forma general y se consideran como Macro actividades, quedando a criterio del Comité de Implantación el desglose detallado de cada una de ellas.

FASE 0: PREPARATIVOS

- **Actividad A: Creación del Presupuesto para la Implantación y Operación del Sistema de Gestión y Manejo de la información.**

El Departamento de Gestión Integrada determinará el Presupuesto de Gastos necesario para la realización de todas las Actividades de Implantación. Esto se realizará en base al siguiente procedimiento:

No.	Actividad	Responsable
1	Elaboración de presupuesto con base a la evaluación económica del proyecto	Asesoría Externa
2	Evalúa el presupuesto de Implementación y realiza observaciones pertinentes	Gerencia del Proyecto.
3	Envía el presupuesto para su aprobación final a la Junta directiva	Gerencia del Proyecto.
4	Revisa y aprueba presupuesto de implantación	Junta Directiva

Tabla 121: Actividades de la creación del presupuesto para la implantación y operación del proyecto.

Diagrama: Flujo grama del Procedimiento

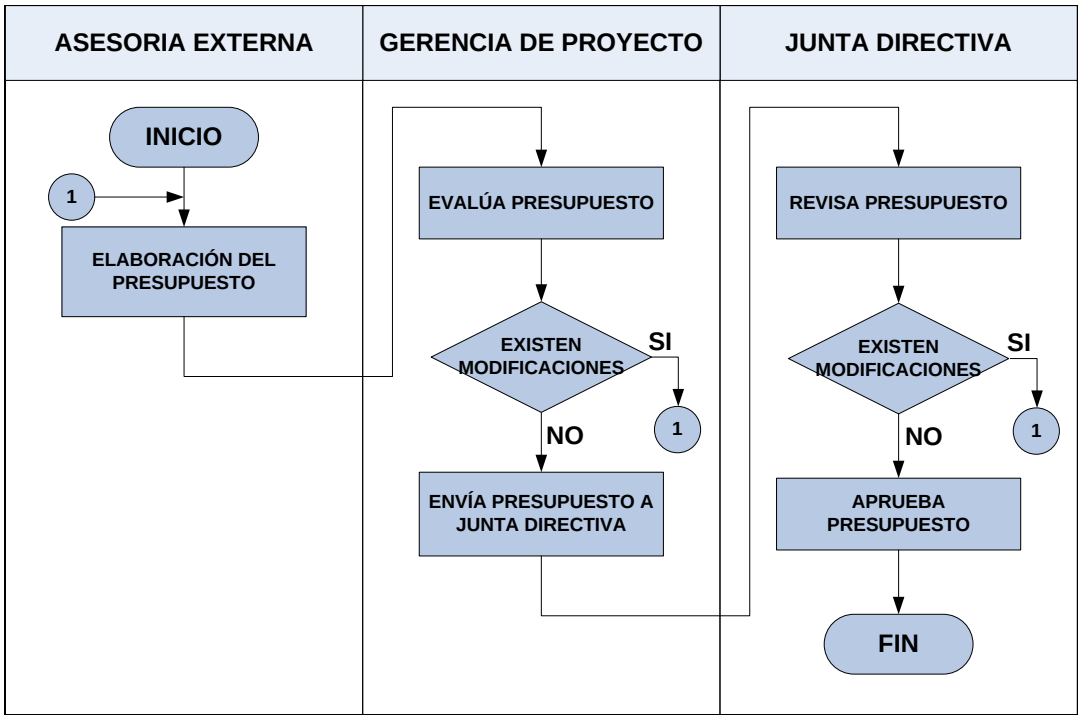


Figura 49: Diagrama de flujo para la creación del presupuesto de la implantación y operación del SGSI.

- **Actividad B: Evaluación y Aprobación del Plan de Implantación.**

La Junta Directiva discutirá y aprobará el programa de Implantación del Sistema de Gestión en Seguridad de la información, en esta actividad participarán los directivos, en dicha discusión se tomarán en consideración los resultados obtenidos del diagnostico en cuanto al manejo y gestión de la información como la situación actual de CEL en relación a la Norma ISO 27000. El plan de implantación deberá de ser revisado para su aprobación final por la Junta directiva de la comisión.

No.	Actividad	Responsable
1	Convoca a reunión a Junta directiva	Presidente de la Comisión
2	Revisan el Plan de Implantación del sistema y Sugieren ajustes de ser necesario	Directivos
3	Elabora un acta donde firmaran los miembros.	Secretaria
4	Realiza ajustes y re envía plan de Implantación revisado a la Gerencia General de CEL	Jefe de gestión Integrada
5	Revisa y aprueba plan de implantación o realiza las observaciones correspondientes	Junta Directiva

Tabla 122: Actividades de la evaluación y aprobación del plan de implantación del proyecto.

Diagrama: Flujo grama del procedimiento

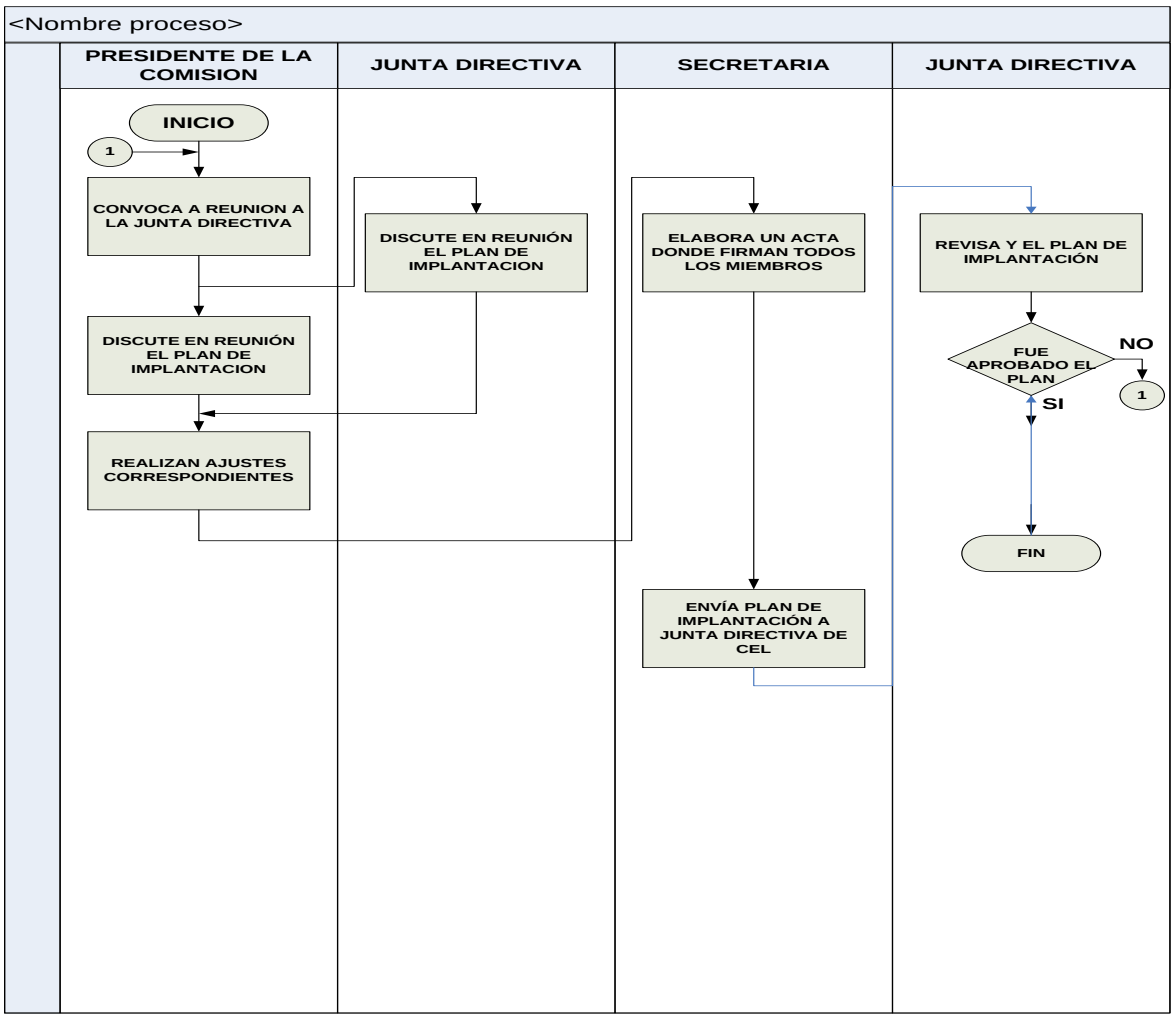


Figura 50: Diagrama de flujo de la evaluación y aprobación del plan de implantación.

- **Actividad C: Creación del Comité de Implantación del Sistema de Seguridad de la Información SGSI.**

El Área de gestión integrada AGI en conjunto con Recursos humanos realiza la selección y el reclutamiento del personal que conformará el Comité de Implantación, para ello se seguirá el procedimiento de selección de personal.

A continuación se presenta la propuesta de la Estructura que deberá tener el Comité de Implantación del SGSI.

FUNCIONES DEL COMITÉ DE IMPLANTACIÓN

- **Jefe De Gestión Integrada (Director del Comité de Implantación)**

  Tendrá la máxima responsabilidad y autoridad para poner en práctica todas las Actividades del Programa de Implantación y tendrá como misión principal obtener el Funcionamiento Óptimo

del Sistema, para lo cual deberá Planear, Organizar y Controlar el desarrollo de las Actividades de la Implantación, proporcionándole a los Grupos Administrativos y Técnicos, toda la ayuda que necesiten para el cumplimiento de sus Funciones, para lo cual se mantendrá en completa comunicación con las Autoridades de la junta directiva de la comisión.

- **Gerente del Proyecto (Coordinador del Área Técnico – Administrativa)**

Le corresponderá la ejecución de todas aquellas Actividades Administrativas, como la Selección de Personal, Trámites para la Adquisición de Materiales y Equipo y Contacto con Jefes o Encargados de los procesos claves para Coordinar la Integración de personal en estas Tareas.

Le corresponde la Dirección de todas las Actividades Técnicas como la Planeación, Dirección y Control de todos los Trabajos y Obras necesarias para que los Medios de Protección, Modificación de Instalaciones, Capacitación en aspectos Técnicos, etc.; se lleven a cabo de conformidad a los Requerimientos definidos en este estudio.

- **Asesoría Externa**

Les corresponde apoyar al Gerente del Proyecto, en el desarrollo de las Actividades asignadas por el Director del Comité de Implantación, dando también soporte teórico practico en el método de implantación.

- **Actividad D: Contratación de Personal de Capacitación en Gestión de Seguridad de la información.**

Consiste en la selección análisis del perfil, competencias. (Contratación: se hará según establezca necesario el jefe de gestión integrada obedeciendo a la necesidad de especialistas en el tema iso27000)

FASE I: ENTENDIMIENTO DE LOS REQUERIMIENTOS DEL MODELO

- **Actividad E: Capacitación y Taller con niveles estratégicos y tácticos en Gestión y Manejo de la seguridad de la información.**

Capacitación dirigida a los niveles tanto estratégicos como tácticos, se esclarecerán los requerimientos de la norma y la lógica del funcionamiento del SGSI y los beneficios para la institución, esto se logra mediante un taller en el cual los niveles estratégicos y tácticos deciden democráticamente la mejor metodología de implantación.

FASE II: DETERMINACION DEL ALCANCE

- **Actividad F: Capacitación Estratégica. Capacitación Táctica.**

-Capacitación estratégica sobre el alcance del sistema.

Se identifican los factores críticos de éxito de la comisión y, por otro lado, se identifican los procesos críticos de la organización; determinación del grado de criticidad en relación con su exposición al riesgo de la información.

-Capacitación táctica para determinar el alcance del modelo.

Se identifican con gran detalle los componentes de cada proceso y las interfaces con otros procesos de la comisión, y con entidades externas de la institución, para posteriormente efectuar el análisis y la evaluación de riesgo.

FASEIII: ANALISIS Y VALUACION DEL RIESGO

- **Capacitación**

  Esta actividad estará a cargo de las personas designadas para tal efecto. Se capacitará en los siguientes temas:

  - **Actividad G:** Capacitación en análisis y evaluación del riesgo.
  - **Actividad H:** Capacitación en Políticas de seguridad de la información y objetivos
  - **Actividad I:** Capacitación y Taller en Evaluación de las opciones para el tratamiento de riesgo
  - **Actividad J:** Capacitación y Taller en selección de controles y objetivos de control.
  - **Actividad K:** Capacitación en declaración de Aplicabilidad.

FASE IV: PLAN DE CONTINUIDAD DEL NEGOCIO

- **Actividad L:** Capacitación y taller en análisis de riesgo y escenarios de amenazas.
- **Actividad M:** Capacitación y Taller en estrategias de continuidad.
- **Actividad N: .**Capacitación y taller en plan de reanudación de operaciones.
- **Actividad Ñ:** Capacitación y taller en plan de reanudación de operaciones.

FASEV: IMPLEMENTAR Y OPERAR

- **Actividad O:** Capacitación en plan de tratamiento de riesgos.
- **Actividad P:** Capacitación y taller en efectividad de controles y métricas.

FASE VI: MONITORIARA Y REVISAR

- **Actividad Q:** Capacitación y Taller en incidentes y eventos de seguridad.
- **Actividad R:** Capacitación y taller en revisiones periódicas del SGSI.

FASE VII: MANTENER Y MEJORAR

- **Actividad S:** Capacitación en como Implementar Las Acciones Correctivas y Preventivas.

FASE VIII: DESARROLLO DE COMPETENCIAS ORGANIZACIONALES

- **Actividad T:** Entrenamiento en Documentación del SGSI.
  Actividad encaminada para que el personal afectado por la implantación del modelo tenga las destrezas para poder documentar procedimientos, políticas, instrucciones de trabajo y saber identificar registros del sistema de seguridad de la información.
- **Actividad U:** Entrenamiento en el manejo de la acción correctiva y preventiva.
  Consiste en entrenar al personal en la recolección de datos de todas las ocurrencias de incidentes de seguridad significativos del SGSI, el objetivo es que con base en evidencias objetivas de ocurrencia, se vean las tendencias y la comisión desarrolle acciones preventivas para evitar que la no conformidad se presente; especializando

al personal en el conocimiento de la metodología y las herramientas para el correcto manejo de la acción correctiva y preventiva.

- **Actividad V:** Entrenamiento en manejo de la auditoría interna.
  Exigida en la clausula 6 de la norma, consiste en un adiestramiento de la comisión a sí misma para demostrar que su sistema se mantiene y que busca nuevas oportunidades de mejora.
  Capacitación, conocimiento y capacidad son las competencias que se resaltaran para identificar los auditores internos

- **Actividad W:** Entrenamiento en el manejo del sistema de información.
  Es importante que el personal que gerencia el SGSI permanezca informado en tiempo real de lo que ocurre en el sistema; por tal motivo se debe entrenar a los involucrados en el sistema de información que es el software plataforma del SGSI

FASE IX: MANUAL DE SEGURIDAD DE LA INFORMACION.

- **Actividad X:** Capacitación sobre manual de seguridad de la información.

FASE X: MONTAJE FISISCO

- **Actividad Y:** Montaje del Espacio físico de la Oficina de Manejo y seguridad de la información.

FASE XI: PUESTA EN MARCHA

- **Actividad Z:** Prueba Piloto del Sistema de manejo y seguridad de la información.
- **Actividad AA:** Evaluación de la Implantación y Retroalimentación.
- **Actividad AB:** Puesta en Operación del Sistema de manejo y seguridad de la información.

FASE XII: AUDITORIAS INTERNAS

- **Actividad AC:** Ejecución de auditorías Internas
  Se deberá capacitar al personal para llevarlas a cabo bien sea una u otra opción, las auditorias deben realizarse cumpliendo con todas las exigencias de la clausula 6 de la norma y utilizando el lineamiento ISO19011:2002 para llevar a cabo la auditoría interna

FASE XIII: OBTENCION DE CERTIFICACION INTERNACIONAL.

La certificación es un aval muy importante para mostrar a terceros que se tiene un sistema de gestión de seguridad de la información implantada de conformidad con el estándar ISO 27001:2005, y que una empresa acreditada para dicho efecto da fe de esto.

- **Actividad AD:** Búsqueda de la Empresa certificadora.
  Las empresas certificadoras tienen que estar acreditadas. Una fuente de información muy confiable sobre empresas certificadoras acreditadas, para saber sobre estas y

conocer sobre tendencias de certificación del ISO 27001:2005, es el portal www.xisec.com

Otro aspecto que debe contemplarse, al buscar empresas certificadoras, es su experiencia en la industria o actividad en la que la comisión está ubicada. Se debe buscar empresas certificadoras que tengan experiencia y a la vez que puede dan aportar experiencia. Por lo último para minimizar los errores en la escogitacion, se deberá contactar a los clientes de la empresa certificadora y pedir referencias sobre el desempeño de la certificadora

- **Actividad AE:** Realización de la auditoria por parte de la certificadora.
  La auditoria de certificación ISO 27001:2005, consta de dos fases.
  a. Revisión de toda la documentación realizada.
     Aquí es muy importante tener toda la documentación 4.3.1 de la norma en el manual. Prácticamente toda la auditoria de la primera fase gira sobre una revisión a los documentos de la clausula 4.3.1.
  b. Auditoria de cumplimiento
     Los auditores de la empresa certificadora acudirán a la empresa y verificaran que todo lo documentado este implantado, de no encontrar mayores no conformidades se le otorgaría la certificación a la comisión.
- **Actividad AF:** Obtención de la certificación.
  Es una serie de procesos netamente administrativos y papeleos para obtener el documento final.

F. TIEMPOS DE ACTIVIDADES

El Tiempo promedio de duración de cada Actividad está dado en **Días Hábiles** y la Implantación finalizará hasta que se obtenga el funcionamiento completo del Sistema. Una vez identificadas las Actividades del Plan de Implantación se procederá a calcular el Tiempo Esperado para cada una de dichas Actividades, operación que se realizará mediante el uso de la Fórmula que se presenta a continuación:

$$te = \frac{t_o + 4t_n + t_p}{6}$$

Donde:

t_e = Tiempo Esperado

t_o = Tiempo Óptimo

t_n = Tiempo Normal

t_p = Tiempo Promedio

ACTIVIDAD	DEPENDENCIA	DESCRIPCIÓN DE ACTIVIDAD	to	tn	tp	Te
A	….	Creación del presupuesto para la implantación y Operación del SGSI	10	12	20	13
B	A	Evaluación y aprobación del Plan de Implantación	10	15	20	15

C	B	Creación del Comité de Implantación del SGSI	8	10	15	11
D	C	Contratación del personal de Capacitación en GSI	6	8	10	8
E	D	Capacitación y Taller con niveles estratégicos y tácticos en Gestión y Manejo de la seguridad de la información	3	4	5	4
F	E	Capacitación Estratégica y Capacitación Táctica	5	6	7	6
G	D	Capacitación: análisis y evaluación del riesgo.	4	5	6	5
H	G	Capacitación: Políticas de seguridad de la información y objetivos	4	5	6	5
I	H	Capacitación y Taller: Evaluación de las opciones para el tratamiento de riesgo	5	7	8	7
J	I	Capacitación y Taller: Selección de controles y objetivos de control	5	7	8	7
K	J	Capacitacion: Declaracion de Aplicabilidad	4	5	6	5
L	D	Capacitación y taller: Análisis de riesgo y escenarios de amenazas	5	7	8	7
M	L	Capacitación y Taller: Estrategias de continuidad.	4	5	6	5
N	M	Capacitación y taller: Plan de reanudación de operaciones	4	5	6	5
O	D	Capacitación :Plan de tratamiento de riesgos	5	6	7	6
P	O	Capacitación y taller : efectividad de controles y métricas	4	5	6	5
Q	P	Capacitación y Taller: Incidentes y eventos de seguridad	4	5	6	5
R	Q	Capacitación y taller: revisiones periódicas del SGSI	4	5	6	5
S	R	Capacitación: Como Implementar Las Acciones Correctivas y Preventivas	7	10	12	10
T	F, K, N, S	Entrenamiento en Documentación del SGSI	3	4	5	4
U	T	Entrenamiento en manejo de la acción Correctiva y Preventiva	3	4	5	4
V	U	Entrenamiento en manejo de la auditoría interna.	3	4	5	4
W	V	Entrenamiento en el manejo del sistema de información	3	4	5	4
X	W	Capacitación: Manual de seguridad de la información.	4	5	7	5
Y	X	Montaje del Espacio físico de la Oficina de Manejo y seguridad de la información	7	10	12	10
Z	Y	Prueba Piloto del Sistema de manejo y seguridad de la información	10	15	20	15
AA	Z	Evaluación de la Implantación y Retroalimentación	5	8	10	8
AB	AA	Puesta en Operación del Sistema de manejo y seguridad de la información	5	7	10	7
AC	AB	Ejecucion de auditorias Internas	20	25	30	25
AD	AC	Búsqueda de la Empresa certificadora.	5	7	10	7
AE	AD	Realización de la auditoria por parte de la certificadora	10	15	20	15
AF	AE	Obtencion de la certificacion.	30	35	40	35

Tabla 123: Tiempo de las actividades de la implantación del proyecto.

G. MATRIZ DE RESPONSABILIDADES DEL PERSONAL CLAVE EN LA IMPLEMENTACIÓN.

Todas las actividades de Implantación del SGSI estarán bajo la responsabilidad del Comité de Implantación propuesto, estando a su vez sujetos a los lineamientos La Comisión.

ACCION	Autorizar:	Verificar:	Responsable:	Recibe Informe:
SIGNIFICADO	A	V	R	I

DESCRIPCIÓN DE ACTIVIDAD	ALTA GERENCIA	JEFATURA DE GESTION INTEGRADA	GERENTE DEL PROYECTO	ASESORIA EXTERNA
Creación del presupuesto para la implantación y Operación del SGSI	I	A, V	R	
Evaluación y aprobación del Plan de Implantación	I	A, V		
Creación del Comité de Implantación del SGSI	I	A, V	R	
Contratación del personal de Capacitación en GSI	I	A, V	R	
Capacitaciones, talleres y entrenamientos			I, A, V	R
Montaje del Espacio físico de la Oficina de Manejo y seguridad de la información	I	A, V	R	
Prueba Piloto del Sistema de manejo y seguridad de la información			R	
Evaluación de la Implantación y Retroalimentación.	I	A	R,V	
Puesta en Operación del Sistema de manejo y seguridad de la información	I	A	R	
Ejecución de auditorías Internas			R	
Búsqueda de la Empresa certificadora.		A, V, R		
Realización de la auditoria por parte de la certificadora.		A, V		
Obtención de la certificación.	I	V, R		

Tabla 124: Matriz del personal clave para la implantación del proyecto.

H. CÁLCULO DE TIEMPOS POR ACTIVIDAD, HOLGURA, DESVIACIÓN Y DURACIÓN TOTAL DEL PROYECTO

A partir de los datos presentados anteriormente se calcula el Tiempo de Duración de las Actividades, con sus respectivas holguras, obteniendo la Duración Total del Proyecto y el Lapso de Holgura para el mismo:

ACTIVIDAD	DURACION	INICIO MÁS TEMPRANO	FINALIZACIÓN MÁS TEMPRANA	INICIO MÁS TARDÍO	FINALIZACIÓN MÁS TARDÍA	HOLGURA
A	13	0	13	0	13	0
B	15	13	28	13	28	0
C	11	28	39	28	39	0
D	8	39	47	39	47	0
E	4	47	51	68	72	21
F	6	51	57	72	78	21
G	5	47	52	49	54	2
H	5	52	57	54	59	2
I	7	57	64	59	66	2
J	7	64	71	66	73	2
K	5	71	76	73	78	2
L	7	47	54	61	68	14
M	5	54	59	68	73	14
N	5	59	64	73	78	14
O	6	47	53	47	53	0
P	5	53	58	53	58	0
Q	5	58	63	58	63	0
R	10	63	68	63	68	0
S	5	68	78	68	78	0
T	4	78	82	78	82	0
U	4	82	86	82	86	0
V	4	86	90	86	90	0
W	4	90	94	90	94	0
X	5	94	99	94	99	0
Y	10	99	109	99	109	0
Z	15	109	124	109	124	0
AA	8	124	132	124	132	0
AB	7	132	139	132	139	0
AC	25	139	164	139	164	0
AD	7	164	171	164	171	0

AE	15	171	186	171	186	0
AF	35	186	221	186	221	0

Tabla 125: calculo de tiempos por actividades para la implantación del proyecto.

A continuación se presenta el Diagrama ABC en base en estos datos obtenidos.

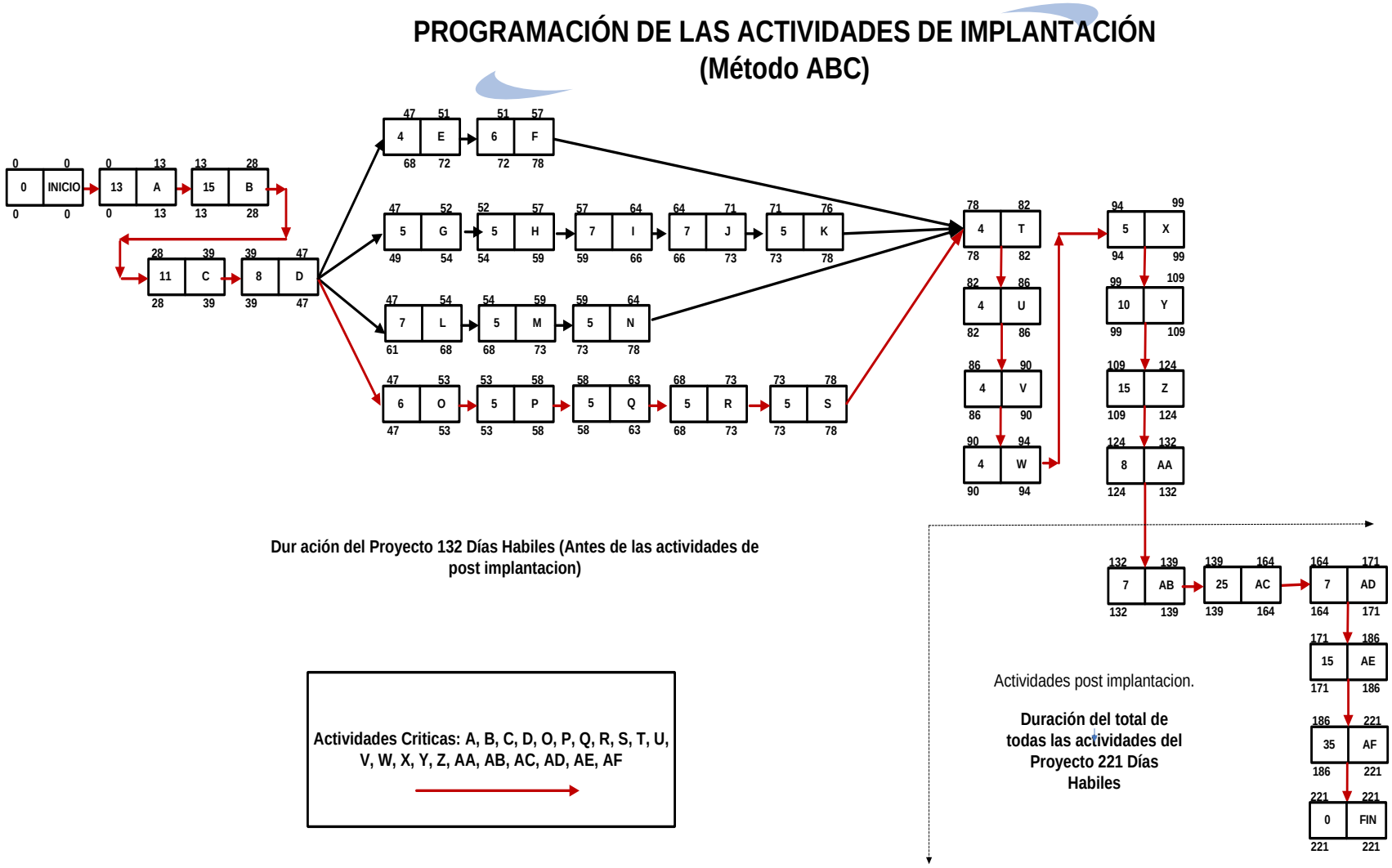


Figura 51: Programación de las actividades de implantación.

I. PROGRAMA DE ACTIVIDADES PARA LA IMPLANTACIÓN DEL SGSI

Teniendo como referencia la duración de las Actividades y las Holguras, se establece la siguiente Programación para la Implantación del Sistema de Gestión

ACTIVIDAD	DESCRIPCIÓN DE ACTIVIDAD	DURACION (DIAS)	FECHA INICIO	FECHA FINALIZACION
A	Creación del presupuesto para la implantación y Operación del SGSI	13	01/10/2009	16/10/2009
B	Evaluación y aprobación del Plan de Implantación	15	19/10/2009	06/11/2009
C	Creación del Comité de Implantación del SGSI	11	09/11/2009	23/11/2009
D	Contratación del personal de Capacitación en GSI	8	24/11/2009	3/12/2009
E	Capacitación y Taller con niveles estratégicos y tácticos en Gestión y Manejo de la seguridad de la información	4	4/12/2009	9/12/2009
F	Capacitación Estratégica y Capacitación Táctica	6	10/12/2009	17/12/2009
G	Capacitación: análisis y evaluación del riesgo.	5	4/12/2009	10/1/2010
H	Capacitación: Políticas de seguridad de la información y objetivos	5	10/12/2009	16/12/2009
I	Capacitación y Taller: Evaluación de las opciones para el tratamiento de riesgo	7	17/12/2009	23/12/2009
J	Capacitación y Taller: Selección de controles y objetivos de control	7	04/01/2010	12/01/2010
K	Capacitacion: Declaration de Aplicabilidad	5	13/01/2010	19/2/2010
L	Capacitación y taller: Análisis de riesgo y escenarios de amenazas	7	04/12/2009	14/12/2009
M	Capacitación y Taller: Estrategias de continuidad.	5	15/12/2009	22/12/2009
N	Capacitación y taller: Plan de reanudación de operaciones	5	23/12/2010	07/01/2010
O	Capacitación :Plan de tratamiento de riesgos	6	04/12/2009	11/12/2009
P	Capacitación y taller : efectividad de controles y métricas	5	14/12/2009	21/12/2009
Q	Capacitación y Taller: Incidentes y eventos de seguridad	5	22/12/2009	06/01/2010
R	Capacitación y taller: revisiones periódicas del SGSI	5	07/01/2010	14/01/2009
S	Capacitación: Como Implementar Las Acciones Correctivas y Preventivas	10	15/01/2010	29/01/2010
T	Entrenamiento en Documentación del SGSI	4	01/02/2010	04/02/2010
U	Entrenamiento en manejo de la acción Correctiva y Preventiva	4	05/02/2010	10/02/2010
V	Entrenamiento en manejo de la auditoría interna.	4	11/02/2010	16/02/2010
W	Entrenamiento en el manejo del sistema de información	4	17/02/2010	23/02/2010
X	Capacitación: Manual de seguridad de la	5	24/02/2010	02/03/2010

	información.			
Y	Montaje del Espacio físico de la Oficina de Manejo y seguridad de la información	10	03/03/2010	17/03/2010
Z	Prueba Piloto del Sistema de manejo y seguridad de la información	15	18/03/2010	08/04/2010
AA	Evaluación de la Implantación y Retroalimentación	8	09/04/2010	21/04/2010
AB	Puesta en Operación del Sistema de manejo y seguridad de la información	7	22/04/2010	30/04/2010
AC	Ejecucion de auditorias Internas	25	04/05/2010	08/06/2010
AD	Búsqueda de la Empresa certificadora.	7	09/06/2010	21/06/2010
AE	Realización de la auditoria por parte de la certificadora	15	22/06/2010	13/07/2010
AF	Obtencion de la certificacion.	35	14/07/2010	25/08/2010

Tabla 126: Programación de actividades para la implantación del proyecto.

J. DIAGRAMA DE GANNT

A continuación se presenta el diagrama de GANNT, en el cual se puede observar de manera esquemática la ejecución de actividades.

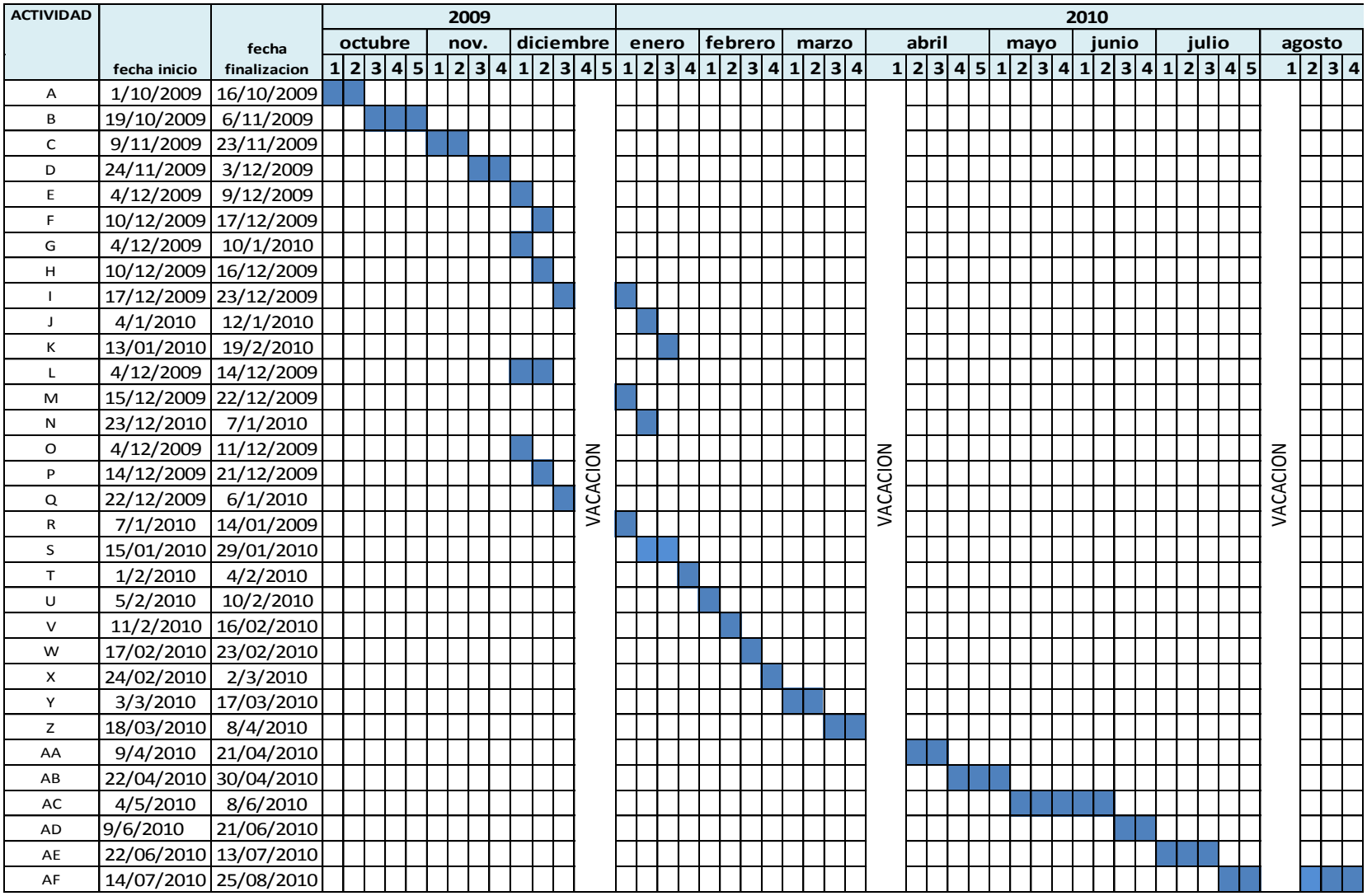


Grafico 11: Diagrama de Gannt para la implantación del proyecto

K. COSTOS DE IMPLANTACIÓN

Los Costos de Implantación se refieren a los Costos de Inversión por la realización del Proyecto, exceptuando los Costos por el Diseño del Sistema:

COSTO (DESEMBOLSO) DE INVERSIÓN	
RUBRO	COSTO
Costos de Capacitación a las Autoridades de CEL	$ 577.4
Costos de Capacitación al personal de las aéreas involucradas	$6,672.0
Costo de Equipo, materiales, servicios e instalaciones	$30,205
Costo de Documentación	$560.24
Costos del Sistema de Información Gerencial	$ 480.0
Costos de la estructura organizativa de la Administración del proyecto	$ 38,557.5
Costos de la Certificación	$ 27,830
TOTAL	**$ 104,882.14**

Tabla 127: Resumen de costos para la implantación del proyecto.

Por lo tanto, CEL tendría que efectuar un **desembolso** de **$ 104,882.14**, para implantar el Sistema de Gestión en términos de inversión inicial

FLUJO DE EFECTIVO

Los fondos para la implantación provendrán de la cuenta presupuestaria 2009-2010 de la Unidad de Gestión Integrada previamente solicitada y aprobada por la Unidad Financiera, los costos de implantación se desembolsaran de la siguiente manera siguiendo todos los procedimientos que la Unidad de Adquisiciones y Contrataciones Institucionales (UACI) de CEL:

Política de Desembolsos:

Los desembolsos se realizaran bimensualmente al final de cada periodo de acuerdo a las actividades asociadas.

La UACI será la encargada de liquidar todas las órdenes de requerimientos tanto de Recursos Humanos, Materiales y Servicios.

A continuación se detalla los desembolsos y la distribución de los costos a lo largo del proyecto

ACTIVIDAD	DESCRIPCIÓN DE ACTIVIDAD	FECHA INICIO	FECHA FIN	COSTOS	DESEMBOLSOS
A	Creación del presupuesto para la implantación y Operación del SGSI	1/10/2009	16/10/2009	N/A	$8,288.90
B	Evaluación y aprobación del Plan de Implantación	19/10/2009	6/11/2009	$3,855.75	
C	Creación del Comité de Implantación del SGSI	9/11/2009	23/11/2009	N/A	
D	Contratación del personal de Capacitación en GSI	24/11/2009	3/12/2009	$3,855.75	

E	Capacitación y Taller con niveles estratégicos y tácticos en Gestión y Manejo de la seguridad de la informacion	4/12/2009	9/12/2009	$577.40	
F	Capacitación Estratégica y Capacitación Táctica	10/12/2009	17/12/2009	N/A	$13,906.91
G	Capacitación: análisis y evaluación del riesgo.	4/12/2009	10/1/2010	$476.57	
H	Capacitación: Políticas de seguridad de la información y objetivos	10/12/2009	16/12/2009	$476.57	
I	Capacitación y Taller: Evaluación de las opciones para el tratamiento de riesgo	17/12/2009	23/12/2009	$4,332.32	
J	Capacitación y Taller: Selección de controles y objetivos de control	4/1/2010	12/1/2010	$476.57	
K	Capacitacion: Declaracion de Aplicabilidad	13/01/2010	19/2/2010	$476.57	
L	Capacitación y taller: Análisis de riesgo y escenarios de amenazas	4/12/2009	14/12/2009	$476.57	
M	Capacitación y Taller: Estrategias de continuidad.	15/12/2009	22/12/2009	$476.57	
N	Capacitación y taller: Plan de reanudación de operaciones	23/12/2010	7/1/2010	$476.57	
O	Capacitación :Plan de tratamiento de riesgos	4/12/2009	11/12/2009	$476.57	
P	Capacitación y taller : efectividad de controles y métricas	14/12/2009	21/12/2009	$476.57	
Q	Capacitación y Taller: Incidentes y eventos de seguridad	22/12/2009	6/1/2010	$476.57	
R	Capacitación y taller: revisiones periódicas del SGSI	7/1/2010	14/01/2009	$476.57	
S	Capacitación: Como Implementar Las Acciones Correctivas y Preventivas	15/01/2010	29/01/2010	$4,332.32	
T	Entrenamiento en Documentación del SGSI	1/2/2010	4/2/2010	N/A	
U	Entrenamiento en manejo de la acción Correctiva y Preventiva	5/2/2010	10/2/2010	N/A	$35,017.32
V	Entrenamiento en manejo de la auditoria interna.	11/2/2010	16/02/2010	N/A	
W	Entrenamiento en el manejo del sistema de información	17/02/2010	23/02/2010	N/A	
X	Capacitación: Manual de seguridad de la información.	24/02/2010	2/3/2010	$4,332.32	
Y	Montaje del Espacio físico de la Oficina de Manejo y seguridad de la información	3/3/2010	17/03/2010	$30,205.00	

Z	Prueba Piloto del Sistema de manejo y seguridad de la información	18/03/2010	8/4/2010	$480.00	
AA	Evaluación de la Implantación y Retroalimentación	9/4/2010	21/04/2010	N/A	$8,271.76
AB	Puesta en Operación del Sistema de manejo y seguridad de la información	22/04/2010	30/04/2010	$4,416.01	
AC	Ejecucion de auditorias Internas	4/5/2010	8/6/2010	$3,855.75	
AD	Búsqueda de la Empresa certificadora.	9/6/2010	21/06/2010	N/A	
AE	Realización de la auditoria por parte de la certificadora	22/06/2010	13/07/2010	$3,855.75	$39,397.25
AF	Obtencion de la certificacion.	14/07/2010	25/08/2010	$35,541.50	
TOTAL					$104,882.14

Tabla 128: Flujo de efectivo por actividades para la implantación del proyecto.

TIEMPO DURACION DEL PROYECTO	DESEMBOLSOS
Noviembre	$8,288.90
Febrero	$13,906.91
Abril	$35,017.32
Junio	$8,271.76
Agosto	$39,397.25
TOTAL	$104,882.14

Tabla 129: Resumen de desembolsos de efectivo para la implantación del proyecto.

L. CONTROL DE LA IMPLANTACIÓN

El Control de la Implantación se llevará a cabo comparando el Avance Real de la Implantación con la Programación Planeada, haciéndose los Ajustes necesarios para corregir las Deficiencias que se presenten sobre la marcha.

El Comité de Implantación deberá contar con los instrumentos necesarios que permitan un seguimiento adecuado de Control en las distintas Actividades de Implantación del Sistema, con la finalidad de realizarlas en el Tiempo Programado y con los Recursos establecidos, el Jefe de la Unidad de Gestión Integrada del comité de implantación es el responsable de llevar este control y lo efectuará semanalmente, para poder corregir desviaciones en un tiempo mínimo. A continuación se presenta el formato propuesto para llevar este control.

FORMATO DE SEGUIMIENTO DE LAS ACTIVIDADES DE IMPLANTACIÓN									
ACTIVIDAD	**DEPENDENCIA**	**DESCRIPCIÓN DE ACTIVIDAD**	**RESPONSABLE**	**FECHA INICIO**	**FECHA FINALIZACION**	**SEGUIMIENTO**			
						REALIZADA		**FECHA DE FINALIZACIÓN**	**OBSERV.**
A	....	Creación del presupuesto para la implantación y Operación del SGSI	GERENTE DEL PROYECTO	01/10/2009	16/10/2009	SI	NO		
B	A	Evaluación y aprobación del Plan de Implantación	ALTA GERENCIA	19/10/2009	06/11/2009	SI	NO		
C	B	Creación del Comité de Implantación del SGSI	ALTA GERENCIA	09/11/2009	23/11/2009	SI	NO		
D	C	Contratación del personal de Capacitación en GSI	GERENTE DEL PROYECTO	24/11/2009	3/12/2009	SI	NO		
E	D	Capacitación y Taller con niveles estratégicos y tácticos en Gestión y Manejo de la seguridad de la información	ASESORIA EXTERNA	4/12/2009	9/12/2009	SI	NO		
F	E	Capacitación Estratégica y Capacitación Táctica	ASESORIA EXTERNA	10/12/2009	17/12/2009	SI	NO		
G	F	Capacitación: análisis y evaluación del riesgo.	ASESORIA EXTERNA	18/12/2009	4/1/2010	SI	NO		
H	G	Capacitación: Políticas de seguridad de la información y objetivos	ASESORIA EXTERNA	5/1/2010	11/1/2010	SI	NO		
I	H	Capacitación y Taller: Evaluación de las opciones para el tratamiento de riesgo	ASESORIA EXTERNA	12/1/2010	20/01/2010	SI	NO		
J	I	Capacitación y Taller: Selección de controles y objetivos de control	ASESORIA EXTERNA	21/01/2010	29/01/2010	SI	NO		
K	J	Capacitacion: Declaracion de Aplicabilidad	ASESORIA EXTERNA	1/2/2010	5/2/2010	SI	NO		
L	K	Capacitación y taller: Análisis de riesgo y escenarios de amenazas	ASESORIA EXTERNA	8/2/2010	16/02/2010	SI	NO		
M	L	Capacitación y Taller: Estrategias de continuidad.	ASESORIA EXTERNA	16/02/2010	22/02/2010	SI	NO		
N	M	Capacitación y taller: Plan de reanudación de operaciones	ASESORIA EXTERNA	23/02/2010	1/3/2010	SI	NO		
O	N	Capacitación :Plan de tratamiento de riesgos	ASESORIA EXTERNA	2/3/2010	9/3/2010	SI	NO		
P	O	Capacitación y taller : efectividad de controles y métricas	ASESORIA EXTERNA	10/3/2010	16/3/2010	SI	NO		
Q	P	Capacitación y Taller: Incidentes y eventos de seguridad	ASESORIA EXTERNA	17/03/2010	23/3/2010	SI	NO		
R	Q	Capacitación y taller: revisiones periódicas del SGSI	ASESORIA EXTERNA	24/3/2010	30/3/2010	SI	NO		

S	R	Capacitación: Como Implementar Las Acciones Correctivas y Preventivas	ASESORIA EXTERNA	31/3/2010	6/4/2010	SI	NO		
T	S	Entrenamiento en Documentación del SGSI	ASESORIA EXTERNA	7/4/2010	12/4/2010	SI	NO		
U	T	Entrenamiento en manejo de la acción Correctiva y Preventiva	ASESORIA EXTERNA	13/4/2010	16/4/2010	SI	NO		
V	U	Entrenamiento en manejo de la auditoria interna.	ASESORIA EXTERNA	19/4/2010	22/4/2010	SI	NO		
W	V	Entrenamiento en el manejo del sistema de información	ASESORIA EXTERNA	23/4/2010	28/4/2010	SI	NO		
X	W	Capacitación: Manual de seguridad de la información.	ASESORIA EXTERNA	29/4/2010	5/5/2010	SI	NO		
Y	X	Montaje del Espacio fisico de la Oficina de Manejo y seguridad de la información	GERENTE DEL PROYECTO	6/5/2010	19/5/2010	SI	NO		
Z	Y	Prueba Piloto del Sistema de manejo y seguridad de la información	GERENTE DEL PROYECTO	20/5/2010	10/6/2010	SI	NO		
AA	Z	Evaluación de la Implantación y Retroalimentación	GERENTE DEL PROYECTO	11/6/2010	22/6/2010	SI	NO		
AB	AA	Puesta en Operación del Sistema de manejo y seguridad de la información	GERENTE DEL PROYECTO	23/6/2010	1/7/2010	SI	NO		
AC	AB	Ejecucion de auditorias Internas	GERENTE DEL PROYECTO	2/7/2010	9/8/2010	SI	NO		
AD	AC	Búsqueda de la Empresa certificadora.	ALTA GERENCIA	10/8/2010	18/8/2010	SI	NO		
AE	AD	Realización de la auditoria por parte de la certificadora	GERNTE DEL PROYECTO	19/8/2010	9/9/2010	SI	NO		
AF	AE	Obtencion de la certificacion.	ALTA GERENCIA	10/9/2010	29/10/2010	SI	NO		

Tabla 130: Control de la implantación del proyecto.

M. CUADRO RESUMEN DE INDICADORES A UTILIZAR, EN EL PROYECTO DE IMPLEMENTACION DEL SGSI

NOMBRE	FORMULA	DESCRIPCION.
% de avance **PA**	$\frac{AR\_(avance\_real)}{AP\_(avance\_programado)}$	**Permite observar el avance de las actividades al tiempo de control, así como el porcentaje de avance de todo el proyecto, ya que es un índice que se realizara para avance individual y acumulado.**
% de ejecución del tiempo **PET**	$\frac{TR(tiempo\_real)}{TP(tiempo\_programado}$	**Permite observar las variaciones de la programación de tiempo de ejecución a nivel de los subsistemas para poder tomar decisiones respecto a correcciones en las actividades.**
Grado de cobertura del trabajo **GCT**	$\frac{actividades\_finalizadas}{actividades\_programadas\_a\_finalizar.}$	**Da el resultado de la planeación de ejecución de las actividades para un subsistema específico.**
Desvío de la ejecución del periodo de tiempo **DEPT**	Fechas programadas de finalización - fecha real de finalización.	**Permite conocer las variaciones respecto a fechas de inicio y finalización de actividades, para poder modificar las siguientes actividades en sus fechas de inicio y finalización.**
Nivel de desvío del plan **NDP**	$\frac{actividades\_no\_programadas\_realizadas}{actividades\_programadas\_realizadas}$	**Permite medir la planeación realizada por el jefe del proyecto, midiendo el grado de conocimiento del jefe con respecto al proyecto.**
Cumplimiento del plan **CP**	$\frac{actividades\_atrasadas}{actividades\_programadas.}$	**Permite observar el porcentaje de atraso de las actividades para un subsistema para ajustar la planeación de ejecución de las mismas.**
Costos directos administrativos de operación por actividad. **CDAOPA**	$\frac{gastos\_ad\ \min\ istrativos}{actividades\_realizadas.}$	**Permite conocer, cuanto está costando en la parte administrativa la realización de las actividades en promedio.**

Tabla 131: Indicadores de la implantación del proyecto.

N. CERTIFICACION ISO 27000[29]

Certificación

Las organizaciones internacionales de normalización llevan años trabajando en la estandarización de estos sistemas y desde febrero de 2004 existe una norma nacional de certificación, la UNE-71502:2004, que será una importante herramienta para las empresas y consultores que decidan acometer este tipo de proyectos.

En concreto esta norma determina el marco para establecer, implantar, documentar y evaluar un SGSI de acuerdo a la norma UNE-ISO/IEC-17799:2002 dentro del contexto de los riesgos identificados por la organización. La UNE-ISO/IEC-17799:2002 presenta a su vez un Código de buenas prácticas para la gestión de la Seguridad de la Información.

El Proceso de Certificación ISO 27000, tiene como objetivo demostrar a Terceros la conformidad del Sistema de Gestión con los requisitos de las Normas ISO 27000.
La *"Propuesta del SGSI bajo las normas ISO 27000"* que se ha presentado, contiene el diseño de los instrumentos necesarios para cumplir con los requisitos de las Normas ISO 27000.

1. **Actividades a Desarrollar en el Proceso de Certificación ISO 27000**

La Propuesta del Sistema de Gestión llega hasta la Etapa de Implementación del Sistema. Por lo tanto para que CEL logre la Certificación en lSO 27000, debe de realizar las siguientes actividades:

a) Contactar una Entidad Certificadora

CEL debe Acudir a una entidad certificadora para iniciar los trámites respectivos. Entre algunas de las entidades reconocidas en el país que se encargan de estos procesos de certificación se puede mencionar AENOR.

b) Tramite Inicial de Certificación

Previo a los requisitos que la empresa certificadora exigirá a CEL, este deberá llenar una solicitud para iniciar Trámites de Proceso de Certificación.

[29] Ver Anexo 19: Solicitud de certificación .

c) Proceso de Certificación para AENOR:

El aporte que como equipo que desarrolla el Trabajo de Graduación hace a la contraparte es establecer los pasos que CEL tendrá que realizar para iniciar el proceso de certificación 6 meses o un año después del funcionamiento u operación del sistema, además para iniciar este proceso se proporciona la solicitud en el Anexo 19 para llevar a cabo el tramite con la empresa acreditada certificadora (AENOR), que es la empresa que ha certificado los otros tres sistemas de gestión que CEL posee.

El proceso se inicia tras la recepción de la solicitud que se remite a las empresas que lo requieren y consta, básicamente, de cinco fases:

a. Análisis de la Documentación

El Equipo Auditor estudia, en las oficinas de AENOR o en las de la empresa solicitante, la documentación del para evaluar su coherencia y adecuación a los requisitos de especificación ISO 27000.

b. Visita Previa

En ella los auditores visitan la empresa con los siguientes objetivos:

- Evaluar las acciones llevadas a cabo por la empresa como respuesta a las observaciones recogidas en el análisis de la documentación.
- Comprobar el grado de implantación y adecuación del SGSI de la empresa.
- Aclarar cuantas dudas pueda tener la empresa sobre el proceso de certificación.

c. Auditoria Inicial

El Equipo auditor evalúa el SGSI conforme a los requisitos de la especificación ISO 27000. Las no conformidades encontradas se reflejan en un informe que será comentado y entregado a la empresa en la Reunión final de Auditoria.

d. Plan de Acciones Correctivas

La empresa dispone de un plazo de tiempo establecido para presentar a AENOR un Plan de Acciones Correctivas dirigido a subsanar las no conformidades encontradas en la Auditoria.

e. Concesión

Los servicios de AENOR evalúan el informe de Auditoría y el Plan de Acciones Correctoras, procediendo en su caso, a la concesión de la Marca AENOR de seguridad de información.

En el Diagrama se presenta esquemáticamente cómo es el Proceso de Certificación de AENOR.

Figura 52: Proceso certificación de AENOR.

2. Beneficios de la implantación y certificación bajo la especificación ISO 27000 en CEL

Beneficios de ISO 27000:2005

La reputación de ISO y la certificación de la norma internacional ISO 27001:2005 aumenta la credibilidad de cualquier organización. La norma claramente demuestra la validez de su información y un compromiso real de mantener la seguridad de la información. El establecimiento y certificación de un SGSI puede así mismo transformar la cultura corporativa tanto interna como externa, abriendo nuevas oportunidades de negocio con clientes conscientes de la importancia de la seguridad, además de mejorar el nivel ético y profesional de los empleados y la noción de la confidencialidad en el puesto de trabajo. Aún más, permite reforzar la seguridad de la información y reducir el posible riesgo de fraude, pérdida de información y revelación.

Las organizaciones certificadas en la norma británica BS 7799 pasarán a estarlo en ISO 27001. Según el comunicado para la transición realizado por UKAS en Junio del año 2006, las compañías certificadas en la norma británica BS 7799-2:2002 dispondrán hasta Julio del año 2007 para hacer efectiva la transición.

Por qué SGS?

Obtener la certificación de su Sistema de Gestión de Seguridad de la Información con SGS ayudará a su organización a desarrollar y mejorar el rendimiento del sistema.

Su certificado ISO 27001:2005 obtenido por SGS le permite demostrar niveles altos en la seguridad de la información en el momento de competir por contratos en cualquier ámbito internacional o en actividades de expansión local con objeto de dar cabida a nuevas actividades de negocio.

Las evaluaciones realizadas por SGS a intervalos regulares le ayudan en el uso, monitorización y mejora continua de su sistema y procesos de gestión de la seguridad de la información. Estas evaluaciones mejoran la fiabilidad de su operativa interna para cumplir con los requisitos del cliente, además de una mejora global. También obtendrá el beneficio de una mejora significativa en la motivación, nivel de cumplimiento y entendimiento de la plantilla y su responsabilidad en la seguridad de la información

Hasta la fechas, cientos de pequeñas, medianas y grandes compañías internacionales hacen uso de los servicios de certificación de SGS para realizar las auditorías de sus SGSI según los requisitos del estándar ISO 27001:2005, ratificando a SGS como una de las primeras entidades de certificación preferidas a nivel mundial para este estándar.

Nuestro equipo de auditores cualificados y con experiencia en múltiples sectores de la industria y servicios desarrolla las auditorías de certificación en ISO 27001:2005 al nivel profesional más alto

con el objeto de ayudarle a alcanzar sus objetivos en seguridad de la información así como de negocio.

Beneficios de la ISO 27001

Entre los diferentes beneficios derivados del desarrollo del sistema de gestión de la seguridad de la información y la correspondiente certificación ISO 27001, destacan:

- Garantía de un elevado nivel de confidencialidad gracias a la reducción de los riesgos asociados;
- Garantía de un elevado nivel de disponibilidad gracias a la implementación de un centro de datos de elevada disponibilidad y redundancia y de un centro de disaster recovery que se podrá utilizar en caso de catástrofe;
- Mayor calidad de los servicios ofrecidos a los clientes como consecuencia de una mayor uniformidad y control de los procesos organizativos y de especificación, desarrollo y evaluación del software;
- Desarrollo y motivación de los recursos humanos mediante la responsabilizacion, sensibilización y formación continua en seguridad;
- Conformidad legal: la certificación demuestra a clientes y accionistas que la organización cumple las leyes y reglamentos aplicables, tanto del ordenamiento jurídico como de los reglamentos sectoriales
- Mejora de la imagen corporativa de CEL e incremento de la confianza y credibilidad de los clientes y socios, al tiempo que, en el mercado.

CONCLUSIONES

- ✓ Este documento cubre el vacio generado por la falta de un método documentado sobre cómo proceder a implantar en la Comisión Ejecutiva, un sistema de gestión de seguridad de la información, que le permita a la institución, minimizar los riesgos y asegurar la continuidad de las operaciones.
- ✓ Se presenta los pasos parar realizar dentro de la óptica de la norma ISO27001:2005, el análisis y evaluación de riesgos de activos de la información, así se definió como se establecieron las evaluaciones de tratamientos de riesgos.
- ✓ Se puede concluir que el funcionamiento adecuado del sistema estará directamente relacionado con el apoyo y el sustento que la cultura organizacional de CEL le proporciona al cumplimiento de las exigencias de la norma, Las creencias y valores así como la conducta de los empleados en la institución deben poder apoyar el funcionamiento del SGSI con la rigurosidad necesaria.
- ✓ La norma exige la existencia de una política de seguridad documentada que debe divulgarse en la organización. Así mismo la organización debe asegurarse de que todo el personal relevante este consiente de la relevancia e importancia de sus actividades de seguridad de la información, y de cómo ellos pueden contribuir a lograr los objetivos del sistema de gestión de seguridad de información. La norma pretende alcanzar la idea de que la cultura organizacional, donde se vaya a implantar el modelo, se enrumbe y apoye el funcionamiento del SGSI. La confidencialidad debe de estar arraigada a la cultura organizacional.
- ✓ El Costo del Diseño del SGSI es de $ 22,500.00, pero CEL no incurrirá en estos costos puesto que los tres consultores que han desarrollado este diseño son los estudiantes integrantes de este Trabajo de Graduación. Los Costos de Operación representan la inversión para el primer año de funcionamiento del Sistema de Gestión, siendo un total de $80,474.0
- ✓ El costo total a invertir es de $ 104,882.14
- ✓ Los Costos de Operación representan la inversión para el primer año de funcionamiento del Sistema de Gestión, siendo un total de $80,474.0
- ✓ Los Beneficios Económicos en el primer año de implementación del SGSI en los procesos claves y de apoyo son de $ 540,045.00
- ✓ El Beneficio Costo es de B/C: 8.36, por lo cual bajo este análisis se ACEPTA el Proyecto.
- ✓ La TRI para el proyecto es de 0.13 anos, traducido en meses nos da un aproximado de 1.5 meses, lo cual indica que el tiempo de recuperación es menor que un ano, con lo que concluimos que es proyecto es factible.
- ✓ Los Beneficios Sociales están orientados principalmente a mejorar el servicio de demanda de electricidad tanto para las distribuidoras como para los consumidores finales
- ✓ La duración del proyecto 134 días hábiles

RECOMENDACIONES

- ✓ Tomar este documento como base para futuras aplicaciones a otras instituciones que persigan diseñar un SGSI conforme a sus demandas.
- ✓ Implementar el Sistema Informático de Información Gerencial y así facilitar para los usuarios la implementación del mismo
- ✓ Para que se alcancen los objetivos planteados al inicio se recomienda utilizar este documento como guía para la implantación del mismo.
- ✓ Se recomienda hacer revisiones constantes para corroborar que el sistema está siendo implantado tal cual se ha programado.
- ✓ Se recomienda hacer partícipe al mayor número de personas en la implantación para que la cultura del SGSI sea parte de ellos.

GLOSARIO TECNICO Y ABREVIATURAS

Glosario Norma ISO 27000[30]

Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información, definidos en el contexto de las mismas. Se incluye la correspondencia en inglés de cada uno de los términos.

A

Acción correctiva

(Inglés: Corrective action). Medida de tipo reactivo orientada a eliminar la causa de una no-conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

Acción preventiva

(Inglés: Preventive action). Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI.

Accreditation body

Véase: Entidad de acreditación.

Aceptación del Riesgo

(Inglés: Risk acceptance). Según [ISO/IEC Guía 73:2002]: Decisión de aceptar un riesgo.

Activo

(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

Alcance

(Inglés: Scope). Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta

(Inglés: Alert). Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza

(Inglés: Threat). Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos

(Inglés: Risk analysis). Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Análisis de riesgos cualitativo

(Inglés: Qualitative risk analysis). Análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.

Análisis de riesgos cuantitativo

(Inglés: Quantitative risk analysis). Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Auditor

(Inglés: Auditor). Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

[30] http://www.iso27000.es/glosario.html

Auditoría

(Inglés: Audit). Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación

(Inglés: Authentication). Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

B

BS7799

Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información -no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información -es certificable-. La parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001. Como tal estándar, ha sido derogado ya, por la aparición de estos últimos.

BSI

British Standards Institution. Comparable al AENOR español, es la Organización que ha publicado la serie de normas BS 7799, además de otros varios miles de normas de muy diferentes ámbitos.

C

CEL: Comisión Ejecutiva Hidroeléctrica del Rio Lempa.

Checklist

Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Compromiso de la Dirección

(Inglés: Management commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confidencialidad

(Inglés: Confidenciality). Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Control correctivo

(Inglés: Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo

(Inglés: Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio

(Inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

Control preventivo

(Inglés: Preventive control). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

D

Declaración de aplicabilidad

(Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Desastre

(Inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva

(Inglés: Guideline). Según [ISO/IEC 13335-1:2004]: una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad

(Inglés: Availability). Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

E

Entidad de acreditación

(Inglés: Accreditation body). Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina)

Entidad de certificación

(Inglés: Certification body). Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27000, ISO 9000, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.

Estandarización

Según la ISO es "El proceso de formular y aplicar reglas con el propósito de realizar en orden una actividad específica, para el beneficio y con la obtención de una economía de conjunto óptimo teniendo en cuenta las características funcionales y los requisitos de seguridad…"

Evaluación de riesgos

(Inglés: Risk evaluation). Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento

(Inglés: information security event). Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva

(Inglés: Objective evidence). Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad,

integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

F

Fase 1 de la auditoría

Fase en la que, fundamentalmente a través de la revisión de documentación, se analiza en SGSI en el contexto de la política de seguridad de la organización, sus objetivos, el alcance, la evaluación de riesgos, la declaración de aplicabilidad y los documentos principales, estableciendo un marco para planificar la fase 2.

Fase 2 de la auditoría

Fase en la que se comprueba que la organización se ajusta a sus propias políticas, objetivos y procedimientos, que el SGSI cumple con los requisitos de ISO 27001 y que está siendo efectivo.

G

Gestión de claves

(Inglés: Key management). Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos

(Inglés: Risk management). Proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

I

Impacto

(Inglés: Impact). El costo para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.-.

Incidente

Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad

(Inglés: Integrity). Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos

(Inglés: Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO

Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799

Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO 19011

“Guidelines for quality and/or environmental management systems auditing”. Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001

Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005

ISO 27002

Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio de oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.

ISO 9000

Normas de gestión y garantía de calidad definidas por la ISO.

ISO/IEC TR 13335-3

"Information technology. Guidelines for the management of IT Security .Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

ISO/IEC TR 18044

"Information technology. Security techniques. Information security incident management" Guía de utilidad para la gestión de incidentes de seguridad de la información.

K

KWH: Kilo Wattas por Hora

N

No conformidad

(Inglés: Nonconformity). Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave

(Inglés: Major nonconformity). Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

Norma

Según la ISO "El documento establecido por consenso y aprobado por un organismo reconocido, que se proporciona para uso común y repetido reglas directrices o características para ciertas actividades o sus resultados, con el fin de conseguir un grado óptimo en un contexto dado"

NTCI: Normas Técnicas de Control Interno

O

Objetivo

(Inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

P

PHVA

Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

PEPSU: Proveedor-Entrada-Proceso-Salida-Usuario

Plan de continuidad del negocio

(Inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos

(Inglés: Risk treatment plan). Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad

(Inglés: Security policy). Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

Política de escritorio despejado

(Inglés: Clear desk policy). La política de la empresa que indica a los empleados que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.

PRA-XX: Procedimiento Administrativo número XX.

PRO-XX: Procedimiento Operativo número XX.

PRSN-XXX: Procedimiento Normativo número XXX.

R

RI-PRO-XX: Riesgos de información en el proceso de producción, Código XX

RI-COMER-XX: Riesgos de información en el proceso de comercialización, Código XX

RI-RRHH-XX: Riesgos de información en el proceso de Recursos Humanos, Código XX

RI-INFI-XX: Riesgos de información en el proceso de Informática Institucional, Código XX

RC: Registro de Calidad

Riesgo

(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual

(Inglés: Residual Risk). Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

S

Segregación de tareas

(Inglés: Segregation of duties). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información

Según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Selección de controles

Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI

(Inglés: ISMS). Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios de tratamiento de información

(Inglés: Information processing facilities). Según [ISO/IEC 27002:2005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Sistema de Gestión de la Seguridad de la Información

(Inglés: Information Systems Management System). Ver SGSI.

T

Tratamiento de riesgos

(Inglés: Risk treatment). Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

U

UGI: Unidad de Gestión Integrada.

UNE 71502

Norma española de ámbito local como versión adaptada de BS7799-2 (actual ISO 27001), que también guarda relación con UNE-ISO/IEC17799 mediante su Anexo A.

UT: Unidad de Transacciones

V

Valoración de riesgos

(Inglés: Risk assessment). Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad

(Inglés: Vulnerability). Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

FUENTES DE INFORMACIÓN

- ✓ Entrevistas realizadas:
  - o Lic. Rigoberto Salguero; Jefe de la Unidad de Gestión integrada.
  - o Licda. Nelly de Aguila; Jefe de la Unidad Informática Institucional.
  - o Ing. Cáceres; Jefe de la Unidad de Producción.
  - o Licda. Irma Elena de Urquilla; Jefe de la Unidad de Desarrollo Humano.
  - o Ing. Juan Carlos Rivera; Jefe de la Unidad de Comercialización.
- ✓ Protocolo de Procedimientos Interno de La Comisión Ejecutiva del Rio Lempa CEL.
  - o Autor: Unidad de Gestión Integrada
  - o Paginas de la 5 a la 32.
- ✓ Manual de Procedimientos de la Unidad de Gestión Integrada.
  - o Autor: Unidad de Gestión Integrada
  - o Paginas: de la 6 a la 68.
- ✓ Guía para una Gestión basada en Procesos
  - o Autor: Instituto Andaluz de Tecnología
  - o Capítulos del 1 al 3
- ✓ Metodología de Investigación
  - o Autor: Roberto Hernández Sampieri; Carlos Fernández Collado; Pilar Baptista Lucio
  - o Editorial: Mc Graw Hill, Mexico 2003
  - o Capítulos del 1 al 10.
- ✓ Tesis: "Propuesta de una Sistema de Gestión de Calidad basado en las Normas ISO 9 000 para la Facultad de Ingeniería y Arquitectura.
  - o Año 2005 T252
- ✓ Tesis: Propuesta de Diseño de un Sistema de Gestión de Calidad basado en las Normas ISO 9000:2000 en la Administración Académica Central de la Universidad de El Salvador
  - o Autores: Alicia Beatriz Azucena Martínez
  - o Rosa Melida Galeano Pérez
  - o Facultad de Ingeniería y Arquitectura. Ingeniería Industrial
- ✓ Consultas en internet.
  - http://www.iso27000.es
  - http://www.iso27000.es/sgsi.html
  - http://www.iso27000.es/iso27000.html
  - http://www.iso27000.es/glosario.html
  - http://www.iso27000.es/doc_sgsi_all.htm
  - http://www.sgsigroup.com/index_archivos/slide0001.htm

ANEXOS

ANEXO 1: SISTEMA DE GESTION INTEGRADA

A. SISTEMA DE GESTIÓN INTEGRADA

1. Introducción al Sistema de Gestión Integrada

La Comisión Ejecutiva Hidroeléctrica del Río Lempa, que a lo largo de este documento se ha denominado como "CEL" ha implementado un Sistema de Gestión Integrada (SGI), compuesto por los siguientes sistemas:

- Sistema de Gestión de la Calidad, basado en la norma ISO 9001:2000,
- Sistema de Gestión Ambiental, basado en la norma ISO 14001:2004, y un
- Sistema de Gestión de Seguridad y Salud Laboral, basado en la especificación OHSAS 18001:1999.

CEL adquiere la responsabilidad de dar cumplimiento a lo pactado dentro de la estructura del SGI; asumiendo la calidad, el medio ambiente y la seguridad y salud laboral como aspectos primordiales y estratégicos de la gestión de la Institución, mediante la participación activa y oportuna del recurso humano, como un medio eficaz para el logro de la Política Integrada y los Objetivos en el desarrollo de la gestión institucional.

2. Alcance del Sistema de Gestión Integrada

El Sistema de Gestión Integrada de CEL es aplicable a las actividades de *Generación* y *Comercialización* de energía eléctrica.
El Sistema es implementado, mantenido y mejorado en los siguientes centros de trabajo:

a) Oficinas Centrales, ubicadas en la Novena Calle Poniente, número 950, San Salvador;

b) Central Hidroeléctrica Cerrón Grande, ubicada en el Cantón Monte Redondo, Jurisdicción de Potonico, Departamento de Chalatenango, y el Cantón San Sebastián, Jurisdicción de Jutiapa, Departamento de Cabañas;

c) Central Hidroeléctrica 5 de Noviembre, ubicada en el Cantón San Nicolás, Jurisdicción de Sensuntepeque, Departamento de Cabañas, y el Cantón Potrerillos, Jurisdicción de Nombre de Jesús, Departamento de Chalatenango;

d) Central Hidroeléctrica 15 de Septiembre, ubicada en el Cantón San Lorenzo, Jurisdicción de San Ildefonso, Departamento de San Vicente, y el Cantó Condadillo, Jurisdicción de Estanzuelas, Departamento de Usulután;

e) Central Hidroeléctrica Guajóyo, ubicada en el Cantón Belén Guija, Jurisdicción de Metapán, Departamento de Santa Ana;

f) Complejo de Bodegas San Ramón, final 75 Avenida Norte y Calle El Volcán, San Ramón, Mejicanos; y,

g) Centro Social Costa CEL, kilómetro 6½ carretera a los Blancos, San Luis La Herradura, Departamento de la Paz.

3. El Sistema de Gestión Integrada

(Requisitos 4.1 de ISO 9001:2000, ISO 14001:2004 y OHSAS 18001:1999)

CEL ha estructurado su organización con una gestión por procesos, en el cual establece, documenta, implementa y mantiene un Sistema de Gestión Integrada con el fin de cumplir con su Política Integrada, sus objetivos y obtener una mejora continua de su Sistema, Productos y Procesos.

Estos últimos se clasifican en dos tipos: Procesos Clave o de Negocio y Procesos de Apoyo.

El sistema engloba la estructura organizativa, las responsabilidades, los procesos, los procedimientos y los recursos necesarios para llevar a cabo la gestión de la calidad, el medio ambiente y la seguridad y salud laboral en la organización y mejorar continuamente su eficacia.

El sistema de gestión integrada está sometido a un proceso de revisión y mejora continua basándose en la información que aporta el mismo sistema, incluyendo las comunicaciones de todo el personal, el cliente y otras partes interesadas.

Para desarrollar el Sistema de Gestión Integrada, se han establecido:

- Los procesos necesarios y la interacción de los mismos, los cuales se presentan en la sección B de este capitulo, IDENTIFICACIÓN DE LOS PROCESOS.
- El seguimiento de la satisfacción del cliente.
- Los métodos y criterios para asegurar el funcionamiento efectivo y el control de los procesos.
- La sistemática para asegurar la disponibilidad de la información necesaria para apoyar el funcionamiento efectivo y el seguimiento de los procesos.
- Las actividades para medir la conformidad en la ejecución de los procesos y su seguimiento, así como para llevar a cabo las acciones necesarias para lograr los resultados planificados y la mejora continúa de los mismos.

a) Descripción de la Documentación del Sistema de Gestión Integrada

(Requisitos 4.2 de ISO 9001:2000, y 4.4.4 de ISO 14001:2004 y OHSAS 18001:1999)

i. Documentación

La documentación del Sistema de Gestión Integrada de CEL tiene la siguiente estructura:

a) La Política de Gestión Integrada.

b) El Manual de Gestión Integrada (MGI), el cual describe el Sistema de Gestión Integrada, su alcance y la interacción entre los procesos y los procedimientos documentados.

c) El Manual de Descripción de Puestos (MDP), que establece las jerarquías, los perfiles, las responsabilidades y los riesgos laborales de cada puesto de trabajo.

d) El Manual de Organización, el cual describe las responsabilidades de cada dependencia de CEL.

e) Los procesos (fichas de procesos), los cuales son documentos que describen un conjunto de actividades mutuamente relacionadas, las cuales transforman elementos de entrada en resultados.

f) Los procedimientos, que son los documentos que describen las actividades o procesos que afectan a toda la organización, incluidos los procedimientos obligatorios exigidos por las Normas ISO 9001:2000, ISO 14001:2004 y la Especificación OHSAS 18001:1999. El Manual está integrado por dos categorías de procedimientos: Los procedimientos operativos, los que corresponden a la Coordinación Técnica o Coordinación de Proyectos, y los procedimientos administrativos, que corresponden al resto de dependencias de la organización.

g) Los registros, que presentan resultados de los procesos, procedimientos o instrucciones de trabajo y que proporcionan evidencia objetiva.

h) Documentos externos e internos.

Esta estructura documental se pueda apreciar en la figura siguiente:

ii. Administración de Documentos

(Requisitos 4.2.3 de ISO9001:2000, y 4.4.4 de ISO14001:2004 y OHSAS 18001:1999)

El procedimiento para la elaboración, modificación y control de documentos (PRA06-01) establece el método de CEL para elaborar, modificar, validar, aprobar, controlar, distribuir y archivar los documentos del Sistema de Gestión Integrada: manuales, fichas de proceso, procedimientos e instrucciones de trabajo.

Los documentos del sistema se mantienen en papel y en formato digital para consulta a través de la intranet.

iii. Control de Registros

(Requisitos 4.2.4 de ISO 9001:2000, 4.5.4 de ISO14001:2004 y 4.5.3 de OHSAS 18001:1999)

El control de los registros del SGI se lleva a cabo de acuerdo al procedimiento para la Elaboración, Modificación y Control de Documentos (PRA06-01).

En algunas dependencias los registros son digitales y se generan archivos de respaldo, de acuerdo a la periodicidad definida en los procedimientos correspondientes.

b) Medición Análisis y Mejora

(Requisito 8.1 de ISO 9001:2000)

Se ha definido la planificación e implantación de actividades de seguimiento, medición, análisis y mejora necesarias para asegurar la conformidad en la consecución del producto, así como de la mejora continua, verificación de la conformidad del Sistema de Gestión Integrada y la utilización de los métodos aplicables.

c) Seguimiento y Medición

i. Satisfacción del Cliente

(Requisito 8.2.1 de ISO 9001:2000)

La Unidad de Gestión Integrada cuenta con un sistema de seguimiento de la información, sobre la satisfacción y/o insatisfacción de los clientes como una de las medidas de las prestaciones del Sistema de Gestión Integrada. Para establecer los métodos de obtención y utilización de dicha información, se tiene definido el "Procedimiento para la Medición de la Satisfacción de los Clientes" (PRA06-06).

ii. Auditoría Interna

(Requisitos 8.2.2 de ISO 9001:2000, 4.5.5 de ISO 14001:2004 y 4.5.4 de OHSAS 18001:1999)

CEL lleva a cabo a intervalos planificados auditorías internas para determinar si el Sistema de Gestión Integrada es conforme con las actividades planificadas y con los requisitos establecidos por las Normas y Especificación de referencia, y por la propia organización, se encuentran implantados y se mantiene de forma eficaz.
De acuerdo con lo indicado en el procedimiento para la Planificación y Ejecución de Auditorías Internas del Sistema de Gestión Integrada (PRA06-04) el proceso comprende:

- ✓ La elaboración de los planes de auditoría;
- ✓ La asignación de auditores calificados e independientes de la actividad a auditar;
- ✓ La emisión de informes de auditoría su distribución al personal implicado;
- ✓ La identificación de no conformidades, la toma de acciones para eliminar las no conformidades, su seguimiento y verificación, mediante el procedimiento para el seguimiento y control de acciones correctivas y preventivas (PRA06-03) y,
- ✓ La obligación de registrar los resultados e informarlos al Comité de Gestión Integrada.

iii. Seguimiento y Medición de los Procesos

(Requisitos 8.2.3 de ISO 9001:2000, 4.5.1 de ISO 14001:2004 y OHSAS 18001:1999, y 4.5.2 de ISO 14001:2004)

Para confirmar la capacidad de los procesos estratégicos de satisfacer los resultados previstos en los planes de Mantenimiento, Generación, Financiero y de Operaciones, se tienen definidos índices de medición en los siguientes procesos: Procesos Claves: Comercialización y Producción; Procesos de Apoyo: Recursos Humanos, Adquisiciones, Presupuesto, Gestión de la Información, Proyectos, Contratos, Riesgos, Gestión Integrada, Servicios Generales y Facturación y Cobro.
De acuerdo a los datos de estos indicadores, cada área responsable de su proceso, debe tomar acciones necesarias en caso de que se alejen de los valores previstos.
Además, la Unidad de Gestión Integrada, consolida la información relativa a los índices para presentarla al Comité de Gestión Integrada, donde se efectúa el análisis correspondiente y la toma de decisiones para genera la mejora continua en los procesos según lo planificado. El método para la medición y seguimiento de los procesos, se describe en el procedimiento para la Mejora Continua del Desempeño (PRA06-02).
Además de lo estipulado en tal procedimiento, el seguimiento y medición está definido por:

- ✓ La evaluación del cumplimiento legal (PRA06-12);
- ✓ El seguimiento de objetivos, metas y programas (PRA06-02); y
- ✓ En los ámbitos ambientales y de seguridad y salud laboral, el seguimiento de indicadores definidos en los procedimientos relacionados.

La orientación a procesos de la ISO 9001 implica la identificación y descripción de los procesos, incluyendo los métodos de control y supervisión de los procesos claves y el seguimiento de los

mismos. Estos métodos deben permitir demostrar si los procesos, tal y como están definidos, permiten alcanzar los resultados planificados.
En caso de no ser así, se estarán tomando las acciones oportunas para asegurar, en todo caso, la conformidad del producto.

iv. Seguimiento y Medición del Producto

(Requisito 8.2.4 de ISO 9001:2000)

Por medio del procedimiento para la lectura y reporte de las variables de generación, (PR041-07), la Gerencia de Producción, a través de las superintendencias de cada central hidroeléctrica, mide y da seguimiento a las características del producto, con el objeto de verificar que se cumplan los requisaos planificados.
De acuerdo con la planificación de la realización del producto, la Gerencia de Producción comprueba que el producto (generación de energía eléctrica) cumpla con los requisitos planificados.
La medición y seguimiento del producto, de acuerdo con los criterios de aceptación, demuestran la conformidad del producto.
Se conservan registros que demuestran la evidencia de dicha conformidad, incluyendo los responsables de la operación de las unidades generadoras.

d) Control de No Conformidades

i. Control de producto no conforme

(Requisito 8.3 de ISO 9001:2000)

A través del procedimiento, "Gestión del Producto No Conforme (PRA06-07)", la CEL se asegura que el producto este conforme con los requisitos establecidos por el cliente.
CEL mantiene registros de la naturaleza de las no conformidades y de cualquier acción tomada posteriormente.

ii. No conformidades del sistema

(Requisitos 8.5.2 y 8.5.3 de ISO 9001:2000, 4.5.3 de ISO 14001:2004 y 4.5.2 de OHSAS 18001:1999)

Los hallazgos pueden efectuarse durante:

- ✓ Las Auditorías Internas;
- ✓ Las Auditorías Externas;
- ✓ Fallas de Equipos;
- ✓ Incumplimiento de Objetivos;
- ✓ Quejas de Clientes;

- ✓ Accidentes o Incidentes Laborales y Ambientales;
- ✓ En la ejecución de Procesos; y,
- ✓ En los análisis de Procesos del Sistema.

Para el tratamiento de las no conformidades y observaciones se ha desarrollado el procedimiento para el seguimiento y control de acciones correctivas y preventivas, (PRA06-03).
Los accidentes y los incidentes, tanto ambientales como de seguridad, así como las enfermedades profesionales, son considerados no conformidades. Adicionalmente al procedimiento para el seguimiento y control de acciones correctivas y preventivas, (PRA06-03), los accidentes e incidentes activan el procedimiento para la notificación, respuesta, registro y análisis de accidentes e incidentes (PRA06-16). Por su parte, las enfermedades profesionales se gestionan de acuerdo al procedimiento del mismo nombre, PRA16-05.

iii. Análisis de Datos

(Requisitos 8.4 de ISO 9001:2000 y 4.5.1 de ISO 14001:2004 y OHSAS 18001:1999)
Con el objetivo final de determinar la adecuación y eficacia del Sistema de Gestión Integrada y de identificar las áreas de mejora, el Jefe de la Unidad de Gestión Integrada dispone permanentemente, para su análisis sistemático, de los siguientes datos, relativo al funcionamiento del Sistema:

- ✓ Resultados de la medida del grado de satisfacción del cliente, según Satisfacción del Cliente (Requisito 8.2.1 de ISO 9001:2000);
- ✓ Registros de no conformidades (indicado en No conformidades del sistema (Requisitos 8.5.2 y 8.5.3 de ISO 9001:2000, 4.5.3 de ISO 14001:2004 y 4.5.2 de OHSAS 18001:1999) y Control de producto no conforme (Requisito 8.3 de ISO 9001:2000)).
- ✓ Los resultados del seguimiento y medición de los productos y procesos que puedan tener un impacto significativo sobre la calidad, el medio ambiente o las condiciones de seguridad y salud laboral, conforme a lo establecido en los apartados: Seguimiento y Medición de los Procesos (Requisitos 8.2.3 de ISO 9001:2000, 4.5.1 de ISO 14001:2004 y OHSAS 18001:1999, y 4.5.2 de ISO 14001:2004) Seguimiento y Medición del Producto (Requisito 8.2.4 de ISO 9001:2000);
- ✓ Los resultados del seguimiento de indicadores y objetivos/metas, de acuerdo a lo indicado en el procedimiento para la mejora continua del desempeño (PRA06-02);
- ✓ Los resultados de la evaluación de proveedores y contratistas.

e) Mejora

i. Mejora Continua

(Requisito 8.5.1 de ISO 9001:2000 y 4.2, 4.3.3 y 4.6 de ISO 14001:2004 y OHSAS 18001:1999)

La mejora continua se define como la acción recurrente para aumentar la capacidad para cumplir los requisitos.
La Comisión dentro de su plan estratégico ha definido la mejora continua como un objetivo permanente dentro de la organización.
Las jefaturas deben de buscar continuamente mejorar la eficacia de los procesos de la organización antes de que un problema revele oportunidades para la mejora.
La organización debe mejorar continuamente la eficacia del Sistema de Gestión Integrada mediante la aplicación de la Política de Gestión Integrada, los Objetivos, los resultados de las todas internas y externas, los resultados de las inspecciones no programadas de seguridad industrial (PR041-123), el análisis de datos (indicado en Análisis de Datos (Requisitos 8.4 de ISO 9001:2000 y 4.5.1 de ISO 14001:2004 y OHSAS 18001:1999)), las acciones correctivas y preventivas y la revisión por la Dirección Ejecutiva.
La Unidad de Gestión Integrada, planifica y gestiona los procesos necesarios para la mejora continua del Sistema de Gestión Integrada, basados en la implantación de Proyectos de Mejora y Productividad, según la filosofía KAIZEN.

ii. Acción Correctiva

(Requisito 8.5.2 de ISO 9001:2000 y 4.5.3 de ISO 14001:2004 y OHSAS 18001:1999)
La aparición de no conformidades supone la toma de acciones para eliminar la causa de la no conformidad y evitar de esta forma su repetición. Estas acciones correctivas serán proporcionales a los efectos de las no conformidades.
El proceso de gestión incluye:

a) Análisis de las no conformidades;
b) Determinación de sus causas;
c) Propuesta de acciones inmediatas y de acciones correctivas para evitar su repetición, responsables y plazos;
d) Implantación de las acciones correctivas; y
e) Comprobación de su eficacia y cierre.

Las acciones correctivas tendrán su origen en las no conformidades citadas anteriormente. Su gestión se describe en el procedimiento para el seguimiento y control de acciones correctivas y preventivas (PRA06-03).

iii. Acción Preventiva

(Requisito 8.5.3 de ISO 9001:2000 y 4.5.3 de ISO 14001:2004 y OHSAS 18001:1999)
Una acción preventiva es una acción tomada para eliminar la causa de una no conformidad potencial u otra situación indeseable antes de que ocurra. La acción preventiva se adopta para evitar que algo suceda

Para los puntos 8.5.2 y 8.5.3 la norma ISO 9001:2000 obliga a contar con un procedimiento, para nuestro caso es el procedimiento “Seguimiento y Control de las Acciones Correctivas y Preventivas" (PRA06-03), se deben registrar los resultados de las acciones tomadas.
Se ha establecido un método para eliminar la causa de no conformidades potenciales y prevenir, en consecuencia, su aparición. Las acciones preventivas son apropiadas a los efectos de las no conformidades potenciales.
El proceso de gestión supone:

a) Determinación de las no conformidades potenciales y sus causas;
b) Propuesta de acciones preventivas para evitar su ocurrencia, responsables y plazos;
c) Implantación de las acciones; y,
d) Comprobación de su eficacia y cierre.

f) Preparación y Respuesta ante Emergencias

(Requisito 4.4.7 de ISO 14001:2004 y OHSAS 18001:1999)

La identificación y evaluación de los aspectos ambientales en situaciones de emergencia en todos los centros de trabajo, se lleva a cabo mediante el método indicado en el procedimiento para la Identificación y Evaluación de Aspectos Ambientales (PRA06-08). De la misma manera, los riesgos laborales se identifican de acuerdo al procedimiento para identificación de peligros y evaluación y control de riesgos (PRA06-14).
Sobre la base de los procedimientos anteriores, se determinan los aspectos ambientales significativos y riesgos críticos en situación de emergencia que son considerados para la elaboración de los procedimientos y planes de respuesta a las situaciones de emergencia identificadas, tal como lo describe el procedimiento para la preparación y respuesta a emergencias (PRA06-115). Este procedimiento también establece el método para revisar los procedimientos de preparación y respuestas, en particular, después de la ocurrencia de una emergencia ambiental o de seguridad y establecer la forma de aplicar periódicamente tales procedimientos.
Los procedimientos derivados del procedimiento anterior, tienen por propósito prevenir y minimizar las probabilidades de enfermedades, lesiones a las personas e impactos ambientales que puedan estar asociadas a las situaciones de emergencia para las cuales han sido desarrollados. Estos procedimientos son activados por la aplicación del procedimiento para la notificación, atención a lesiones, análisis y registro de accidentes e incidentes (PRA06-16).

ANEXO 2: ELABORACIÓN IDENTIFICACIÓN Y MODIFICACIÓN DE PROCESOS.

Los procesos declarados en el Sistema de Gestión Integrada, son:

PROCESOS DE NEGOCIO (CLAVES): Son los que expresan el objeto y la razón de ser de la institución y que tienen impacto directo en el cliente externo. Son aquellos que directamente contribuyen a realizar el producto o brindar el servicio, en CEL tenemos:

- Proceso de Producción
- Proceso de Comercialización de Energía Eléctrica

PROCESOS DE APOYO: Son los procesos encargados de proveer a la organización de todos los recursos (materiales, humanos y financieros) y crear las condiciones para garantizar el exitoso desempeño de los procesos claves, básicos o fundaméntales de la entidad, en nuestro caso, tenemos:

- Proceso de Facturación y Cobro
- Proceso de Pagos
- Proceso de Administración de Riesgos
- Proceso de Gestión Integrada
- Proceso de Gestión de la Información
- Proceso de Recursos Humanos
- Proceso de Gestión de Adquisiciones
- Proceso de Gestión Presupuestaria
- Proceso de Servicios Generales
- Proceso de Suscripción, Cumplimiento y Terminación de Contratos
- Proceso de Proyectos

ELABORACIÓN

Unidad de Gestión Integrada:

- ❖ Promover la creación de un proceso, cuando surja la necesidad de crearlo en algún(as) área(s) específica(s) de la institución.
- ❖ Crear el equipo de trabajo que será responsable de documentar el proceso, (el equipo de trabajo tiene que estar conformado por las personas involucradas en el desarrollo del proceso y que por su experiencia pueden definir los requisitos de las entradas y salidas del mismo). En el equipo de trabajo participará también una persona de la Unidad de Gestión Integrada.
- ❖ El equipo de trabajo elaborará y validará el proceso, siguiendo los siguientes pasos:

Utilizar el formato RC06-001 de la "Figura 1", en donde:

a. Nombre M Proceso: Debido a que el proceso puede involucrar actividades de más de una dependencia, no siempre el nombre de éste coincidirá con el de la Dependencia que lo preparó. El nombre deberá describir al conjunto de actividades necesarias para transformar las entradas en salidas (resultados)

b. Ambiente de Trabajo: Considera el ambiente de trabajo dentro M cual se desarrolla el proceso, ejemplo: condiciones de seguridad industrial, de orden y limpieza, de iluminación, temperatura, etc. En este apartado se puede hacer mención a los procedimientos relacionados con la gestión M ambiente en los lugares de trabajo.

c. Procesos de Apoyo: Se refiere a otras actividades que son necesarias para que se ejecuten los procesos de negocio (claves), por ejemplo: Selección de personal, capacitación, administración de riesgos, presupuestos, mantenimientos, etc.
d. Entradas: Son los insumos necesarios para que el proceso pueda desarrollarse. Pueden ser documentos, información, materias primas, etc.
e. Requisitos de Entrada: Son las características técnicas que deben tener las entradas para que el proceso se ejecute eficientemente. Estos requisitos deben ser negociados y validados con los proveedores.
f. Proveedor: Es el suministrante de las entradas (insumos), puede ser una dependencia interna a la organización o un proveedor externo.
g. Subprocesos: Subdivisión de un proceso en un grupo de actividades relacionadas.
h. Salidas: Son los resultados del proceso y se puede decir que son las entradas luego de ser procesadas de acuerdo a las actividades de transformación que se ejecutan en cada sub-proceso.
i. Requisitos de Salida: Son las características técnicas que deben tener las salidas para considerar que el proceso fue bien ejecutado y que dichas salidas cumplen con los requisaos y expectativas del cliente. Estas salidas pueden servir de entrada para otros procesos.
j. Cliente: Es quien hará uso de nuestras salidas para iniciar su proceso y es quien define los requisitos de las salidas.
k. Infraestructura: Se refiere a las instalaciones o edificios en los que se lleva a cabo el proceso. En este apartado se mencionan los procedimientos relacionados con el mantenimiento de las mismas.
l. Recurso Humano: Indica los puestos y número de personas en cada puesto que desarrollan directamente el proceso y de los procedimientos relacionados.

m. Objetivo general del proceso: Debe definir para que se ejecuta ese proceso dentro de la Institución.
n. índice de medición: Son factores que nos permiten medir el rendimiento y desempeño de cada uno de los procesos planificados. Los indicadores se pueden expresar en ratios, porcentajes, números naturales, etc.
o. Frecuencia de Medición: Indica cada cuanto tiempo se estará evaluando el cumplimiento de los índices de medición. Cada año se debe de revisar el proceso para su validación incluyendo sus índices.
p. índice de Comparación: Son los resultados "meta", a los cuales la empresa quiere llegar con cada uno de sus procesos. Estos se pueden ajustar cada cierto tiempo con el objeto de optimizar el proceso.

IDENTIFICACIÓN

Codificar los esquemas de procesos, de acuerdo a la siguiente estructura: PR- Nombre del Proceso - No. de revisión, en donde:

PR:	Proceso
Nombre del Proceso:	Nombre general del proceso en forma resumida. El nombre del proceso no deberá tener como mínimo 5 caracteres.
No. de Revisión:	Número de la última revisión realizada al proceso, la cual se numerará en orden correlativo, comenzando por 01.-

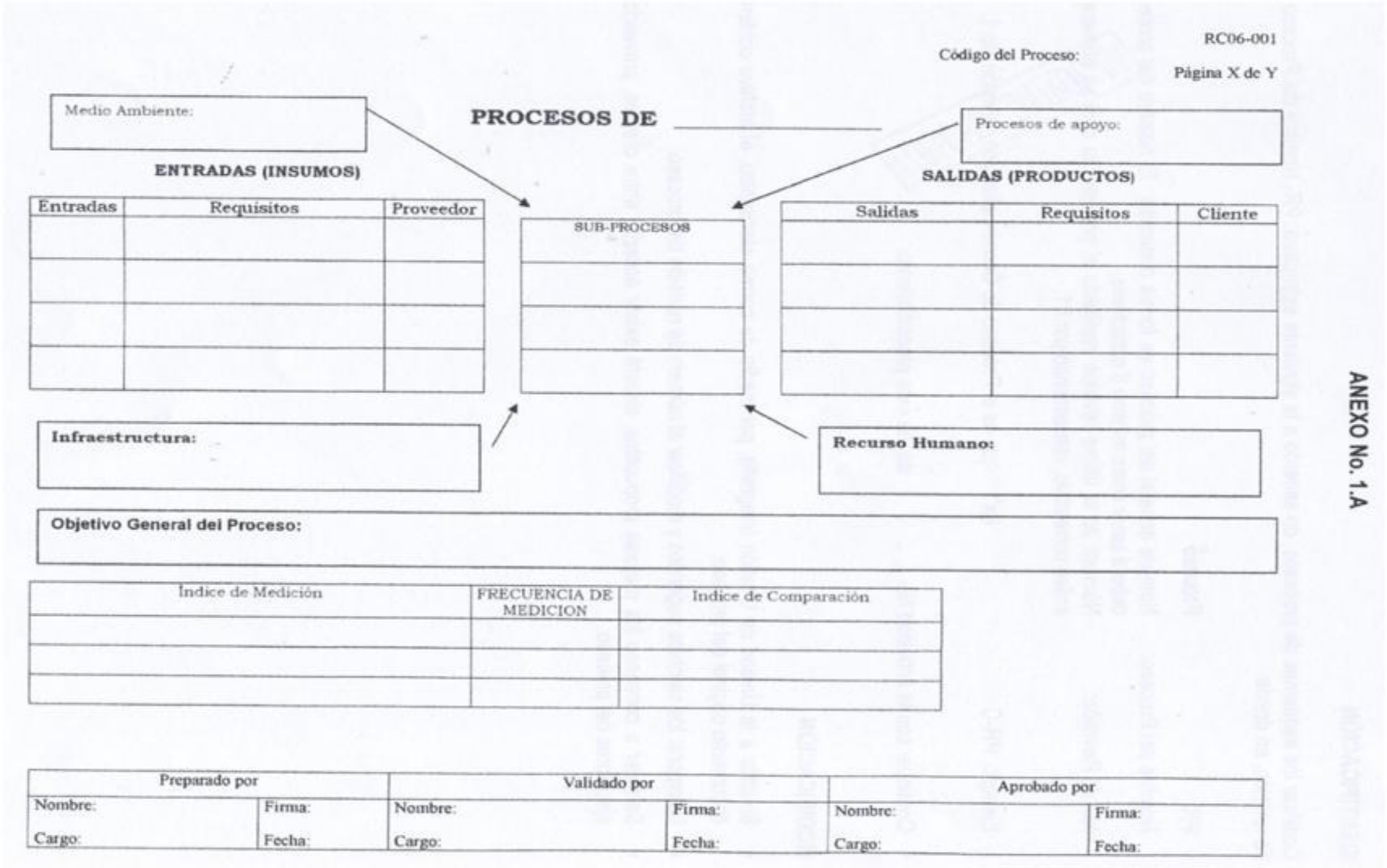
Ejemplo: PR-Comercialización-01 Indica que es el Proceso de Comercialización, revisión No. 1.

- ❖ Continuar con la actividad No. 2 en adelante, de este procedimiento.

MODIFICACIÓN

- Solicitar a la Unidad de Gestión Integrada, por medio de correo electrónico, el archivo conteniendo documento original del proceso.
- Incorporar los cambios sugeridos y modificar el número de revisión del proceso.
- Someter a consenso las mejoras propuestas, deberá existir acuerdo entre clientes, proveedores y ejecutores del proceso.

Figura 1:



Código del Proceso: RC06-001

Página X de Y

Medio Ambiente:

PROCESOS DE _____

Procesos de apoyo:

ENTRADAS (INSUMOS)

SALIDAS (PRODUCTOS)

Entradas	Requisitos	Proveedor

SUB-PROCESOS

Salidas	Requisitos	Cliente

Infraestructura:

Recurso Humano:

Objetivo General del Proceso:

Índice de Medición	FRECUENCIA DE MEDICION	Indice de Comparación

Preparado por		Validado por		Aprobado por	
Nombre:	Firma:	Nombre:	Firma:	Nombre:	Firma:
Cargo:	Fecha:	Cargo:	Fecha:	Cargo:	Fecha:

ANEXO No. 1.A

ANEXO 3: ELABORACIÓN IDENTIFICACIÓN Y MODIFICACIÓN DE PROCEDIMIENTOS Y REGISTROS

1. PROCEDIMIENTOS

Para la elaboración de procedimientos deberá formarse el equipo de trabajo que será responsable de documentar y/o modificar el procedimiento y definir las responsabilidades.
El equipo de trabajo tiene que estar conformado por las personas involucradas en el proceso y que por su experiencia, conocen más del mismo.

1.1. ELABORACIÓN DE PROCEDIMIENTOS

Utilizar el formato del Anexo No. 2.A

1) Escribir los procedimientos en computadora con letra "Arial" número 10, justificado, a espacio sencillo y los subtítulos se resaltarán en negrita y alinearán a la izquierda. El tipo de papel será Bond tamaño carta.
2) Llenar la página de Título y Aprobación de Procedimientos/instrucciones de Trabajo/Manuales (Anexo No. 2.A).
3) Detallar lo siguiente:
    a. Objetivo: ¿Qué se quiere lograr con el procedimiento?
    b. Alcance: Especifica el campo de aplicación del procedimiento.
    c. Disposiciones Legales o Reglamentarias.
4) Redactar el procedimiento:

Describir la forma especificada para llevar a cabo las actividades, tomando en cuenta los requerimientos del cliente, cumpliendo con lo siguiente:

- ❖ Iniciar todas las actividades con un verbo en infinitivo. No utilizar la palabra etc.
- ❖ No utilizar abreviaciones a menos que se contemplen en las definiciones.
- ❖ Escribir oraciones completas (Ejemplo.: Solicitar al Departamento….."el" archivo conteniendo "la" plantilla)
- ❖ Utilizar subtítulos para separar partes de un mismo procedimiento, si se considera necesario.
- ❖ No escribir actividades que no realiza el usuario del procedimiento, por ejemplo: actividades que realiza el proveedor, el contratista o el cliente.
- ❖ Si una actividad es muy complicada, ésta puede desmembrarse en una o varias instrucciones de trabajo.
- ❖ Identificar el/los responsable/s de cada actividad.
- ❖ Indicar, si fuera necesario, las especificaciones o aclaraciones que permitan comprender mejor la actividad.
- ❖ Determinar los recursos necesarios para realizar el procedimiento que se está documentando.
- ❖ Cuestionar todas las actividades en relación con:
    - ¿Qué? ¿Quién? ¿Cuándo? ¿Cómo? ¿Dónde? ¿Por qué? ¿Para qué? ¿Es útil? ¿A quién le sirve? ¿Se puede hacer más fácil, más seguro o más económico? ¿Aún es necesario?
    - Utilizar los siguientes criterios de reducción de actividades, teniendo presente:

- Lo que empieza por "RE".
- Lo que sólo genera costos.
- Lo que no agrega valor.
- Lo que no es útil a nadie.
- Lo que dificulta otros procesos.
- No se debe eliminar ningún requerimiento legal ni reglamentario vigente aplicable.

❖ Discutir las ventajas del nuevo procedimiento.
❖ Repetir los pasos anteriores hasta que el resultado sea satisfactorio y redactar el procedimiento en el cuadro que se presenta en el Anexo No. 2.A.
❖ Corregir el procedimiento, si hace falta.

5) Listar los anexos o instrucciones de trabajo que se incluyen en el procedimiento, agregándose con numeración continua a la del procedimiento y dentro del mismo formato del procedimiento. De ser necesario, se podrán incluir formularios incluidos en los anexos, en forma escaneada.
6) Definiciones. En este apartado se deberá elaborar un listado de las palabras que se utilizan en el procedimiento, explicando su significado cuando sea necesario aclarar algunos conceptos.

1.2. IDENTIFICACIONES DE PROCEDIMIENTOS.

CLASIFICACIÓN DE PROCEDIMIENTOS.

Los procedimientos se clasificarán de la siguiente forma:

PRO: Procedimientos de la Coordinación Técnica y Gerencia de Ingeniería.

PRA: Procedimientos Administrativos (todas las demás dependencias no incluidas en el inciso anterior).

- Código:

  Para la asignación de códigos de procedimientos, la Unidad de Gestión Integrada realizará lo siguiente:

  - Clasificar el procedimiento de acuerdo al inciso 1.2 y luego agregar el número asignado en el listado de Códigos de Dependencias, que sigue a continuación.

  - Luego, agregar un guión + el número correlativo del procedimiento, comenzando por 01.

- Revisión: Indica el No. de última revisión realizada al procedimiento, la cual se numerará en orden correlativo, comenzando por 00.

CÓDIGOS DE DEPENDENCIAS

NOMBRE DE LA DEPENDENCIA	CÓDIGO
Unidad de Gestión Integrada	06
Unidad de Estudios y Responsabilidad Social	07
Unidad de Comunicaciones	08
Unidad Comercial	09
Gerencia Legal	10
Departamento de Gestión y Financiamiento de Proyectos (UGCP)	14
Departamento de Seguimiento de Proyectos (UGCP)	15
Unidad Administración de Riesgos	16
Unidad de Informática Institucional	17
Unidad Adquisiciones y Contrataciones Institucionales	18
Departamento de Licitaciones	19
Departamento de Compras y Suministros	20
Gerencia Admón. y Desarrollo Humano	21
Unidad de Desarrollo Humano	22
Departamento de Administración de Contratos - UACI	23
Unidad Administrativa	24
Unidad de Servicios Generales	25
Departamento de Programación Financiera	30
Departamento de Tesorería	31
Unidad Ambiental	40
Gerencia de Producción	41
Superintendencia Cerrón Grande	42
Superintendencia 5 de Noviembre	47
Superintendencia 15 de Septiembre	52
Superintendencia Guajóyo	57
Gerencia de Ingeniería	61

NOTA: Los códigos han sido asignados hasta nivel de departamento.
Por ejemplo, en el procedimiento código PRA30-01:
PRA30 = indica que es un procedimiento que corresponde al Depto. de Programación Financiera
01 = que es el primer procedimiento de esa dependencia.

1.3. MODIFICACIÓN DE PROCEDIMIENTOS:

- Solicitar a la unidad de Gestión Integrada, por Medió de correo electrónico, el archivo conteniendo documento original del procedimiento.
- Llenar la hoja del “Anexo No. 2.B” e incorporaría M documento después de la hoja de título y aprobación.
- Incorporar los cambios sugeridos y modificar el número de revisión del procedimiento.

2. IDENTIFICACIÓN, Y MODIFICACIÓN DE REGISTROS.

2.1. IDENTIFICACIÓN

Los registros serán los formularios ya completados, que están incluidos en los procedimientos o instrucciones de trabajo relacionadas y que representan evidencia de la ejecución de la actividad.

- La codificación de registros será realizada por la Unidad de Gestión Integrada, de la siguiente forma:
  - Colocará en la parte superior derecha de cada formulario, las letras RC seguidas por el número asignado a la dependencia responsable del procedimiento de referencia y luego el número correlativo de tres dígitos.

Por ejemplo: RC41-001:
Indica que es el Registro No. 1 de la Gerencia de Producción.

- Además, elaborará el Listado de Control de Registros, utilizando el Formato RC06-004 del Anexo No. 6.3., en donde:
  - Código: código del registro.
  - Nombre: nombre del registro.
  - Documento de Referencia: Código del procedimiento o de la instrucción de trabajo que le da origen al registro.
  - Tiempo de Retención: Período mediante el cual se mantendrá el registro disponible.
  - Dependencia responsable: Dependencia responsable del procedimiento.
  - Disposición: Destino que se da al registro una vez que se cumple su tiempo de retención. Por ejemplo: destrucción, archivo en otro lugar, etc.

2.2. MODIFICACIÓN DE REGISTROS

Si necesita modificar los formularios:
De ser necesario hacer modificaciones a los formularios, se deberán seguir las indicaciones incluidas en la figura 2, para el caso de procedimientos y en el Anexo 3, sí son instrucciones de trabajo.
Tome en cuenta que si utiliza formularios diferentes a los que se encuentran en los procedimientos aprobados, se considerará una **no conformidad** con el Sistema de Gestión Integrada.

2.3. INDICACIONES PARA EL USO Y ARCHIVO DE LOS REGISTROS DEL SISTEMA DE GESTIÓN INTEGRADA:

En el caso de registros físicos (en papel):
Al utilizarlos:

- Use exclusivamente los formularios que están en los procedimientos aprobados.
- No modifique ninguno de los campos de los formularios.
- No modifique los títulos de los formularios.
- Complete los formularios con bolígrafo y con letra legible.
- Evite las enmendaduras, tachaduras y borrones

Al archivarlos tome en cuenta lo siguiente:

- Mantenga los registros en buen estado y limpios (por ejemplo: si manchas de grasa, café, comida, etc.)
- Los registros deben estar archivados de manera que puedan encontrarse en el menor tiempo posible.
- Los registros deben estar ordenados, ya sea, en orden cronológico, por registros del mismo tipo o asunto.
- El tiempo de resguardo de los registros deberá ser el establecido en el listado de control de registros del sistema de Gestión Integrad
- Al cumplirse el tiempo de resguardo de los registros, eliminar, guardar, microfilmar, los documentos que ya cumplieron con su tiempo de retención.

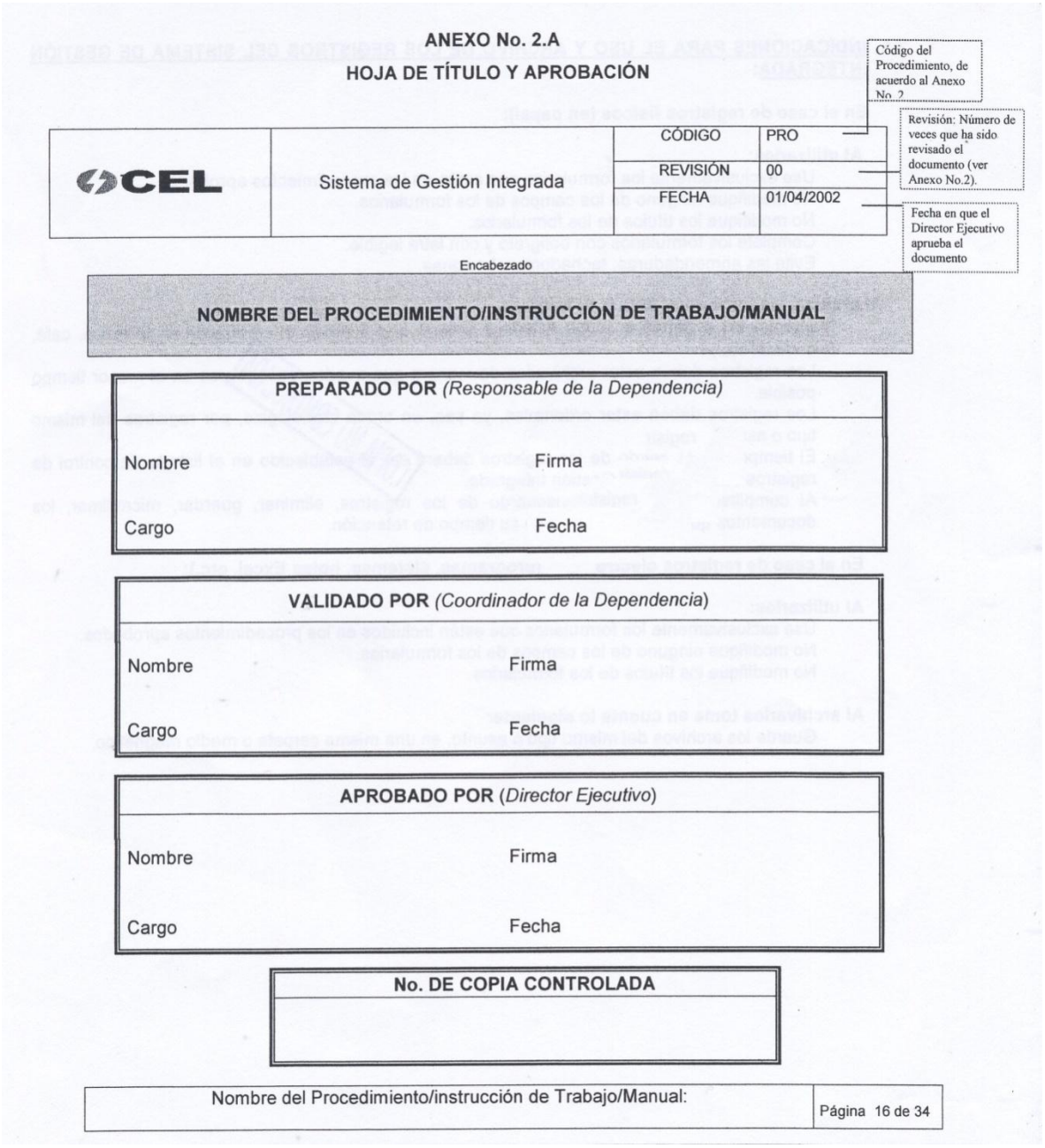
En el caso de registros electrónicos (programas, sistemas, hojas Excel, etc.):
Al utilizarlos:

- Use exclusivamente los formularios que están incluidos en los procedimientos aprobados.
- No modifique ninguno de los campos de los formularios.
- No modifique los títulos de los formularios.

Al archivarlos tome en cuenta lo siguiente:

- Guarde los archivos del mismo tipo o asunto, en una misma carpeta o medio magnético.

FIGURA 2:



ANEXO No. 2.A

HOJA DE TÍTULO Y APROBACIÓN

Código del Procedimiento, de acuerdo al Anexo No. 2

Revisión: Número de veces que ha sido revisado el documento (ver Anexo No.2).

Fecha en que el Director Ejecutivo aprueba el documento

CEL	Sistema de Gestión Integrada	CÓDIGO	PRO
		REVISIÓN	00
		FECHA	01/04/2002

Encabezado

NOMBRE DEL PROCEDIMIENTO/INSTRUCCIÓN DE TRABAJO/MANUAL

PREPARADO POR *(Responsable de la Dependencia)*	
Nombre	Firma
Cargo	Fecha

VALIDADO POR *(Coordinador de la Dependencia)*	
Nombre	Firma
Cargo	Fecha

APROBADO POR (*Director Ejecutivo*)	
Nombre	Firma
Cargo	Fecha

No. DE COPIA CONTROLADA

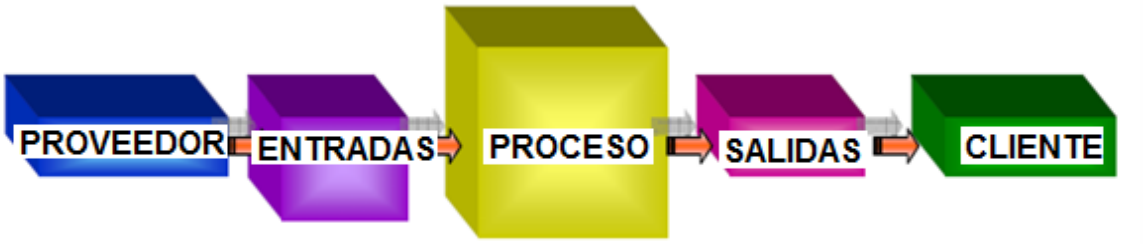
Nombre del Procedimiento/instrucción de Trabajo/Manual:	Página 16 de 34

ANEXO 4: HERRAMIENTAS Y TÉCNICAS DE INGENIERÍA A UTILIZAR.

A. HERRAMIENTAS Y TÉCNICAS DE INGENIERÍA A UTILIZAR

1. MODELO PEPSU (PROVEEDOR-ENTRADA-PROCESO-SALIDA-CLIENTE)

Técnica usada para la representación de procesos.



2. DIAGRAMA DE FLUJO DE DATOS

Definición

El Diagrama de Flujo es una representación gráfica de la secuencia de pasos que se realizan para obtener un cierto resultado. Este puede ser un producto, un servicio, o bien una combinación de ambos.

Los diagramas de flujos de datos (DFD), es una técnica de modelización, que nos muestra un sistema como una red de procesos conectados entre ellos por flujos y almacenamientos de datos.

Es un modelo que proporciona el punto de vista funcional de un sistema.

Características principales

Capacidad de Comunicación

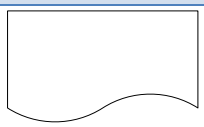
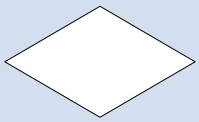
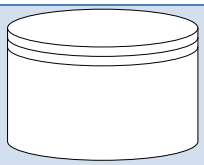
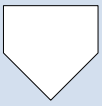
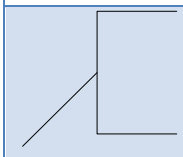
Permite la puesta en común de conocimientos individuales sobre un proceso, y facilita la mejor comprensión global del mismo.

Claridad

Proporciona información sobre los procesos de forma clara, ordenada y concisa.

Símbolo: Imagen o figura con la que se representa un concepto.

Simbología:

SÍMBOLO	REPRESENTA	SÍMBOLO	REPRESENTA
	Terminador (inicio y fin del flujo)		Entrada manual de Datos
	Proceso o actividad a realizar		Salida de Documentos
	Toma de decisión		Base de Datos
	Entrada de Datos		Almacenamiento
	Referencia o conector en la misma pagina		Referencia o conector para otra pagina
	Conector		
	Anotación o aclaración		Funcionamiento manual

3. MULTIVOTACIÓN

¿Qué es?

La Multivotación es una técnica en grupo para reducir una larga lista de elementos a unos pocos manejables (generalmente de tres a cinco).

¿Cuándo se utiliza?

- Utilizar la Multivotación cada vez que la técnica de Lluvia de Ideas o una técnica similar ha producido una lista larga que necesita reducirse.

- También deberá utilizarse al final de un Diagrama de Causa y Efecto, para seleccionar las primeras 3 a 5 “causas» a ser investigadas.

¿Cómo se utiliza?

1. Revisar la lista-, combinar los elementos similares, si es posible.
2. Asignar una letra a los elementos restantes (ver muestra, página siguiente).
3. Dar a cada miembro M equipo un número de votos igual al 20 por ciento del número de elementos en la lista. Se pueden suministrar “puntos” adhesivos a los participantes para pegar en el rota folio al lado de los elementos que seleccionen. Los miembros del equipo pueden determinar cómo distribuir sus votos: uno por elemento-, un número igual de votos a vados elementos; todos los votos a un elemento y sucesivamente.
4. Encerrar en un círculo los elementos que reciban el mayor número de votos.
5. Si todavía quedan más elementos de los deseados, se puede realizar una segunda ronda de votación. Utilizar únicamente los elementos señalados.
6. Repetir los pasos 4 y 5 hasta que la lista se reduzca de tres a cinco elementos.

Relación con otras Herramientas:
La Multivotación generalmente se relaciona con:

- ✓ Lluvia de Ideas
- ✓ Diagrama de Causa y Efecto
- ✓ Análisis del Campo de Fuerzas
- ✓ Matriz de planeación de acciones
- ✓ Checklist para la reunión de Datos
- ✓ Diagrama de afinidad.

4. DIAGRAMA SÍNTOMA-CAUSA-EFECTO

¿Qué es?

Un diagrama de Causa y Efecto es la representación de vados elementos (causas) de un sistema que pueden contribuir a un problema (efecto). Fue desarrollado en 1943 por el Profesor Kaoru Ishikawa en Tokio. Algunas veces es denominado Diagrama Ishikawa o Diagrama Espina de Pescado por su parecido con el esqueleto de un pescado. Es una herramienta efectiva para estudiar procesos y situaciones, y para desarrollar un plan de recolección de datos.

¿Cuándo se utiliza?

El Diagrama de Causa y Efecto es utilizado para identificar las posibles causas de un problema específico. La naturaleza gráfica del Diagrama permite que los grupos organicen grandes cantidades de información sobre el problema y determinar exactamente las posibles causas. Finalmente, aumenta la probabilidad de identificar las causas principales.

El Diagrama de Causa y Efecto se debe utilizar cuando se pueda contestar "sí" a una o a las dos preguntas siguientes

1. ¿Es necesario identificarlas causas principales de un problema?
2. ¿Existen ideas y/u opiniones sobre las causas de un problema?

Relación con otras Herramientas:

Un Diagrama de Causa y Efecto normalmente se relaciona con:

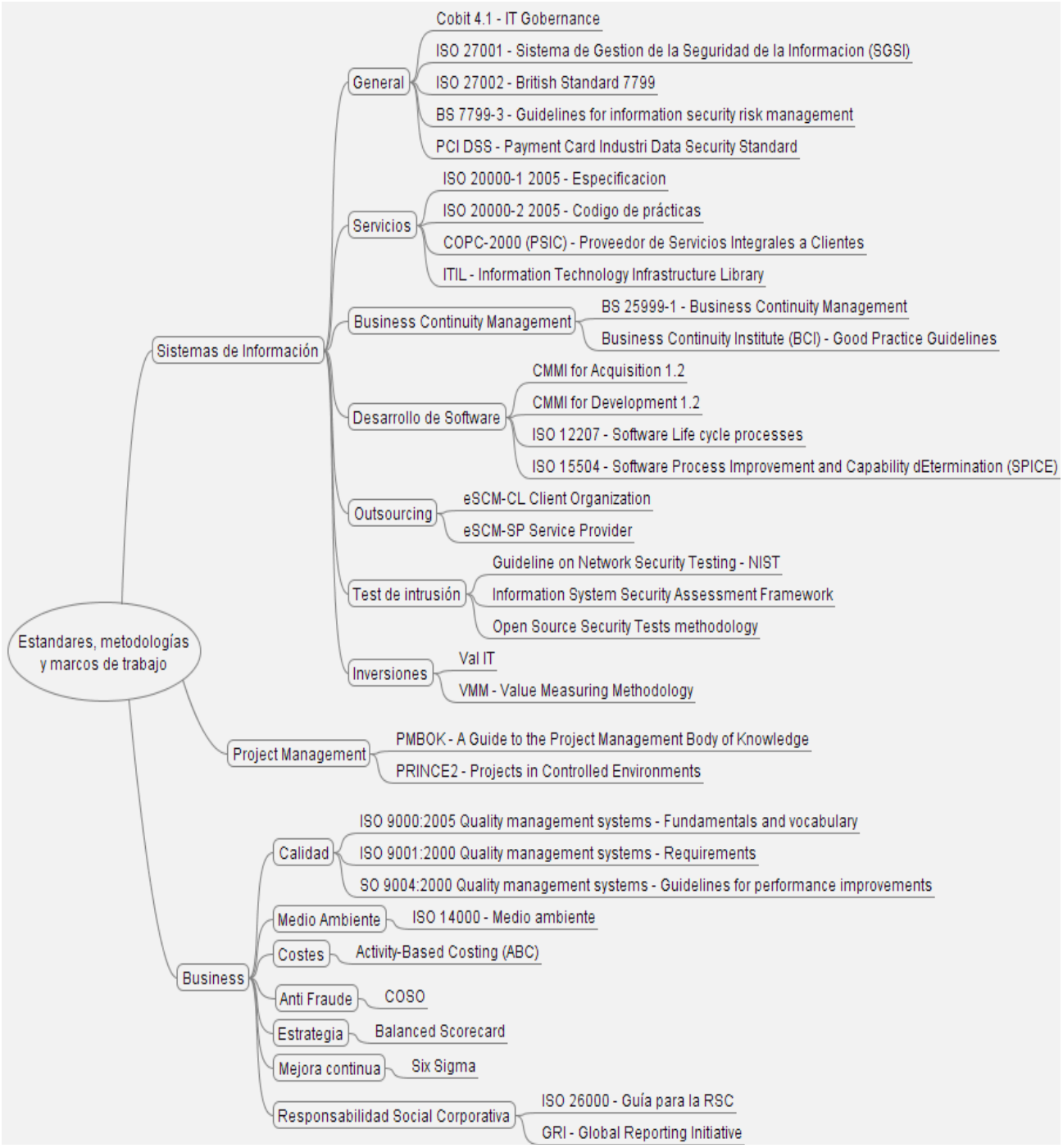
- ✓ Lluvia de Ideas
- ✓ Diagrama de Interrelaciones
- ✓ Gráfica de Pareto Multivotación
- ✓ Técnica de Grupo Nominal
- ✓ Diagrama de Afinidad
- ✓ Cinco Por Qués?

ANEXO 5: LISTADOS COMPLETO DE LOS ESTÁNDARES VIGENTES HASTA SEPTIEMBRE 2008, DESARROLLADOS Y PUBLICADOS POR EL COMITÉ TÉCNICO CONJUNTO Y SU SUB-COMITÉ ISO JTC1 / SC27.

ESTÁNDAR	DESCRIPCIÓN
ISO/IEC 9798-1:1997	Tecnología de la información, técnicas de seguridad, Autenticación de entidad Parte 1: Generalidades.
ISO/IEC 9798-2:1999	Tecnología de la información, técnicas de seguridad, Autenticación de entidad Parte 2: Mecanismos que usan algoritmos para la encriptación de datos o claves.
ISO/IEC 9798-3:1998	Tecnología de la información, técnicas de seguridad, parte 3: Mecanismos que usan técnicas de firma digitales.
ISO/IEC 9798-4:1999	Tecnología de la información, técnicas de seguridad, parte 4: Mecanismos que usan una función de comprobación criptográfica.
ISO/IEC 9798-5:2004	Tecnología de la información, técnicas de seguridad, parte 5: Mecanismos que usan técnicas de conocimiento cero.
ISO/IEC 9798-6:2005	Tecnología de la información, técnicas de seguridad, Parte 6: Mecanismos que usan el manual de transferencia de datos.
ISO/IEC 10116:2006	Tecnología de la información, técnicas de seguridad, Modos de operación que bloquean una cifra para un n bit.
ISO/IEC 10118-1:2000	Tecnología de la información, técnicas de seguridad, Métodos para generar claves: Parte 1: Generalidades.
ISO/IEC 10118-2:2000	**Tecnología de la información, técnicas de seguridad, Parte 2: Funciones para generar claves usando un bloqueo de cifras de N bit.**
ISO/IEC 10118-3:2004	Tecnología de la información, técnicas de seguridad, Parte 3: Funciones para generar claves delicadas.
ISO/IEC 10118-3:2004/Amd 1:2006	Tecnología de la información, técnicas de seguridad, Funciones para generar claves delicadas.
ISO/IEC 10118-4:1998	Tecnología de la información, técnicas de seguridad Parte 4: Funciones para generar claves usando una modulación aritmética.
ISO/IEC 11770-1:1996	Tecnología de la información, técnicas de seguridad, Manejo o control de claves Parte 1: estructura, marcos o esquemas.
ISO/IEC 11770-2:2008	Tecnología de la información, técnicas de seguridad, Manejo o control de claves Parte 2: Mecanismos que usan técnicas simétricas.
ISO/IEC 11770-3:2008	Tecnología de la información, técnicas de seguridad, Manejo o control de claves Parte 3: Mecanismos que usan técnicas asimétricas.
ISO/IEC 11770-4:2006	Tecnología de la información, técnicas de seguridad, Manejo o control de claves Parte 4: mecanismos basados en elementos ocultos.
ISO/IEC 13335-1:2004	Tecnología de la información, técnicas de seguridad, Manejo de la información y tecnología en la seguridad de la información, Parte 1: Conceptos y modelos para información y dirección de seguridad de tecnología de comunicaciones.
ISO/IEC 13888-1:2004	Técnicas de seguridad, no rechazadas, parte 1: generalidades.

ISO/IEC 13888-2:1998	Tecnología de la información, técnicas de seguridad, Técnicas de seguridad, no rechazadas, parte 2: Mecanismos que usan técnicas simétricas.
ISO/IEC 13888-3:1997	Tecnología de la información, técnicas de seguridad, Técnicas de seguridad, no rechazadas, parte 3: Mecanismos que usan técnicas asimétricas.
ISO/IEC TR 14516:2002	Tecnología de la información, técnicas de seguridad, Directrices para el empleo y dirección de servicios de confianza a terceras partes.
ISO/IEC 14888-1:2008	Tecnología de la información, técnicas de seguridad, Firmas digitales con apéndice - Parte 1: Generalidades.
ISO/IEC 14888-2:2008	Tecnología de la información, técnicas de seguridad, Firmas digitales con apéndice - Parte 2: Mecanismos basados en factorización de números enteros.
ISO/IEC 14888-3:2006	Tecnología de la información, técnicas de seguridad, Firmas digitales con apéndice - Parte 3: Mecanismos basados en logaritmos discretos.
ISO/IEC 15292:2001	Tecnología de la información, técnicas de seguridad, Procedimientos de registro del Perfil de protección.
ISO/IEC 15408-1:2005	Tecnología de la información, técnicas de seguridad, Criterio de evaluación para la seguridad IT Parte 1: Introducción y modelo general.
ISO/IEC 15408-2:2008	**Tecnología de la información, técnicas de seguridad, Criterio de evaluación para la seguridad IT, Parte: 2: Componentes funcionales de seguridad.**
ISO/IEC 15408-3:2008	Tecnología de la información, técnicas de seguridad, Criterio de evaluación para la seguridad IT, Parte 3: Componentes de aseguramiento/garantía de Seguridad.
ISO/IEC TR 15443-1:2005	Tecnología de la información, técnicas de seguridad, Un marco para el aseguramiento de seguridad IT - Parte 1: Descripción y marco.
ISO/IEC TR 15443-2:2005	Tecnología de la información, técnicas de seguridad, Un marco para el aseguramiento de seguridad IT, Parte 2: métodos de aseguramiento.
ISO/IEC TR 15443-3:2007	Tecnología de la información, técnicas de seguridad, Un marco para el aseguramiento de seguridad IT, Parte 3: análisis de métodos de aseguramiento.
ISO/IEC TR 15446:2004	Tecnología de la información, técnicas de seguridad, Guía para la producción de Perfiles de Protección y Seguridad Objetiva.
ISO/IEC 15816:2002	Tecnología de la información, técnicas de seguridad, Objetos de Seguridad Información para el control de acceso.
ISO/IEC 15945:2002	Tecnología de la información, técnicas de seguridad, Especificación de servicios TTP para apoyar el uso de firmas digitales.
ISO/IEC 15946-1:2008	Tecnología de la información, técnicas de seguridad, Técnicas criptográficas basadas en curvas elípticas Parte 1: Generalidades
ISO/IEC 18014-1:2008	Tecnología de la información, técnicas de seguridad, servicios de marcación de tiempo, Parte 1: Estructura.
ISO/IEC 18014-2:2002	Tecnología de la información, técnicas de seguridad, servicios de marcación de tiempo, Parte 2: Mecanismos que producen señales independientes.
ISO/IEC 18014-3:2004	Tecnología de la información, técnicas de seguridad, servicios de marcación de tiempo, Parte 3: Mecanismos que producen señales unidas.
ISO/IEC 18028-1:2006	Tecnología de la información, técnicas de seguridad, red de seguridad IT, Parte 1: Manejo / dirección de red de seguridad.
ISO/IEC 18028-2:2006	Tecnología de la información, técnicas de seguridad, red de seguridad IT, Parte 2: Arquitectura de seguridad de red.
ISO/IEC 18028-3:2005	Tecnología de la información, técnicas de seguridad, red de seguridad IT. Parte 3: Aseguramiento de comunicaciones entre redes usando entradas de seguridad.
ISO/IEC 18028-4:2005	Tecnología de la información, técnicas de seguridad, red de seguridad IT, Parte 4: Asegurando de acceso remoto.
ISO/IEC 18028-5:2006	Tecnología de la información, técnicas de seguridad, red de seguridad IT, Parte 5: Asegurar comunicaciones a través de redes que usan redes virtuales privadas.

ISO/IEC 18031:2005	Tecnología de la información, técnicas de seguridad, Generación de bit aleatorios.
ISO/IEC 18032:2005	Tecnología de la información, técnicas de seguridad, Generación de números primos.
ISO/IEC 18033-1:2005	Tecnología de la información, técnicas de seguridad, Encriptación de algoritmos, Parte 1: Generalidades.
ISO/IEC 18033-2:2006	**Tecnología de la información, técnicas de seguridad, Encriptación de algoritmos; Parte 2: cifras asimétricos.**
ISO/IEC 18033-3:2005	Tecnología de la información, técnicas de seguridad, Encriptación de algoritmos; Parte 3: Bloqueo de cifras.
ISO/IEC 18033-4:2005	Tecnología de la información, técnicas de seguridad, Encriptación de algoritmos; Parte 4: Flujo de cifras.
ISO/IEC 18043:2006	Tecnología de la información, técnicas de seguridad, Selección, despliegue y operaciones de sistemas de detección de intrusión.
ISO/IEC TR 18044:2004	Tecnología de la información, técnicas de seguridad; Manejo de incidentes en la seguridad de la información.
ISO/IEC 18045:2008	Tecnología de la información, técnicas de seguridad, Metodología para la evaluación de la seguridad IT.
ISO/IEC 19790:2006	Tecnología de la información, técnicas de seguridad, Requerimientos de seguridad de módulos de encriptación.
ISO/IEC TR 19791:2006	Tecnología de la información, técnicas de seguridad, Evaluación de Seguridad de sistemas operacionales.
ISO/IEC 21827:2002	Tecnología de la información, Ingeniería de Sistemas de Seguridad, Modelo de capacidad de maduración.
ISO/IEC 24759:2008	Tecnología de la información, técnicas de seguridad, requerimientos de evaluación para módulos criptográficos.
ISO/IEC 24762:2008	Tecnología de la información, técnicas de seguridad, Directrices para la información y servicios tecnológicos de comunicaciones para la recuperación en desastres.
ISO/IEC 27001:2005	Tecnología de la información, técnicas de seguridad, Sistemas de Gestión de seguridad de la información; Requisitos.
ISO/IEC 27002:2005	Tecnología de la información, técnicas de seguridad, Código de buenas Prácticas para Gestión de seguridad de la información.
ISO/IEC 27005:2008	Tecnología de la información, técnicas de seguridad, Administración de riesgos de la seguridad de la información.
ISO/IEC 27006:2007	Tecnología de la información, técnicas de seguridad, Requerimientos para estructura de auditorías y certificación de sistemas de Gestión de seguridad de la información.


Estandares, metodologías y marcos de trabajo
Sistemas de Información
General
Cobit 4.1 - IT Gobernance
ISO 27001 - Sistema de Gestion de la Seguridad de la Informacion (SGSI)
ISO 27002 - British Standard 7799
BS 7799-3 - Guidelines for information security risk management
PCI DSS - Payment Card Industri Data Security Standard
Servicios
ISO 20000-1 2005 - Especificacion
ISO 20000-2 2005 - Codigo de prácticas
COPC-2000 (PSIC) - Proveedor de Servicios Integrales a Clientes
ITIL - Information Technology Infrastructure Library
Business Continuity Management
BS 25999-1 - Business Continuity Management
Business Continuity Institute (BCI) - Good Practice Guidelines
Desarrollo de Software
CMMI for Acquisition 1.2
CMMI for Development 1.2
ISO 12207 - Software Life cycle processes
ISO 15504 - Software Process Improvement and Capability dEtermination (SPICE)
Outsourcing
eSCM-CL Client Organization
eSCM-SP Service Provider
Test de intrusión
Guideline on Network Security Testing - NIST
Information System Security Assessment Framework
Open Source Security Tests methodology
Inversiones
Val IT
VMM - Value Measuring Methodology
Project Management
PMBOK - A Guide to the Project Management Body of Knowledge
PRINCE2 - Projects in Controlled Environments
Business
Calidad
ISO 9000:2005 Quality management systems - Fundamentals and vocabulary
ISO 9001:2000 Quality management systems - Requirements
SO 9004:2000 Quality management systems - Guidelines for performance improvements
Medio Ambiente
ISO 14000 - Medio ambiente
Costes
Activity-Based Costing (ABC)
Anti Fraude
COSO
Estrategia
Balanced Scorecard
Mejora continua
Six Sigma
Responsabilidad Social Corporativa
ISO 26000 - Guía para la RSC
GRI - Global Reporting Initiative

ANEXO 6: METODOLOGÍA DE LA INVESTIGACIÓN.

A. METODOLOGÍA DE LA INVESTIGACIÓN

1. GENERALIDADES

Para dar inicio a la etapa de investigación y recopilación de datos es necesario describir el conjunto de pasos que se seguirá para la realización de esta, además de establecer el tipo de método de investigación a emplear con el fin de tener una guía especifica y una manera de proceder sobre la cual se desarrolle esta recopilación de información.

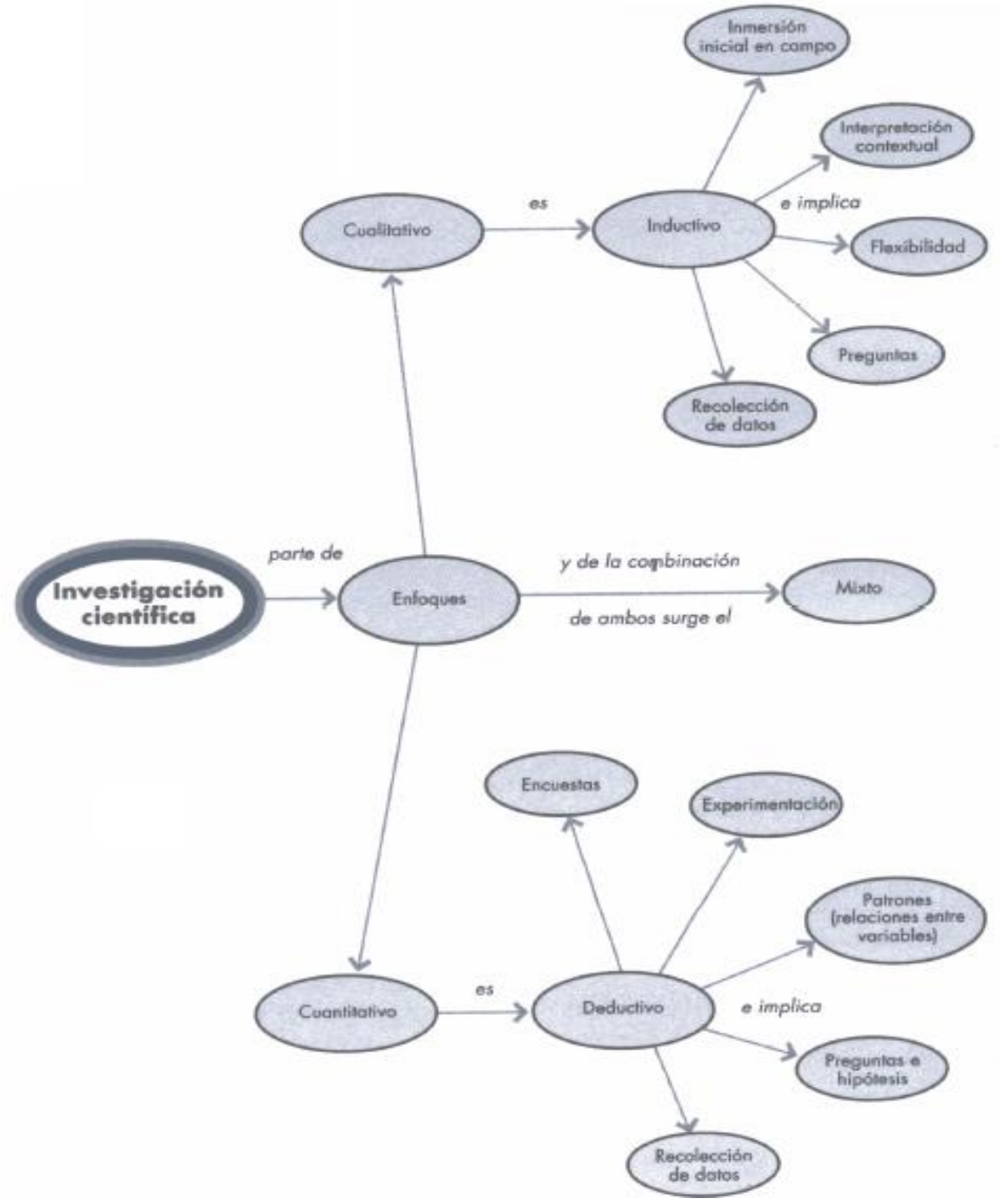
Esta recopilación de información brindará las bases para el desarrollo del diagnostico que determine la situación actual para el desarrollo del Sistema de Gestión del Manejo y seguridad de la Información que es el objetivo del presente proyecto.

Para poder dar un buen orden y garantizar la recopilación de toda la información necesaria que garantizará un buen diagnostico, es necesario realizar esta recopilación de manera metódica para evitar que dentro del desarrollo del estudio se dejen de considerar fuentes de datos o variables que puedan hacer la diferencia en una buena toma de decisiones.

A través de una investigación de diferentes métodos para la realización de investigaciones se ha optado por la aplicación de la Metodología de ***Roberto Sampieri Hernández***, esta metodología se ha seleccionado por ser de carácter universal, es decir, el conjunto de pasos que ésta describe, puede ser aplicada a cualquier tipo de investigación, permitiendo a través de esto que sea una metodología que puede ser interpretada por cualquier investigador que esté interesado en el tema, proporcionando además una guía que podrá ser aplicada a investigaciones posteriores relacionadas con el tema.

La metodología incluye una serie de pasos sistemáticos que incluyen la totalidad de los elementos dando la certeza que la investigación se desarrolle de manera ordenada y lógica permitiendo dar valides a los resultados. La metodología se describe en la sección siguiente:

2. ORIGEN DE LA METODOLOGÍA DE SAMPIERI



ESQUEMA DE LA INVESTIGACIÓN

La metodología de Sampieri define y sintetiza los enfoques cuantitativo y cualitativo de la investigación. Asimismo, presenta las etapas del proceso de investigación de manera genérica y las aplica a ambas perspectivas. Además, propone una visión respecto de la investigación que implica la posibilidad de mezclar las dos modalidades de generación de conocimientos en un mismo estudio, lo cual se denomina enfoque "multimodal" de la investigación.

a. Enfoque Cuantitativo

El enfoque cuantitativo utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento en una población.

Enfoque cuantitativo: Usa recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico para establecer patrones de comportamiento.

b. Enfoque Cualitativo

El enfoque cualitativo, por lo común, se utiliza primero para descubrir y refinar preguntas de investigación. A veces, pero no necesariamente, se prueban hipótesis (Grinnell, 1997). Con frecuencia se basa en métodos de recolección de datos sin medición numérica, como las descripciones y las observaciones. Por lo regular, las preguntas e hipótesis surgen como parte del proceso de investigación y éste es flexible, y se mueve entre los eventos y su interpretación, entre las respuestas y el desarrollo de la teoría. Su propósito consiste en "reconstruir" la realidad, tal y como la observan los actores de un sistema social previamente definido.

A menudo se llama "holístico", porque se precia de considerar el "todo", sin reducirlo al estudio de sus partes.

c. Enfoque Multimodal

Este modelo representa el más alto grado de integración o combinación entre los enfoques cualitativo y cuantitativo.

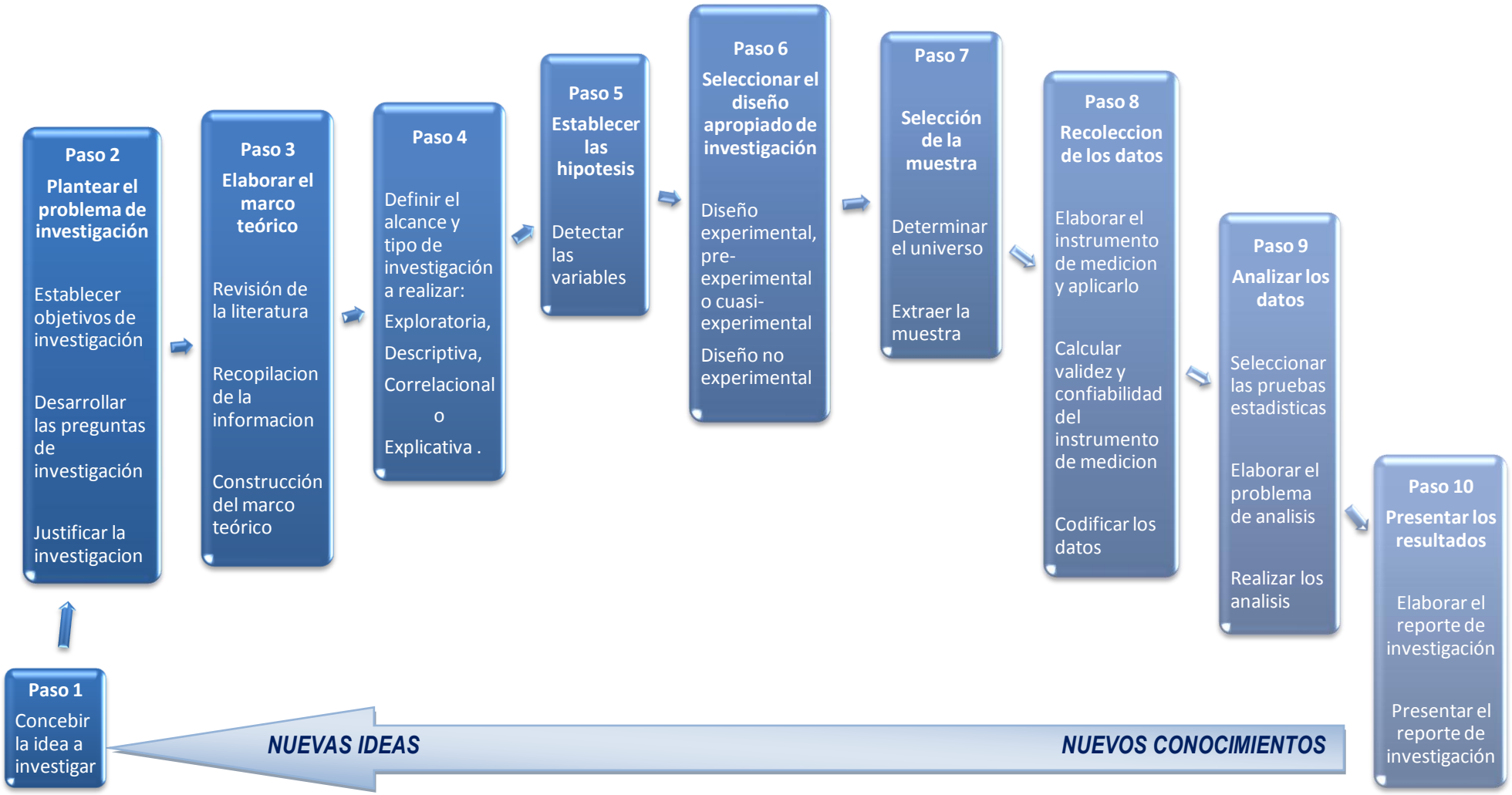
Ambos se entremezclan o combinan en todo el proceso de investigación, o al menos, en la mayoría de sus etapas. Requiere de un manejo completo de los dos enfoques y una mentalidad abierta. Agrega complejidad al diseño de estudio; pero contempla todas las ventajas de cada uno de los enfoques.

La investigación oscila entre los esquemas de pensamiento inductivo y deductivo, además de que por parte del investigador necesita un enorme dinamismo en el proceso. Lleva a un punto de vinculación lo cualitativo y lo cuantitativo

Modelo multimodal (triangulación): convergencia o fusión de los enfoques cuantitativo y cualitativo[31].

Haremos uso de la Metodología de Sampieri ya que reúne las características apropiadas y suministra los elementos necesarios que servirán de guía para la ejecución de nuestra investigación orientada a conocer el estado actual que posee la Comisión en cuanto al manejo y seguridad de la información.

[31] Ver esquema en la siguiente pagina.



Metodología de Sampieri

3. TIPOS DE INVESTIGACIÓN

Cuando se va a resolver un problema de forma científica, es muy conveniente tener un conocimiento detallado de los posibles tipos de investigación que se pueden seguir. Este conocimiento hace posible evitar equivocaciones en la elección del método adecuado para un procedimiento específico.
Conviene anotar que los tipos de investigación difícilmente se presentan puros; generalmente se combinan entre sí y obedecen sistemáticamente a la aplicación de la investigación. Tradicionalmente se presentan tres tipos de investigación. Abouhamad anota que de éstos se desprende la totalidad de la gama de estudios investigativos que trajinan los investigadores.

Tipos de investigación:

- ✓ Histórica Describe lo que era.
- ✓ Descriptiva Explica lo que es.
- ✓ Experimental Describe lo que será.

En cualquiera de los tres tipos anteriores conviene anotar que los hechos o fenómenos que estudiamos hacen relación al tiempo en que éstos se producen.
En la histórica, por ejemplo, los hechos se escapan al investigador por estar en tiempo pasado, mientras que en la descriptiva los hechos que el investigador maneja interactúan con él, y en la experimental al no existir los hechos en la realidad, el investigador debe inducirles y para ello deberá describir qué acontecerá al estos existir.

Investigación descriptiva:

Se propone este tipo de investigación describir de modo sistemático las características de una población, situación o área de interés.

Característica:

Este tipo de estudio busca únicamente describir situaciones o acontecimientos; básicamente no está interesado en comprobar explicaciones, ni en probar determinadas hipótesis, ni en hacer predicciones. Con mucha frecuencia las descripciones se hacen por encuestas (estudios por encuestas), aunque éstas también pueden servir para probar hipótesis específicas y poner a prueba explicaciones.

Ejemplos de investigaciones descriptivas son los siguientes:

- ✓ Un censo de población.
- ✓ Determinar las preferencias de los habitantes de una ciudad por ciertos programas de televisión.
- ✓ Determinar algunas características de las escuelas públicas de un país.

Etapas de la investigación descriptiva

1. Definir en términos claros y específicos qué características se desean describir.
2. Expresar cómo van a ser realizadas las observaciones; cómo los sujetos (personas, escuelas, por ejemplo) van a ser seleccionados de modo que sean muestra adecuada de la población; qué técnicas para observación van a ser utilizadas (cuestionarios, entrevistas u otras) y si se someterán a una pre-prueba antes de usarlas; cómo se entrenará a los recolectores de información.
3. Recoger los datos.
4. Informar apropiadamente los resultados.

ANEXO 7: CUESTIONARIO BASADO EN LA NORMA ISO 27 000

CUESTIONARIO SOBRE SITUACION ACTUAL DE LA SEGURIDAD DE LA INFORMACION EN LOS PROCESOS CLAVES Y DE APOYO EN CEL.

Nombre completo:_____

Unidad a la que pertenece: _____-

Fecha: _____

Objetivo: Documentar la situación actual sobre la seguridad de la información en los procesos de CEL

Indicación: Favor responder objetivamente a cada una de las preguntas siguientes:

1. ¿Qué entiende por seguridad de la Información?_____
   _____
   _____

2. ¿Existe un sistema dentro de La Comisión que busque asegurar la Información?
   Si_____ No____ si no, como se asegura:_____
   _____
3. ¿Los procesos Claves y de Apoyo se encuentran basados bajo el modelo PHVA?
   Si_____ No____ si no, en que están basado:_____
   _____
4. ¿Se cuenta con un alcance y limitaciones definidas en el manejo y seguridad de la Información?
   Si_____ No____ si no, como se delimitan:_____
   _____
5. ¿Se cuenta con políticas definidas en el manejo y seguridad de la Información?
   Si_____ No____ si no, que la rige:_____
   _____
6. ¿Existe una metodología para la evaluación de riesgos de información?
   Si_____ No____ si no, como se evalúan:_____
   _____
7. ¿Se tienen identificados y clasificados los riesgos de información, así como sus amenazas y vulnerabilidades?
   Si_____ No____ si no, como se hace:_____
   _____
8. ¿Se usan criterios para identificar y clasificar los riesgos?
   Si_____ cuales:_____
   No____ si no, bajo que los identifican y clasifican:_____
   _____
9. ¿Se ha previsto el impacto que ocasionan los riesgos de información?
   Si___ cual:_____ No___

10. ¿Se han determinado nivel de riesgo admisible?
    Si_____ cual:_____ No____
11. ¿Existen medidas a tomar ante la existencia de riesgos?
    Si_____ cuales:_____ No____
12. ¿Existe un plan de tratamiento de riesgos?
    Si_____ No____ No se tratan____
13. Si existe un plan de tratamiento de riesgos, ¿Se actualiza constantemente?
    Si_____ No____
    Cada cuanto: 1 mes____
    3 meses_____
    6 meses_____
    1 año____
    Otros intervalos_____
14. ¿Se cumplen las mejoras propuestas?
    Si_____ No____
15. ¿Qué tipo de acciones se toman?
    Preventivas:____
    Correctivas:____
    Otras:_____
16. ¿Existen controles para el tratamiento de los riesgos?
    Si_____ cuales:_____ No____
17. ¿Existen capacitación al personal en cuanto al manejo y seguridad de la información?
    Si_____ con qué frecuencia:_____ No____
18. ¿Qué recursos se destinan para el manejo y seguridad de la Información?
    Equipo____ Infraestructura____
    Tecnología____ Efectivo$$___
    Personal____ Ninguno____
    Técnicas____ Otros:____
    Capacitaciones____
19. ¿Posee un mecanismo que detecte incidentes de seguridad?
    Si_____, especifique_____
    No____
20. ¿Se ejecutan procedimientos de revisión y monitoreo dentro de las formas de manejo y seguridad de la información?
    Si_____ No____
21. ¿Se revisa la efectividad de los controles existentes?
    Si_____ con qué frecuencia:_____ No____
22. ¿Qué tipo de documentos existen en la Comisión?
    Manual de Organización _____
    Manual de puestos_____
    Manual de procedimientos_____
    Otros_____
23. ¿Cada cuánto tiempo se revisan y actualizan los documentos?

Una vez al año _____
Cada semestre _____
Cada trimestre _____
Siempre que hay un cambio _____
No los revisan _____

24. ¿Los documentos en uso se encuentran actualizados?
    Si_____ No____ Algunos(Cuantos)___ No se___
    Ultima fecha de actualización _____
25. ¿Se trabaja siempre de acuerdo a los procedimientos establecidos?
    Si_____ No____ No siempre, especifique:_____
    _____
26. ¿Los documentos están disponibles en los puntos de uso y permanecen legibles y fácilmente identificables?
    Si_____ No____ donde se encuentran:_____
    _____
27. ¿De qué manera se controlan los documentos del establecimiento?
    Hay un encargado de documentos _____
    No hay ningún control _____
    Otros _____
28. ¿La gerencia ha expresado al personal la importancia de la seguridad de la información?

Si_____ De qué forma_____

No____

29. ¿Se destinan recursos para asegurar la información?
    Si_____
    Si en forma limitada:_____
    No____
30. Si se destinan recursos, ¿Existen un adiestramiento y concientización para el uso de los mismos?
    Si_____, Cuales:_____ No____
31. ¿Los recursos destinados alcanzan a cubrir la demanda?
    Si_____ No____ ¿Porque?_____
32. ¿Se realizan auditorías internas sobre el manejo y la seguridad de la información en base a requisitos internacionales?
    Si_____ No____
    Otro tipo de auditoría:_____
    Otros: _____
33. ¿Existe un plan de auditorías establecidos?
    Si_____ No____
    ¿Se aplica debidamente? Si_____ No____
34. ¿Quién o quiénes es/son el/los responsables de efectuar las auditorias?_____
35. ¿La gerencia realiza revisiones generales en cuanto al manejo y seguridad de la Información?
    Si_____ No____
36. Si se realizan revisiones, ¿Estas se encuentran documentadas debidamente?
    Si_____ No____

37. Si se realizan, ¿Cada cuanto tiempo se realizan?
    Cada mes____
    Cada 3 meses____
    Cada 6 meses____
    Cada año____
    Otros intervalos_____
38. ¿Qué insumos se utilizan para realizar las revisiones?
    Resultados de auditorias____
    Retroalimentación de usuarios____
    Técnicas, productos o procedimientos de mejora____
    Estado de acciones preventivas y correctivas____
    Vulnerabilidades o amenazas latentes____
    Resultados de mediciones de controles____
    Otros especifique_____
39. ¿Qué tipo de resultados arroja las revisiones?
    Mejora la eficacia____
    Actualización del plan de tratamiento de riesgos____
    Modificación de procedimientos y controles____
    Necesidades de recursos____
    Otros especifique_____
40. ¿Existe un mecanismo establecido por la Comisión que mejore continuamente el manejo y seguridad de la información?
    Si_____ cual:_____ No____

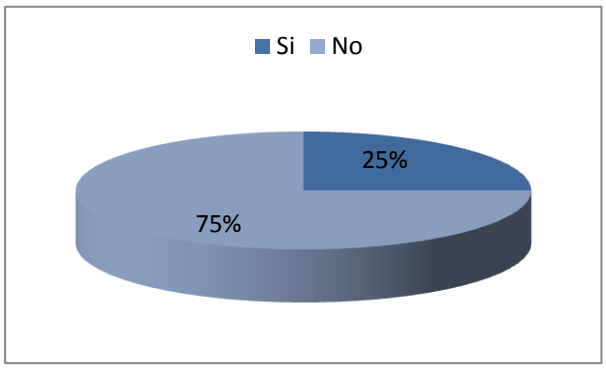
41. Ante un fallo de seguridad ¿Se toman medida o acciones correctivas para eliminar el fallo?
    Si_____ cuales:_____ No____
42. ¿Se toman acciones o medidas preventivas ante fallos de seguridad potenciales?
    Si_____ cuales:_____ No____

ANEXO 8: TABULACIÓN DE DATOS DE ENCUESTA PARA LA UNIDAD DE PRODUCCIÓN

2. ¿Existe un sistema dentro de la Comisión que busque asegurar la información?

R/

Si	No
1	3



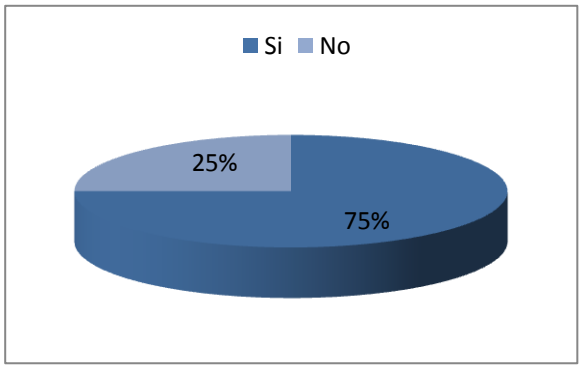
Si no, ¿Cómo se asegura?:

Normativas de archivo institucional (No es un documento específico, sino las buenas prácticas de archivo institucional)

3. ¿Los procesos Claves y de Apoyo se encuentran basados bajo el modelo Planeación, Ejecución, Revisar y Mejorar?

R/

Si	No
3	1

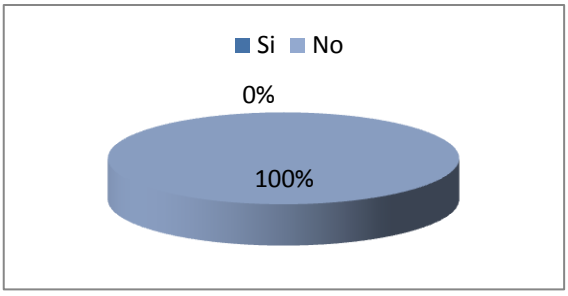


Si no, en que están basados: Desconozco

4. ¿Se cuenta con un alcance y limitaciones definidas en el manejo y seguridad de la información?

R/

Si	No
0	4



Si no, como se delimita:

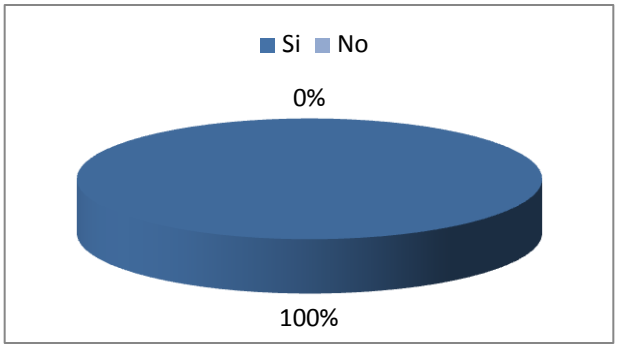
No como documento explicito.

En las normativas de archivo institucional cada Unidad la establece al momento de la definición de la guía de archivo; y para documentos contables y otros confidenciales, hay reglas más específicas para dar seguridad a la información (comprobantes contables, expediente trabajadores, fianzas, contratos originales, escrituras de propiedad, etc.)

5. ¿Se cuenta con políticas definidas en el manejo y seguridad de la información?

R/

Si	No
4	0

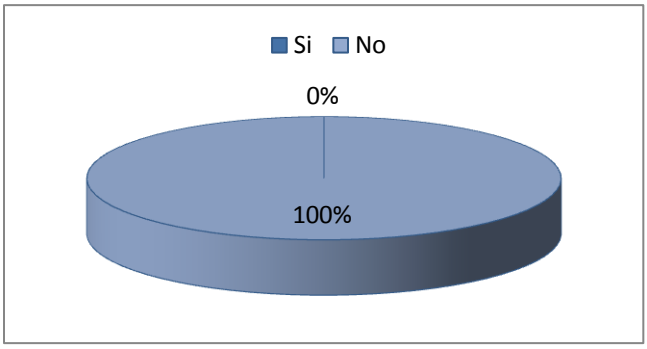


Comentario: Son políticas de verbales de cada jefatura.

6. ¿Existe una metodología para la evaluación de riesgos de la información?

R/

Si	No
0	4



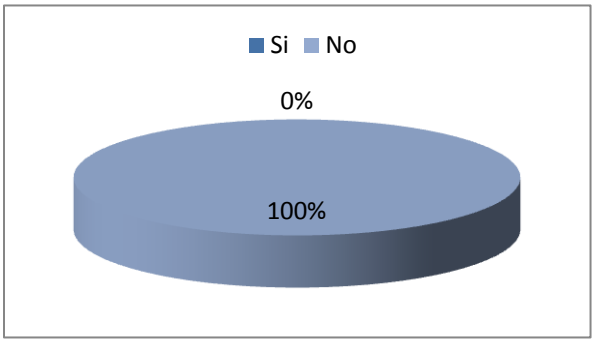
Si no, como los evalúan:

Cada unidad en su ámbito de aplicación, evalúa el riesgo de una pérdida o daño de información. Para el caso del proceso de producción, los registros de calidad (RC derivados de la ejecución de su proceso), su riesgo de pérdida es mínimo.

7. ¿Se tienen identificados y clasificados los riesgos de información, así como sus amenazas y vulnerabilidades?

R/

Si	No
0	4



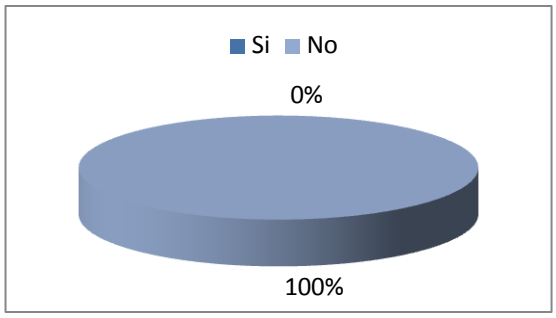
Si no ¿Como se hace?

Solamente para el archivo físico de los RC-Producción, se resguardan de la amenaza de incendio, inundación, terremoto, vandalismo (hurto).

8. ¿Se usan criterios para identificar y clasificar los riesgos?

R/

Si	No
0	4



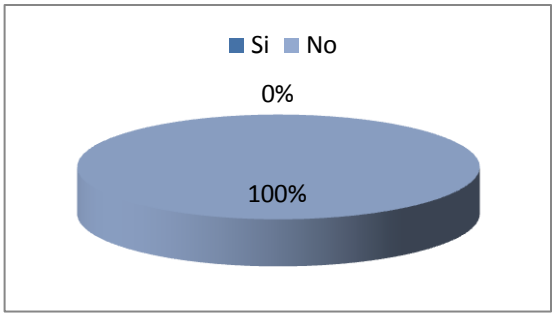
Si no, ¿bajo qué los identifica y clasifica?

Incendio, inundación, terremoto, vandalismo.

9. ¿Se ha previsto el impacto que ocasionan los riesgos de la información?

R/

Si	No
0	4

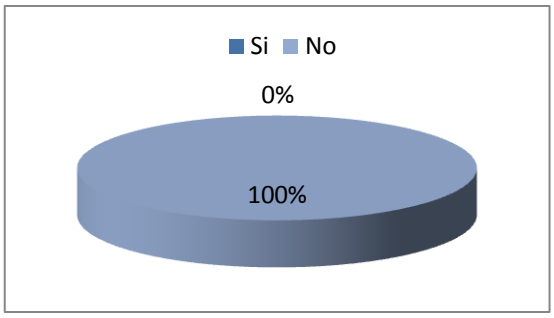


Comentario: No formalmente.

10. ¿Se ha determinado un nivel de riesgo admisible?

R/

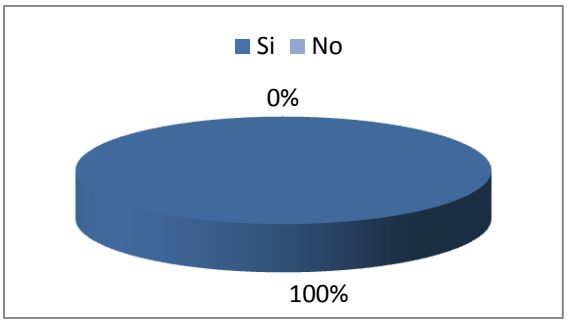
Si	No
0	4



11. ¿Existen medidas a tomar ante la existencia de riesgos?

R/

Si	No
4	0

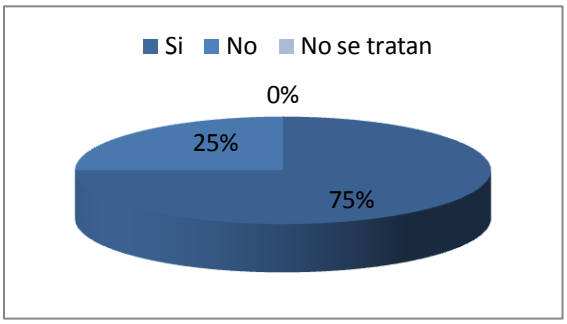


Cuales: Resguardo de los RC-Producción en muebles de archivo anti-llamas y la digitalización de documentos después de un periodo, según se establece en el SG Calidad.

12. ¿Existe un plan de tratamiento de riesgos?

R/

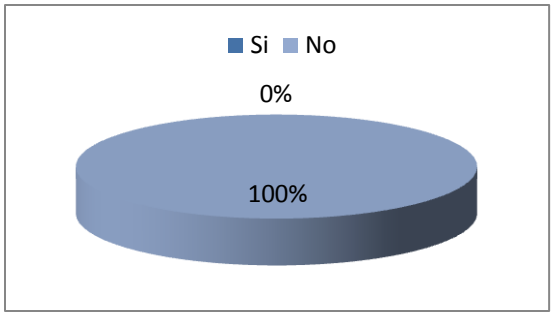
Si	No	No se tratan
3	1	0



13. Si existe un plan de tratamiento de riesgos, ¿se actualiza constantemente?

R/

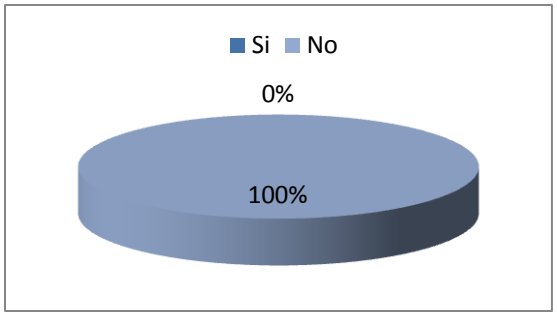
Si	No
0	4



14. ¿Se cumplen las mejoras propuestas al plan?

R/

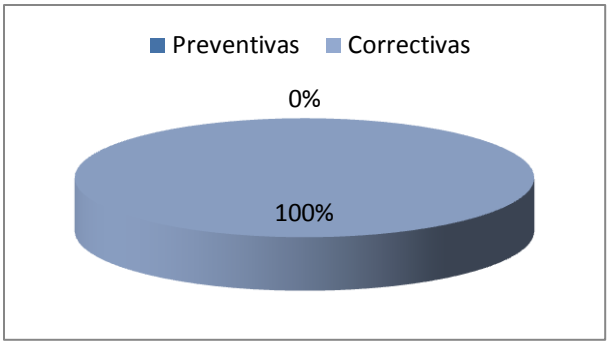
Si	No
0	4



15. ¿Qué tipo de acciones se toman?

R/

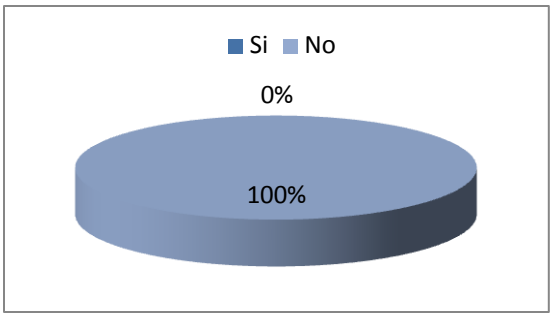
¿Qué tipo de acciones?	
Preventivas	0
Correctivas	4
Otras	0



16. ¿Existen controles para el tratamiento de los riesgos?

R/

Si	No
0	4

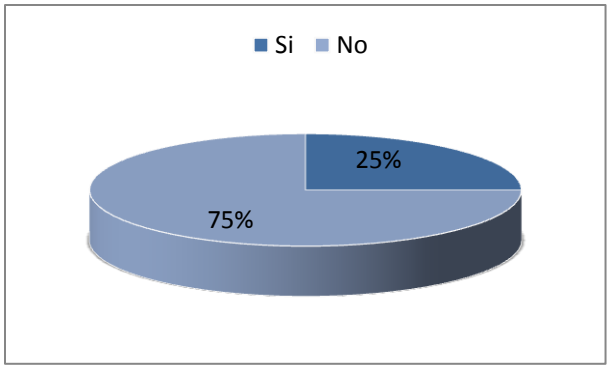


Si no, ¿cómo se controlan? Principalmente la prevención de incentivos y vigilancia de las instalaciones donde se resguardan los documentos para protección por vandalismo (hurto).

17. ¿Existe capacitación al personal en cuanto al manejo y seguridad de la información?

R/

Si	No
1	3

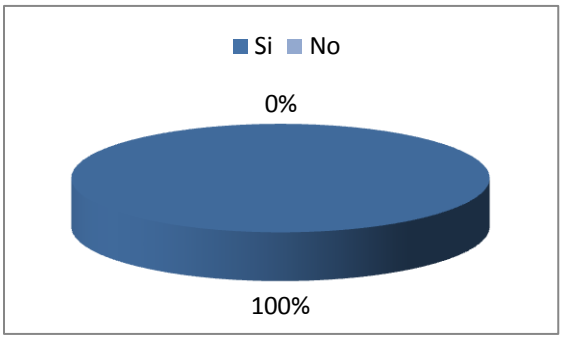


Comentario: Es sentido común.

18. ¿Posee un mecanismo que detecte incidentes de seguridad de la información?

R/

Si	No
4	0

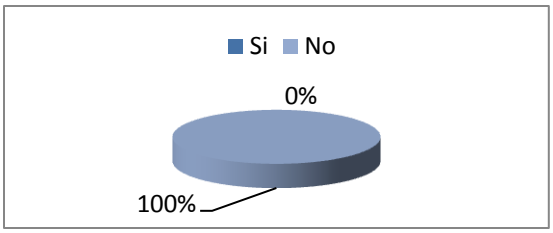


Si, especifique: Hasta cuando se da el incidente de pérdida de información por incendio, inundación, terremoto, vandalismo. Al momento no ha ocurrido en la Gerencia de Producción.

19. ¿Se ejecutan procedimientos de revisión y monitoreo dentro de las formas de manejo y seguridad de la información?

R/

Si	No
0	4

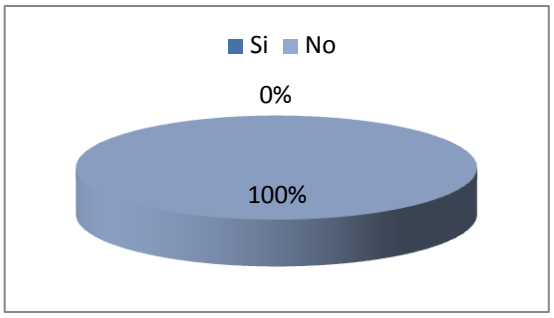


Comentario: Los RC-Producción no son documentos clasificados como confidenciales

20. ¿Se revisa la efectividad de los controles existentes?

R/

Si	No
0	4



21. ¿Qué tipo de documentos existen en la comisión?

R/ RC derivados del proceso de producción (Operación, mantenimiento, Gestión Ambiental PRL)

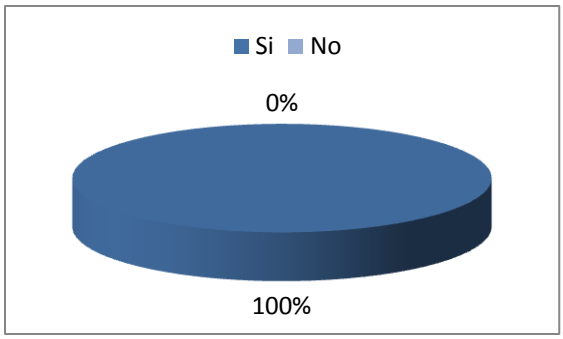
22. ¿Cada cuánto tiempo se revisan y actualizan los documentos?

Descripción	Frecuencia
Una vez al año	0
Cada semestre	0
Cada trimestre	0
Siempre que hay un cambio	0
No los revisan	4

23. ¿Los documentos en uso se encuentran actualizados?

R/

Si	No
4	0



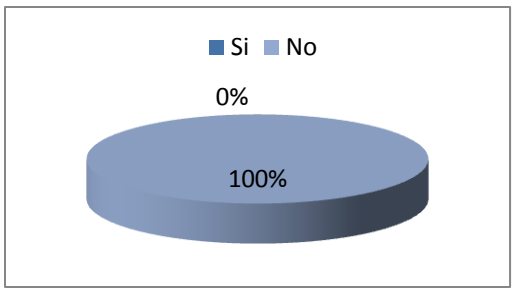
Comentario: Última fecha de actualización fechas diversas ya que son los procedimientos de gestión integrada, que dan origen a los RC.

La unidad de gestión Integrada tiene el control de las fechas de revisión y actualización.

24. ¿Se trabaja de acuerdo a los procedimientos establecidos?

R/

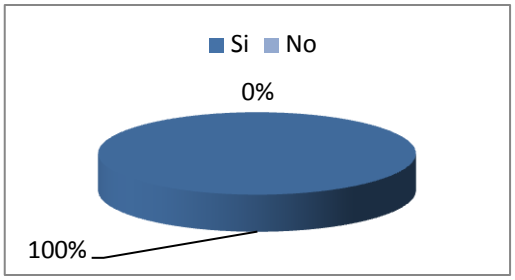
Si	No
0	4



25. ¿Los documentos están disponibles en los puntos de uso y permanecen legibles y fácilmente identificables?

R/

Si	No
4	0



26. ¿De qué manera se controlan los documentos del establecimiento?

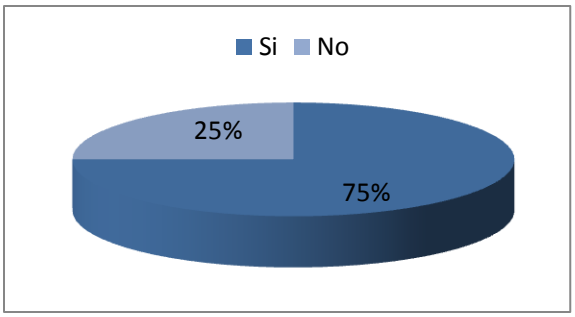
R/

Control de Documentos	
Hay un encargado de documentos	4
No hay ningún control	0
Otros	0

27. ¿La gerencia ha expresado al personal la importancia de la seguridad de la información?

R/

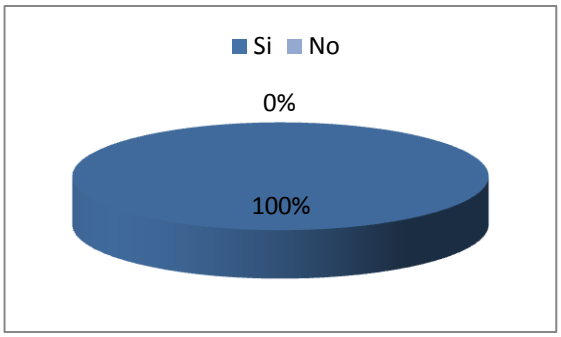
Si	No
3	1



28. ¿Se destinan recursos para asegurar la información?

R/

Si	No
4	0



Cometario: Se destinan recursos en forma limitada.

29. ¿Qué recursos se destinan para el manejo y seguridad de la información?

¿Qué recursos?	
Equipo	0
Tecnología	0
Personal	0
Técnicas	0
Capacitaciones	0
Infraestructura	0
Efectivo	0

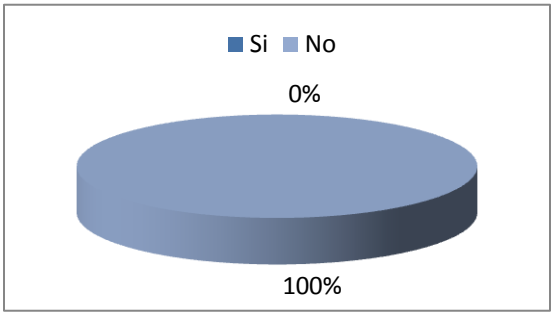
Ninguno	0
Otros	4

Otros: Mobiliario que contiene los RC-Produccion.

30. ¿Si se destinan los recursos, existe un adiestramiento y concientización para el uso de los mismos?

R/

Si	No
0	4

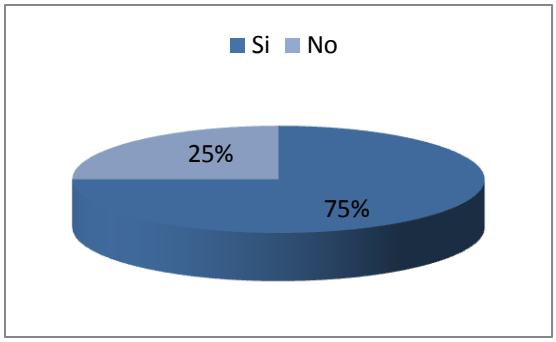


Comentario: La preservación de documentos de archivo y posterior digitalización no requiere un mayor adiestramiento y concientización del personal que genera la información de los RC-Producción no es clasificada confidencial, por materialidad no se hacen más gastos en adiestramiento.

31. ¿Los recursos destinados no alcanzan a cubrir la demanda?

R/

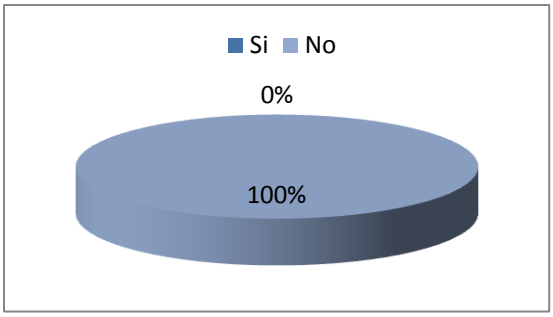
Si	No
3	1



32. ¿Se realizan auditorías internas sobre el manejo y la seguridad de la información en base a requisitos internacionales?

R/

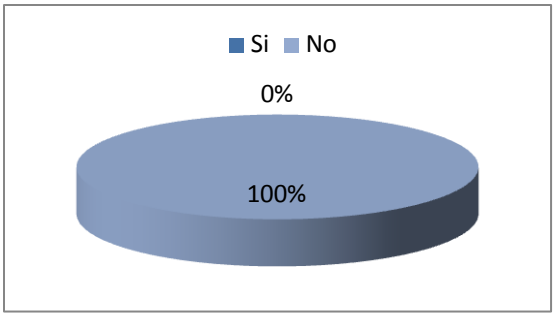
Si	No
0	4



33. ¿Existe un plan de auditorías establecido?

R/

Si	No
0	4



¿Se aplican debidamente?

Si	No
0	4

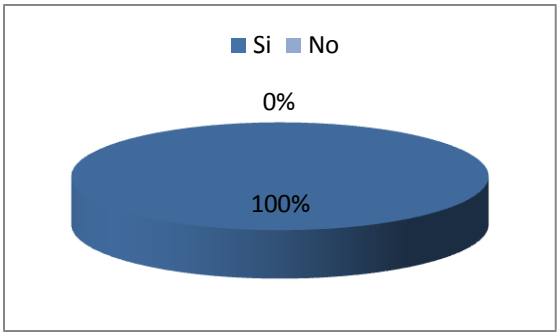
34. ¿Quién o quienes es/son él/los responsables de efectuar las auditorias?

R/ No existe

35. ¿La gerencia realiza revisiones generales en cuanto al manejo y seguridad de la información?

R/

Si	No
4	0



Comentario: Como parte de las gestiones itinerantes y de manera general.

36. Si se realizan ¿Cada cuánto tiempo se realizan?

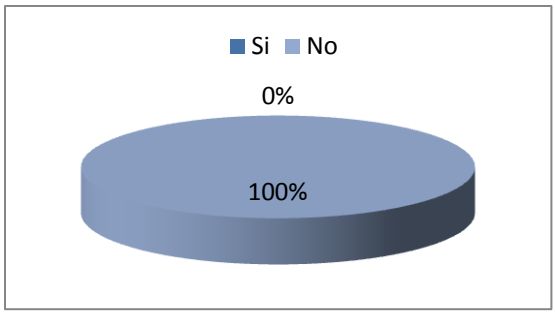
R/

¿Cada cuánto?	
Cada mes	4
Cada 3 meses	0
Cada 6 meses	0
Anualmente	0
Otros intervalos	0
No respondió	0

37. Si se realizan revisiones ¿Estas se encuentran documentadas debidamente?

R/

Si	No
0	4



38. ¿Qué insumos se utilizan para realizar las revisiones?

Insumos	
Resultados de auditorias	0
Retroalimentación de usuarios	3
Técnicas, productos o procedimientos de mejora	0
Estado de acciones correctivas y preventivas	0
Vulnerabilidades o amenazas latentes	3
Resultados de medición de controles	0
Otros	0
No respondió	2

Observación durante recorridos de gestión itinerante.

39. ¿Qué tipo de resultados arrojan las revisiones?

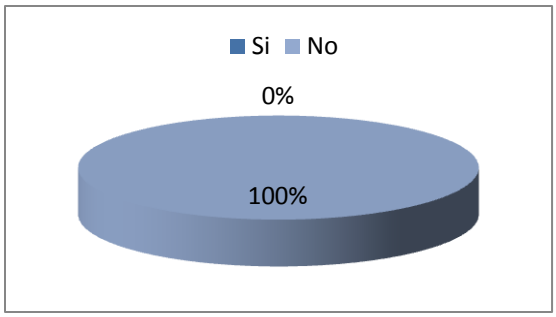
R/

Resultados	
Mejora la eficacia	0
Actualización del plan de tratamiento de riesgos	0
Modificación de procedimientos y controles	0
Necesidades de recursos	4
Otros	0
No respondió	0

40. ¿Existe un mecanismo establecido por la Comisión que mejore continuamente el manejo y seguridad de la información?

R/

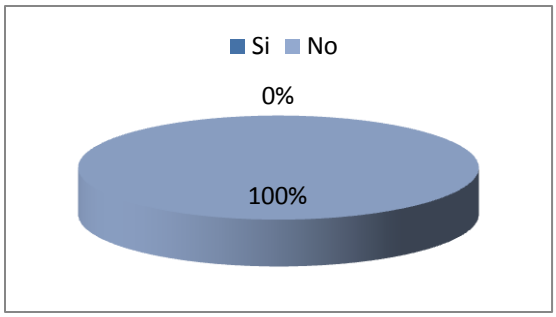
Si	No
0	4



41. Ante un fallo de seguridad ¿se toman medidas o acciones correctivas para eliminar el fallo?

R/

Si	No
0	4

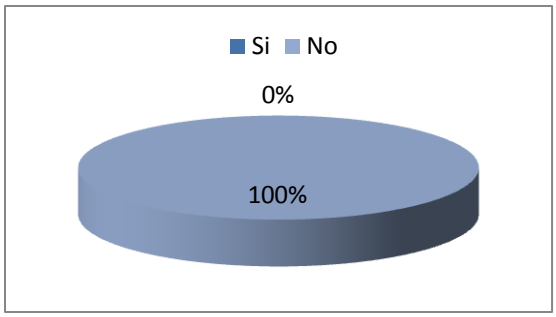


Comentario; RC-Producción no tienen riesgo alto.

42. ¿Se toman acciones o medidas preventivas ante fallos de seguridad potenciales?

R/

Si	No
0	4



Comentario; RC-Producción no tienen riesgo alto.

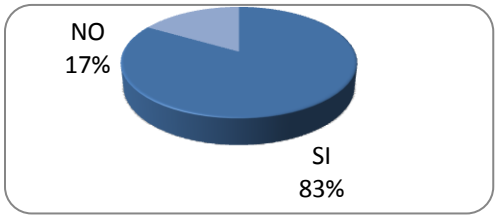
ANEXO 9: TABULACIÓN DE DATOS DE ENCUESTA PARA LA UNIDAD DE COMERCIALIZACIÓN

1. ¿Existe un sistema dentro de La Comisión que busque asegurar la Información?

   Si_____ No____, si no, Como se asegura:

RESPUESTA	FRECUENCIA	%
SI	5	83
NO	1	17
TOTAL	6	100

ANÁLISIS



Solamente una de las 6 personas externo que no se posee un Sistema que busque asegurar la información y que solo se poseen normas internas de control, las formas de asegurar la información es también por la experiencia de los usuarios/ productores de información.

Por el contrario las otras 5 personas aseguran que existe un sistema de seguridad pero al ver sus reflexiones nos damos cuenta que no es un sistema como tal, ellos aseguran poseer contraseñas de seguridad, actualizaciones de virus, prohibiciones de páginas web, regulaciones en la intranet, etc.

Por lo que al analizar los datos se puede concluir que no se posee con un Sistema de seguridad, solamente con algunos componentes.

2. ¿Los procesos Claves y de Apoyo se encuentran basados bajo el modelo Planeación, Ejecución, Revisar y Mejorar?

   Si: ____ No: ____

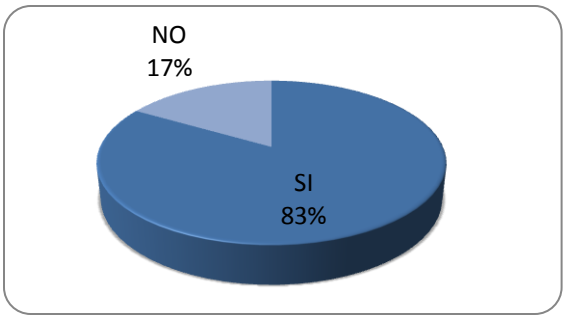
RESPUESTA	FRECUENCIA	%
SI	6	100
NO	0	0.00
DESCONOCE	0	0.00
TOTAL	6	100

ANÁLISIS El 100 **%** asegura contar con un modelo PERM, Contar con un modelo de esa manera facilitara en un futuro poder desarrollar un SGSI ya que trabaja sobre ese mismo enfoque.

3. ¿Se cuenta con un alcance y limitaciones definidas en el manejo y seguridad de la Información?

   Si_____ No____, si no, como se delimita.

RESPUESTA	FRECUENCIA	%
SI	5	83
NO	1	17
TOTAL	6	100



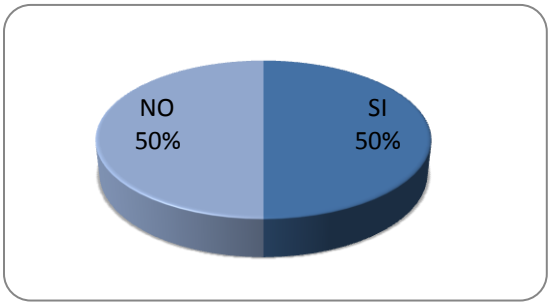
ANÁLISIS

EL 83 **%** asegura poseer un alcance y limitaciones en el manejo y seguridad de la información. El 17% dice que no, y se delimita por medio de claves de acceso y resguardo físico de documentos y por un reglamento institucional que define la responsabilidad de cada usuario de realizar respaldos, y de no sacar información de la institución.

4. ¿Se cuenta con políticas definidas en el manejo y seguridad de la Información?

   Si_____ No____, si no, que la rige:

RESPUESTA	FRECUENCIA	%
SI	3	50
NO	3	50
DESCONOCE	0	0.00
TOTAL	6	100

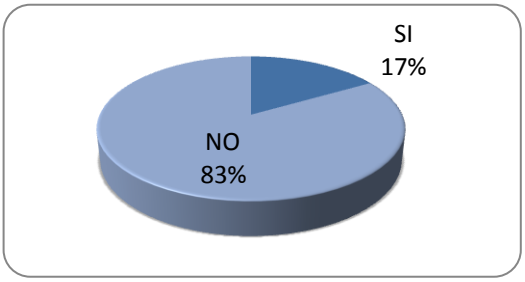


La mitad del personal asegura que existen políticas de aseguramiento de la información. El restante afirma que solo cuentan con conocimientos empíricos sobre su aseguramiento debido a la experiencia de uso y a la importancia de la misma. Por otra parte aseguran poseer políticas con confidencialidad pero que no se encuentran plasmadas en algún documento.

5. ¿Existe una metodología para la evaluación de riesgos de información?

   Si_____ No____, si no, como los evalúan:

RESPUESTA	FRECUENCIA	%
SI	1	17
NO	5	83
DESCONOCE	0	0.00
TOTAL	6	100.00

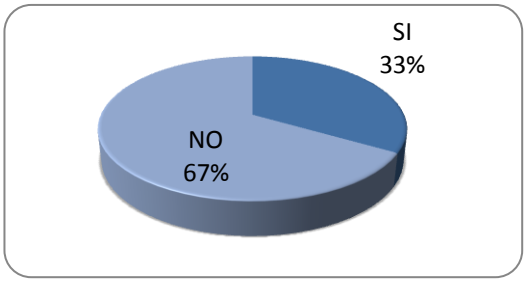


El 17% opina que existe una metodología para evaluación de riesgos de información, por el contrario el 83% manifiesta que no se tiene definida. Eso debido a que no se ha identificado las medidas concretas a tomar y cuáles son los riesgos presentes. Todo es de manera empírica y las medidas se toman cuando se presentan los riesgos y sus consecuencias.

6. ¿Se tienen identificados y clasificados los riesgos de información, así como sus amenazas y vulnerabilidades?

   Si_____ No____, si no, Como se hace:

RESPUESTA	FRECUENCIA	%
SI	2	33.33
NO	4	66.67
DESCONOCE	0	0.00
TOTAL	6	100.00

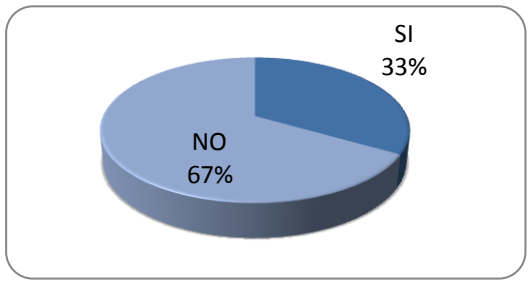


El 33.33 % afirma poseer identificados y clasificados los riesgos de información así como sus amenazas y vulnerabilidades, por el contrario el 66.67% afirma no poseerlos, ellos a la vez dijeron que la forma actual de como se hace es que solamente conocen las vulnerabilidades y la importancia de la información pero nada de manera formal y documentado.

7. ¿Se usan criterios para identificar y clasificar los riesgos?

   Si_____, Cuales: _____ No____, si no, bajo que los identifica y clasifica: _____

RESPUESTA	FRECUENCIA	%
SI	2	33.33
NO	4	66.67
DESCONOCE	0	0.00
TOTAL	6	100.00



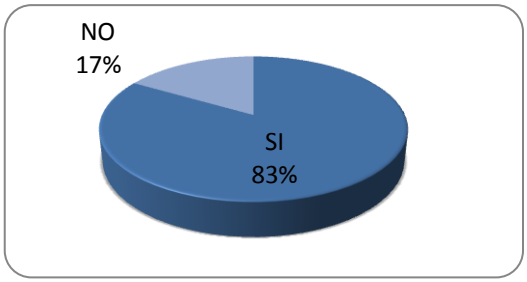
El 33% afirma poseer criterios entre los cuales están: criterios de oportunidad

El 67% afirma no posee criterios y eso debido a que actualmente a información se basa en el tipo e importancia de la misma, o en el peor de los casos cuando suceden los riesgos.

8. ¿Se ha previsto el impacto que ocasionan los riesgos de información?

Si_____, Cuales: _____ No____

RESPUESTA	FRECUENCIA	%
SI	5	83%
NO	1	17%
DESCONOCE	0	0%
TOTAL	6	100%

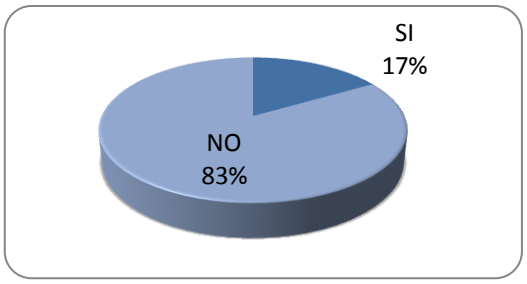


El 83% asegura haber previsto los impactos pero al indagar en cuales solo se han previsto pérdidas económicas y no son las únicas que se deberían de proveer. El 17% asegura no tener previsto los impactos. No se tienen back up de archivos y un fallo ocasionaría perdidas de información sin posibilidad de recuperarla, la unidad no cuenta con un respaldo automático, el cual es manual y no está regulado.

9. ¿Se han determinado nivel de riesgo admisible?

Si_____, Cuales: _____ No____

RESPUESTA	FRECUENCIA	%
SI	1	17%
NO	5	83%
DESCONOCE	0	0%
TOTAL	6	100%

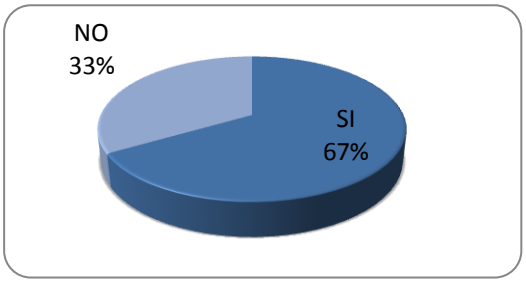


Solamente el 17% asegura tener determinado un nivel de riesgo admisible, dicha aseguración es atribulada solamente a riesgos por virus informáticos lo cual se queda corto y no es del todo confiable. El restante 38% expone no poseer nada sobre eso.

10. ¿Existen medidas a tomar ante la existencia de riesgos?

Si_____, Cuales: _____ No____

RESPUESTA	FRECUENCIA	%
SI	4	67%
NO	2	33%
DESCONOCE	0	0%
TOTAL	6	100%



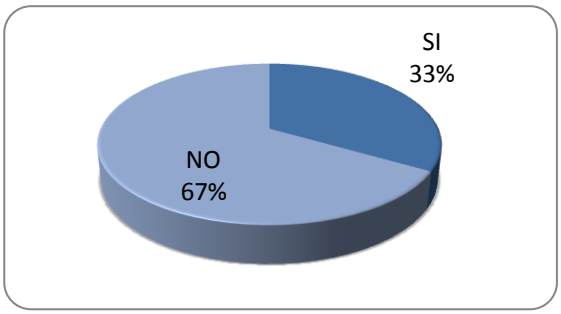
El 67% afirma tener medidas a tomar en el caso de la existencia de riesgos entre ellas están: aseguramientos de elaboración de ofertas, y un proceso contingencia pero ese solo se limita a riesgos al hardware y servicios y no contempla el de carácter humano. Por el contrario el 33% asegura no tener medidas.

11. ¿Existe un plan de tratamiento de riesgos?

Si_____ No____ No se tratan: _____

Si su respuesta es No, pase a la pregunta 17.-

RESPUESTA	FRECUENCIA	%
SI	2	33%
NO	4	67%
DESCONOCE	0	0%
TOTAL	6	100%



Del 100% el 33% asegura poseer un plan de tratamiento de riesgos, y el 67% asegura no poseer y que no se tratan en la actualidad.

12. Si existe un plan de tratamiento de riesgos, ¿Se actualiza constantemente?

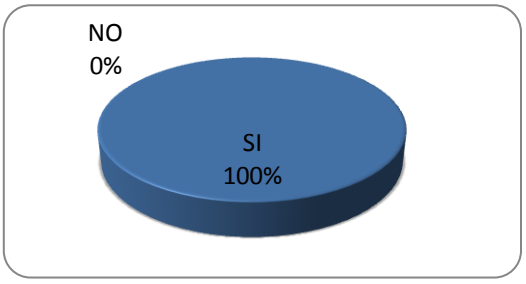
Si_____ No____

Cada cuanto: 1 mes____ 6 meses_____

3 meses_____ 1 año____

Otros intervalos_____

RESPUESTA	FRECUENCIA	%
SI	2	100%
NO	0	0%
DESCONOCE	0	0%
TOTAL	2	100%

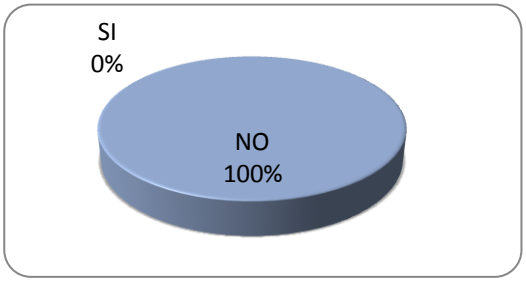


Dicho plan por tratarse de un proceso contingencia se actualiza anualmente o cuando ocurren cambios sustanciales por tratarse de un plan de mejora continúa.

13. ¿Se cumplen las mejoras propuestas al plan?

Si_____ No____

RESPUESTA	FRECUENCIA	%
SI	0	0%
NO	2	100%
DESCONOCE	0	0%
TOTAL	2	100%



Por tratarse de un procedimiento este no incorpora mejoras propuestas.

14. ¿Qué tipo de acciones se toman?

Preventivas: ____
Correctivas: ____
Otras: _____

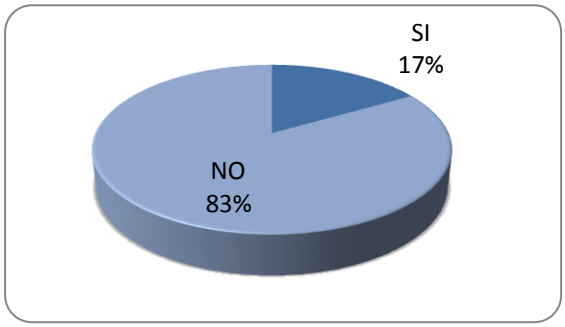
Dicha pregunta no obtuvo respuestas por lo que la pregunta anterior expuso que no se tenían acciones a tomar.

15. ¿Existen controles para el tratamiento de los riesgos?

Si_____, Cuales: ____

No____, si no, como se controlan: _____

RESPUESTA	FRECUENCIA	%
SI	1	17%
NO	5	83%
DESCONOCE	0	0%
TOTAL	6	100%

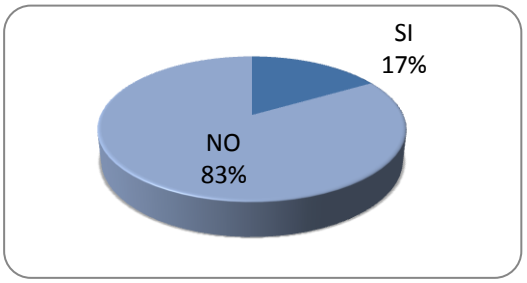


Solamente el 17% asegura poseer controles y entre ellos están verificaciones de la data en cuanto a su acceso y disponibilidad.

16. ¿Existe capacitación al personal en cuanto al manejo y seguridad de la información?

Si____ Con qué frecuencia: _____ No___

RESPUESTA	FRECUENCIA	%
SI	1	17%
NO	5	83%
DESCONOCE	0	0%
TOTAL	6	100%



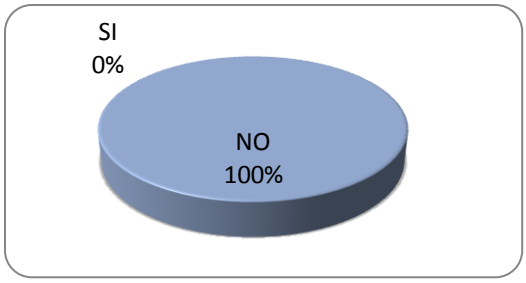
Solamente el 17% asegura recibir capacitaciones cada 6 meses, por el contrario el 83% asegura no poseer capacitaciones en dicho campo.

17. ¿Posee un mecanismo que detecte incidentes de seguridad de la información?

Si_____, especifique_____

No____

RESPUESTA	FRECUENCIA	%
SI	0	0%
NO	6	100%
DESCONOCE	0	0%
TOTAL	6	100%



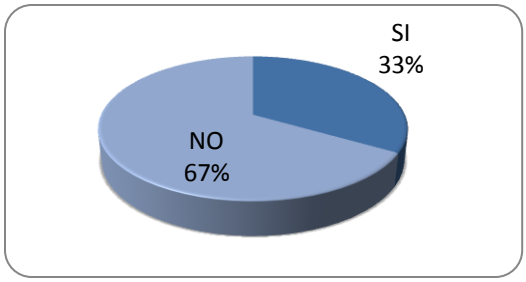
El 100% asegura no poseer mecanismos que detecten incidentes de la seguridad de la información, uno de ellos expuso que los errores se detectan en el día que ocurren.

18. ¿Se ejecutan procedimientos de revisión y monitoreo dentro de las formas de manejo y seguridad de la información?

Si_____, Con qué frecuencia: _____

No____

RESPUESTA	FRECUENCIA	%
SI	2	33%
NO	4	67%
DESCONOCE	0	0%
TOTAL	6	100%



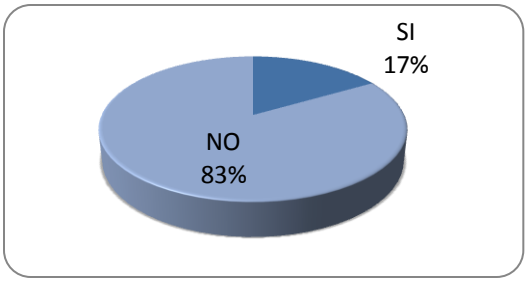
Solamente un 33% asegura haber procedimientos de revisión y monitoreo pero al profundizar y preguntar cómo se hacían se observo que no son procedimientos definidos y solo se hace de manera empírica, ellos lo hacen a diario cuando se actualizan las variables del mercado dentro del sistema. El 67% asegura no poseer revisiones y monitoreos de la misma.

19. ¿Se revisa la efectividad de los controles existentes?

Si_____, Cada cuanto: _____

No____

RESPUESTA	FRECUENCIA	%
SI	1	17%
NO	5	83%
DESCONOCE	0	0%
TOTAL	6	100%



El 17% afirma que la efectividad de los controles se revisa y la frecuencia es diaria, el restante 83% no se revisa la efectividad, esto debido a que los controles son mínimos y no se tienen documentados.

20. ¿Qué tipo de documentos existen en la Comisión?

Manual de Organización _____

Manual de puestos_____

Manual de procedimientos_____

Otros_____

El 100% de los encuestados afirmo poseer los siguientes documentos

Manual de organización

Manual de puestos

Manual de procedimientos

Reglamento interno

Manual de Gestión Integrada

21. ¿Cada cuánto tiempo se revisan y actualizan los documentos?

Una vez al año _____

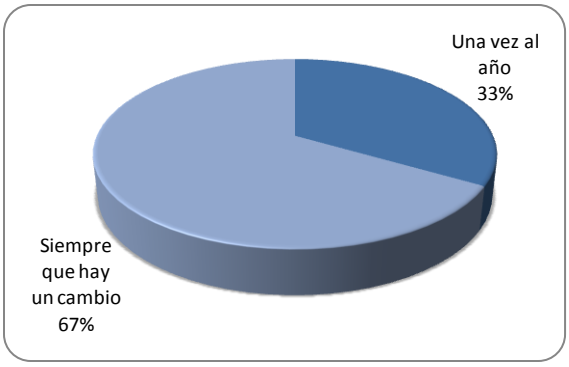
Cada semestre _____

Cada trimestre _____

Siempre que hay un cambio _____

No los revisan _____

RESPUESTA	FRECUENCIA	%
Una vez al año	2	33%
Siempre que hay un cambio	4	67%
DESCONOCE	0	0%
TOTAL	6	100%



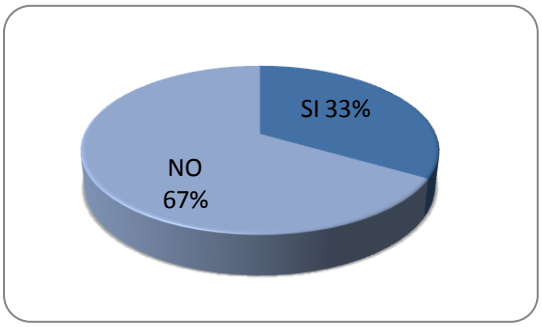
El 33% asegura que los documentos se revisan y actualizan anualmente y el 67% afirma que se revisan siempre que hay un cambio esto debido a la mejora continua de los procesos y/o documentos.

22. ¿Los documentos en uso se encuentran actualizados?

Si_____ No____ Algunos (cuantos):_____No se_____

Ultima fecha de actualización _____

RESPUESTA	FRECUENCIA	%
SI	2	33%
NO	4	67%
DESCONOCE	0	0%
TOTAL	6	100%

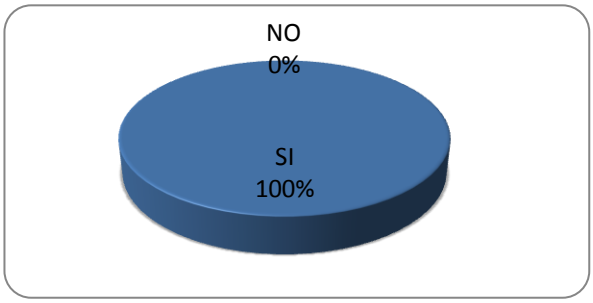


El 33% expreso que los documentos se encuentran actualizados y su fecha de su ultima actualización es el dic/2005, el 67% asegura que no todos están actualizados solamente un 70% de ellos lo están.

23. ¿Se trabaja siempre de acuerdo a los procedimientos establecidos?

Si_____ No____ No siempre, especifique: _____

RESPUESTA	FRECUENCIA	%
SI	6	100%
NO	0	0%
DESCONOCE	0	0%
TOTAL	6	100%

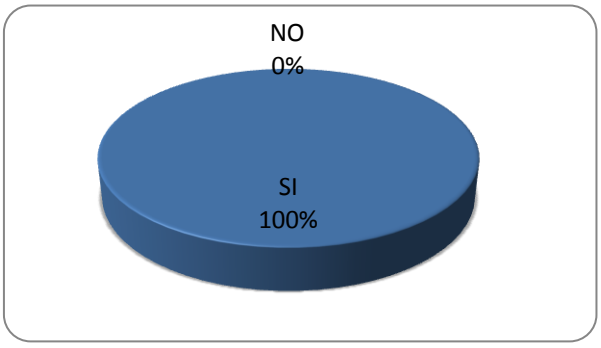


El 100% afirmo que efectivamente las tareas se realizan de acuerdo a los procedimientos establecidos y que por el sistema de calidad continuamente están actualizándolos.

24. ¿Los documentos están disponibles en los puntos de uso y permanecen legibles y fácilmente identificables?

Si_____ No____, Donde se encuentran: _____

RESPUESTA	FRECUENCIA	%
SI	6	100%
NO	0	0%
DESCONOCE	0	0%
TOTAL	6	100%



El 100% asegura que los documentos están disponibles en los puntos de uso y permanecen legibles y fácilmente identificables.

El lugar donde los resguardan o los encuentran es en la intranet y en el archivo general de la Unidad que lo maneja la secretaria.

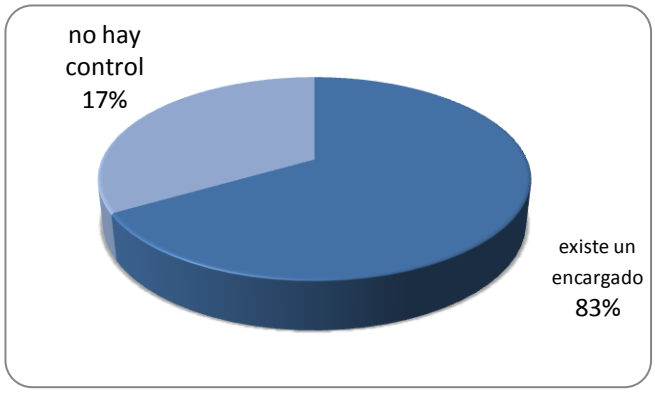
25. ¿De qué manera se controlan los documentos del establecimiento?

Hay un encargado de documentos _____

No hay ningún control _____

Otros _____

RESPUESTA	FRECUENCIA	%
EXISTE UN ENCARGADO	5	83%
NO HAY CONTROL	1	17%
DESCONOCE	0	0%
TOTAL	6	100%



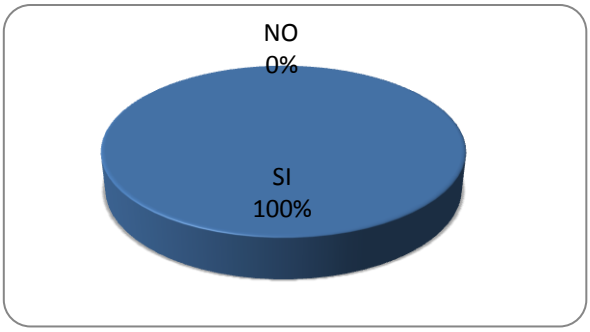
El 83% asegura que existen controles y que existe un encargado para ello, el cual todos afirmaron que la secretaria es la responsable y que existe una hoja de distribución de documentos para uso interno.

Solamente un 17% afirmo que no hay control de dichos documentos.

26. ¿La gerencia ha expresado al personal la importancia de la seguridad de la información?

Si_____ De qué forma_____ No____

RESPUESTA	FRECUENCIA	%
SI	6	100%
NO	0	0%
DESCONOCE	0	0%
TOTAL	6	100%

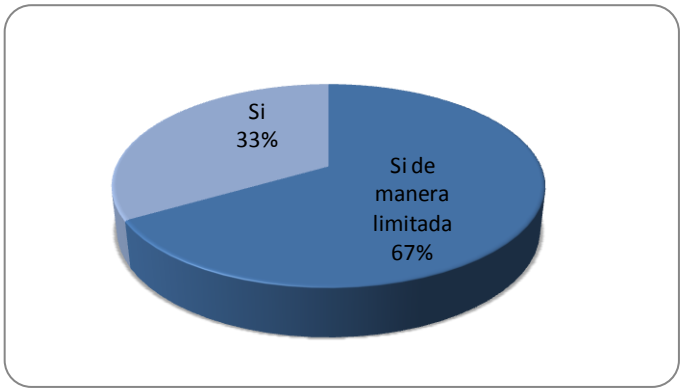


El 100% ha manifestado que la gerencia se ha involucrado y les ha expresado tanto de manera verbal como por medio de correos electrónicos la importancia de la seguridad de la información, también por medio de reuniones.

27. ¿Se destinan recursos para asegurar la información?

Si_____ Si en forma limitada: _____ No____

RESPUESTA	FRECUENCIA	%
SI	2	33%
Si de forma limitada	4	67%
DESCONOCE	0	0%
TOTAL	6	100%

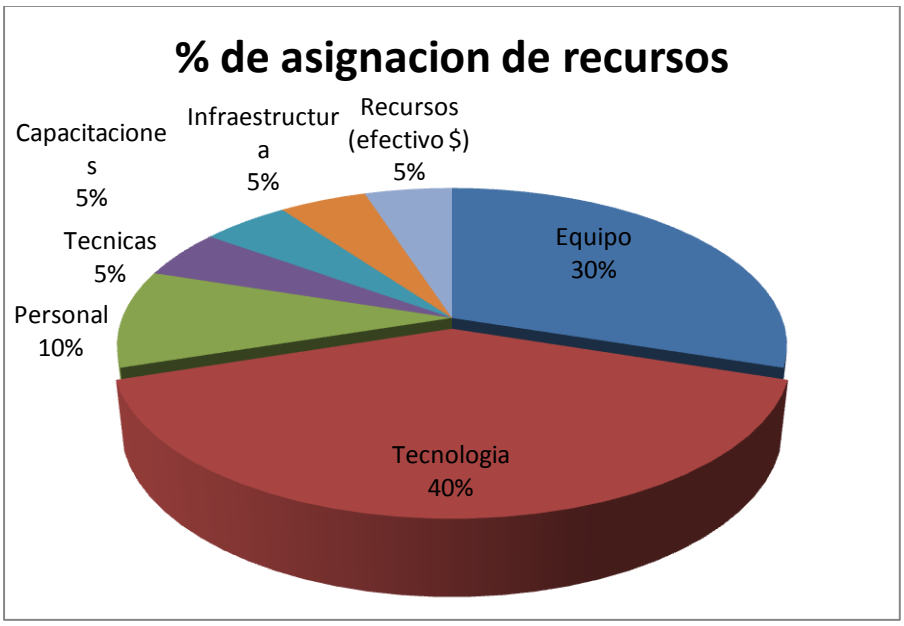


Del 100% el 67% afirma que si se destinan recursos pero de hace limitadamente, y el resto dice que si se hace.

28. ¿Qué recursos se destinan para el manejo y seguridad de la Información?

Equipo____ Capacitaciones____
Tecnología____ Infraestructura____
Personal____ Efectivo$$___
Técnicas____ Ninguno____
Otros:_____

RECURSOS	% DE ASIGNACIÓN
Equipo	30%
Tecnología	40%
Personal	10%
Técnicas	5%
Capacitaciones	5%
Infraestructura	5%
Recursos (efectivo $)	5%

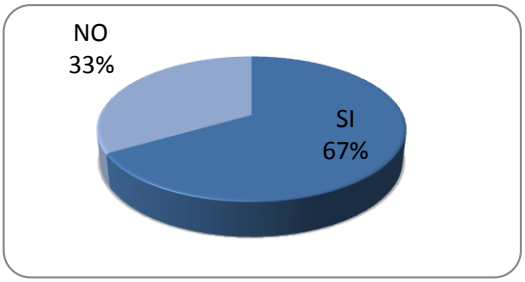


De acuerdo a porcentajes el recurso que más se invierte en asegurar la información es el tecnológico con un 40%, luego el equipo con un 30%, el personal con un 10% y técnicas, capacitaciones, infraestructura y recursos (efectivo $) CON UN 5% respectivamente.

29. ¿Si se destinan recursos, existen un adiestramiento y concientización para el uso de los mismos?

Si_____, Cuales: _____ No____

RESPUESTA	FRECUENCIA	%
SI	4	67%
NO	2	33%
DESCONOCE	0	0%
TOTAL	6	100%

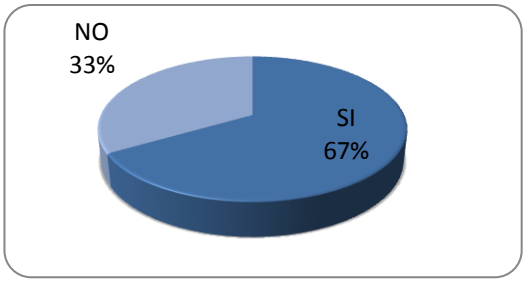


El 33% asegura que no se realizan adiestramientos para los recursos que se invierten para el aseguramiento de la seguridad de la información, el 67% asegura que si y se hace por medio de charlas, capacitaciones y reuniones verbales.

30. ¿Los recursos destinados alcanzan a cubrir la demanda?

Si_____ No____ ¿Porque?_____

RESPUESTA	FRECUENCIA	%
SI	2	33%
NO	4	67%
DESCONOCE	0	0%
TOTAL	6	100%



El 33% afirma que los recursos destinados alcanzan a cubrir la demanda y el 67% de ellos afirman que no atribuyendo a que son limitados los recursos.

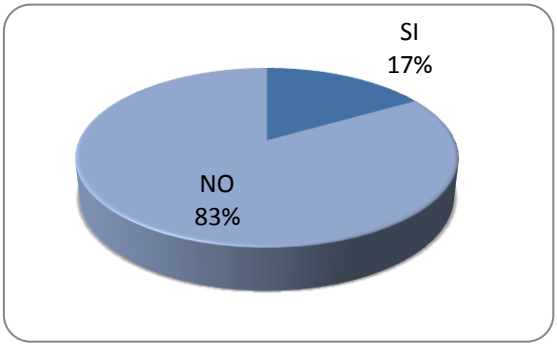
31. ¿Se realizan auditorías internas sobre el manejo y la seguridad de la información en base a requisitos internacionales?

Si_____, Con qué frecuencia: _____ No____

Otro tipo de auditoría: _____

Otros: _____

RESPUESTA	FRECUENCIA	%
SI	1	17%
NO	5	83%
DESCONOCE	0	0%
TOTAL	6	100%

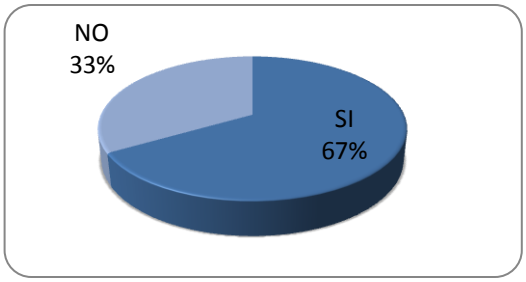


El 17% asegura que existen auditorias pero que no son programadas y el 83% afirma que no existen, solamente las auditorias existentes se enfocan a tener siempre los datos históricos y para afrontar ante la corte de cuentas.

32. ¿Existe un plan de auditorías establecidos?

Si_____ No____

¿Se aplica debidamente? Si_____ No____



RESPUESTA	FRECUENCIA	%
SI	2	33%
NO	4	67%
DESCONOCE	0	0%
TOTAL	6	100%

El 33% afirma que existe un plan de auditorías establecido enfocado a conservar la calidad, el restante dice que no se posee un plan establecido.

33. ¿Quién o quiénes es/son el/los responsables de efectuar las auditorias?_____

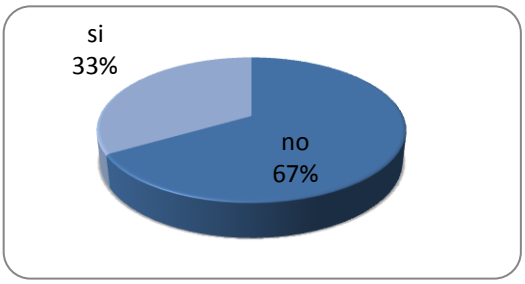
La Unidad responsable de efectuar dichas auditorias es la Unidad de Gestión Integrada atreves de las auditorias respectivas que se realizan anualmente.

34. ¿La gerencia realiza revisiones generales en cuanto al manejo y seguridad de la Información?

Si_____ No____

Si su respuesta es No, pase a la pregunta 41.-

RESPUESTA	FRECUENCIA	%
SI	2	33%
NO	4	67%
DESCONOCE	0	0%
TOTAL	6	100%



El 33% afirma que la gerencia realiza revisiones generales y lo hace por medio de varios tipos de informes. El 67% de ellos afirman que la gerencia no lo hace.

35. Si se realizan, ¿Cada cuanto tiempo se realizan?

Cada mes____
Cada 3 meses____
Cada 6 meses____
Cada año____
Otros intervalos_____

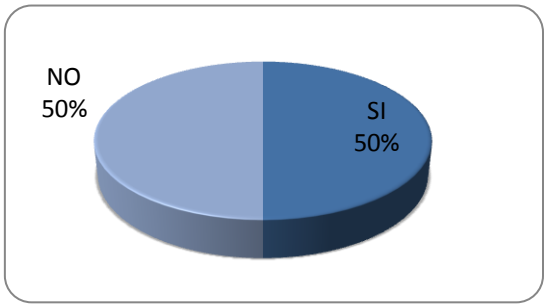
Recursos	% de asignación
mensual	0%
cada 3 meses	0%
cada 6 meses	0%
cada año	0%
periódicamente	100%

El 100% asegura que no hay definido tiempo y que la gerencia lo hace periódicamente cuando requiere informarse o cuando algún procedimiento se ha modificado.

36. Si se realizan revisiones, ¿Estas se encuentran documentadas debidamente?

Si_____ No____

RESPUESTA	FRECUENCIA	%
SI	1	50%
NO	1	50%
DESCONOCE	0	0%
TOTAL	2	100%



El 50% asegura que las revisiones se encuentran documentadas en su totalidad, el otro 50% expuso que no se encuentran documentadas.

37. ¿Qué insumos se utilizan para realizar las revisiones?

Resultados de auditorias____

Retroalimentación de usuarios____

Técnicas, productos o procedimientos de mejora____

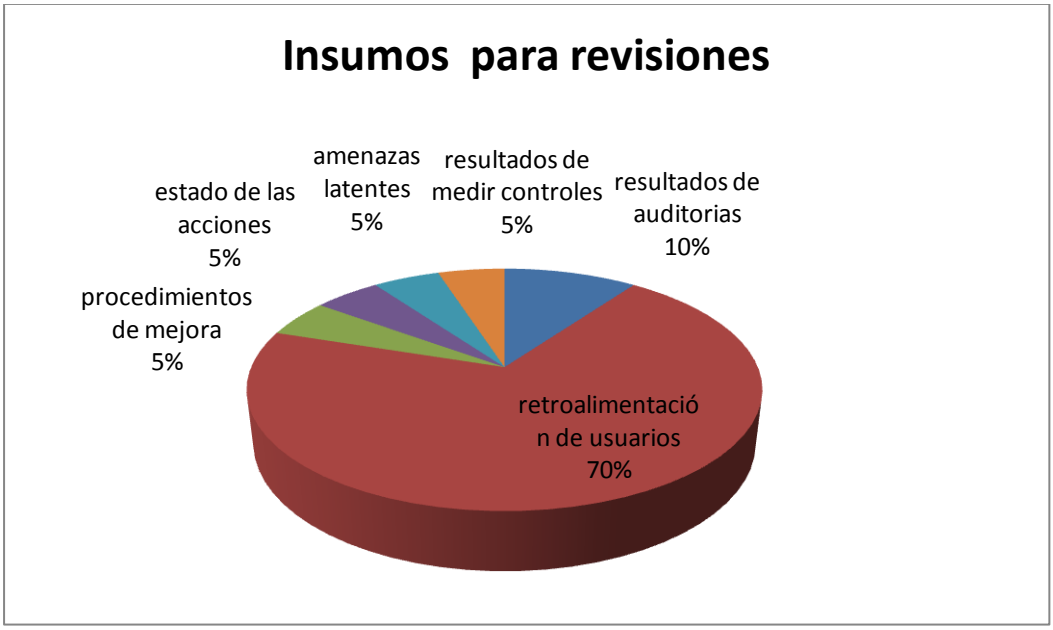
Estado de acciones preventivas y correctivas____

Vulnerabilidades o amenazas latentes____

Resultados de mediciones de controles____

Otros especifique_____

Insumos	% de asignación
Resultados de auditorias	10%
Retroalimentación de usuarios	70%
Procedimientos de mejora	5%
Estado de las acciones	5%
Amenazas latentes	5%
Resultados de medir controles	5%



En un 70% los insumos para realizar las revisiones es originado a partir de una retroalimentación con los usuarios, solamente un 10% se atribuye a los resultados de las auditorias y un 5% para las demás alternativas como lo son procedimientos de mejora, estado de acciones, amenazas latentes, resultados de medir los controles.

38. ¿Qué tipo de resultados arrojan las revisiones?

Mejora la eficacia____

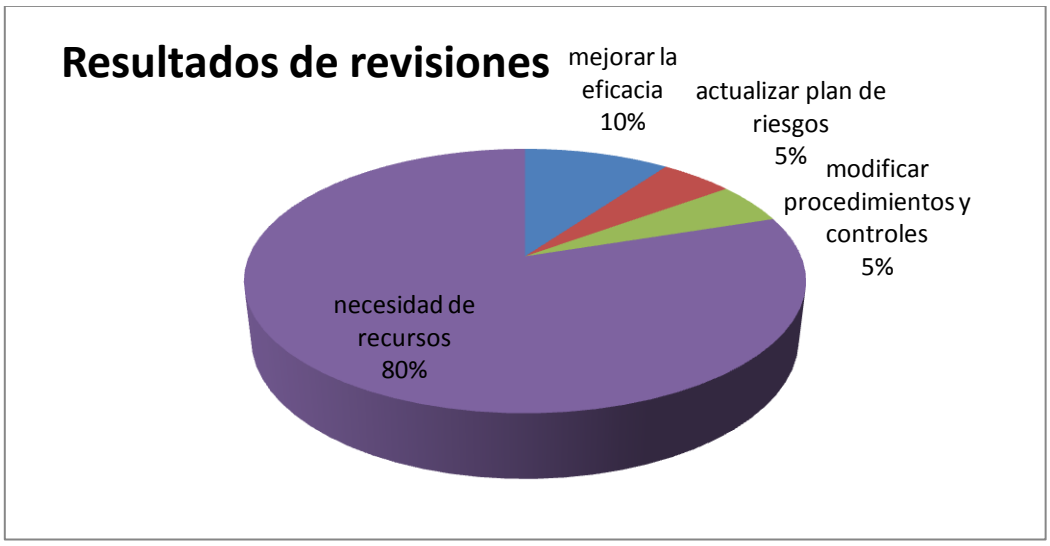
Actualización del plan de tratamiento de riesgos____

Modificación de procedimientos y controles____

Necesidades de recursos____

Otros especifique_____

Recursos	% de asignación
mejorar la eficacia	10%
actualizar plan de riesgos	5%
modificar procedimientos y controles	5%
necesidad de recursos	80%



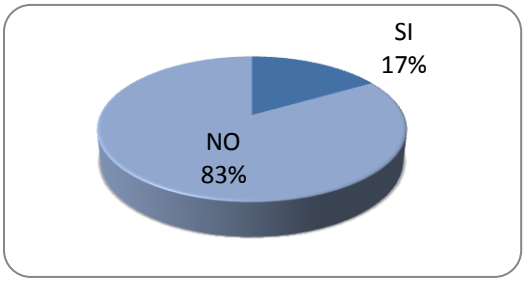
Los resultados en un 70% indican que es necesario invertir más en recursos de todo tipo tanto económico, personal y tecnológico.

Luego un 10% indican que es necesario mejorar la eficacia y para actualizar el plan de riesgos así como para modificar procedimientos y controles solamente un 5% respectivamente.

39. ¿Existe un mecanismo establecido por la Comisión que mejore continuamente el manejo y seguridad de la información?

Si_____ Cual: _____ No____

RESPUESTA	FRECUENCIA	%
SI	1	17%
NO	5	83%
DESCONOCE	0	0%
TOTAL	6	100%

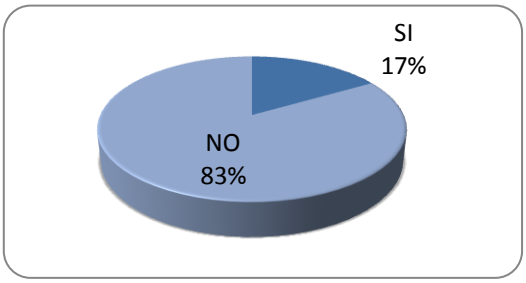


El 17% asegura que existe un mecanismo de mejora continuamente el manejo y seguridad de la información, dicho mecanismo es el desarrollo de sistemas informáticos de control. El restante 83% asegura que no se posee mecanismos de ese tipo.

40. Ante un fallo de seguridad ¿Se toman medidas o acciones correctivas para eliminar el fallo?

Si_____, Cuales: _____ No____

RESPUESTA	FRECUENCIA	%
SI	5	83%
NO	1	17%
DESCONOCE	0	0%



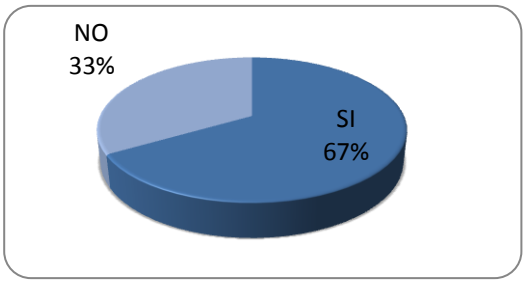
TOTAL	6	100%

El 83% de ellos afirmaron que si se toman medidas y lo primero que se hace es verificar cual fue la fuente o causa y una vez definido eso se establecen las medidas para solucionar y tratar que no suceda de nuevo. Por el contrario el 17% asegura que no se toman medidas correctivas.

41. ¿Se toman acciones o medidas preventivas ante fallos de seguridad potenciales?

Si_____, Cuales: _____ No____

RESPUESTA	FRECUENCIA	%
SI	4	67%
NO	2	33%
DESCONOCE	0	0%
TOTAL	6	100%



El 67% asegura que existen acciones preventivas algunas de ellas se establecen el procedimiento 17-09 y otras son tomadas de acuerdo a la experiencia.

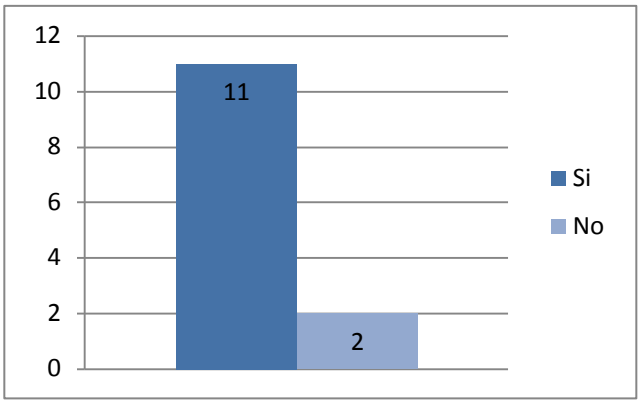
El 33% asegura que no se poseen medidas preventivas ante posibles fallos de seguridad potenciales.

ANEXO 10: TABULACIÓN DE DATOS DE ENCUESTA PARA LA UNIDAD INFORMÁTICA INSTITUCIONAL.

2. ¿Existe un sistema dentro de la Comisión que busque asegurar la información?

R/

Si	No
11	2



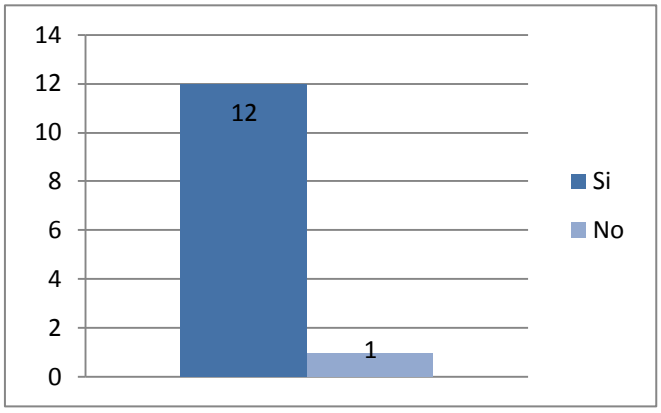
Si no existe como se asegura:

a) Mediante Roles de acceso a los datos, usuarios, contraseñas y seguridad de acceso a la red.
b) Contraseñas y sitios de resguardo.

3. ¿Los procesos Claves y de Apoyo se encuentran basados bajo el modelo Planeación, Ejecución, Revisar y Mejorar?

R/

Si	No
12	1



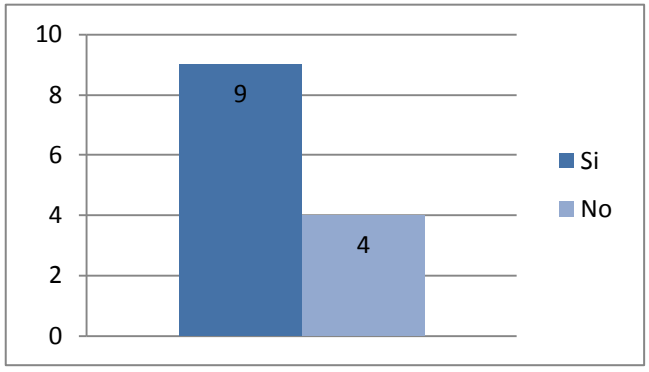
Si no están basados en ese modelo, en que están basados:

a) Existen procedimientos: Sitio de Contingencia, respaldos, asignación de permisos.

4. ¿Se cuenta con un alcance y limitaciones definidas en el manejo y seguridad de la información?

R/

Si	No
9	4



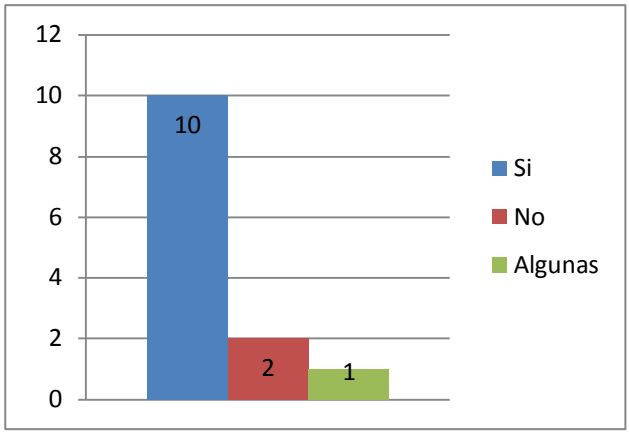
Si no hay alcance y limitaciones definidas, como se delimita:

a) Se concientiza por parte de la jefatura pero no hay nada formal sobre esto.
b) No respondió (2)
c) Se delimita a través de los procedimientos y normativas generadas, las cuales en sí mismas llevan intrínsecamente el componente de seguridad de la información.

5. ¿Se cuenta con políticas definidas en el manejo y seguridad de la información?

R/

Si	No	Algunas
10	2	1



Si no existen políticas, como se rige:

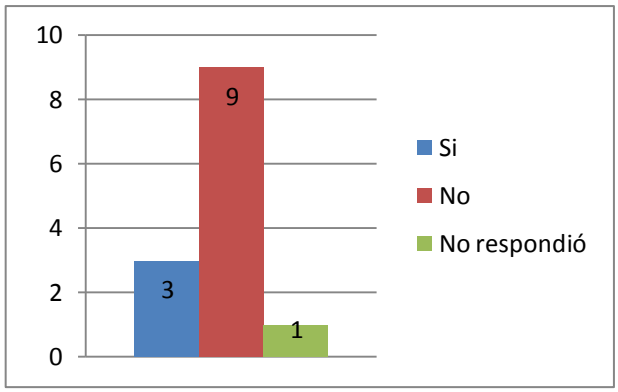
a) No respondieron (2)
b) Algunas: Solamente para el caso de la información electrónica, con énfasis en el acceso.

Si: Se rige con normativas para el manejo del correo, contraseñas, uso de red, etc.

6. ¿Existe una metodología para la evaluación de riesgos de la información?

R/

Si	No	No respondió
3	9	1



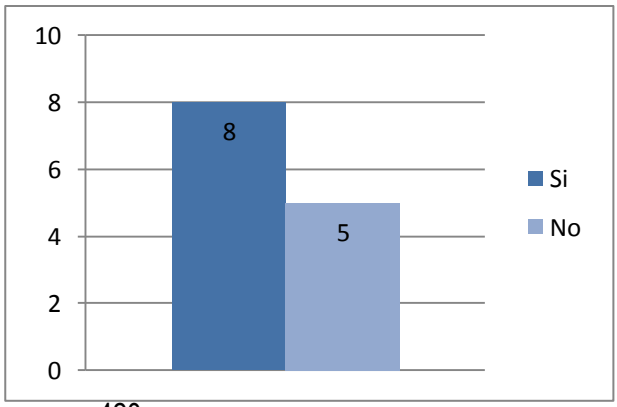
Si no existe como se evalúan:

a) Se evalúan en forma informal y apreciativa
b) Se evalúan considerando los principales eventos que puedan poner en riesgo la información y ante ellos se ha creado un plan de contingencia.
c) De acuerdo a la cobertura de cada área
d) En algunos casos, de forma correctiva, a partir de incidentes, por medio de retroalimentación de usuarios.
e) No respondieron (5)

7. ¿Se tienen identificados y clasificados los riesgos de información, así como sus amenazas y vulnerabilidades?

R/

Si	No
8	5



Si no se tienen identificados y clasificados, como se encuentran:

a) Los riesgos están identificados, pero no clasificado.
b) En forma apreciativa.
c) En forma sistemática y documentada
d) No respondieron (2)

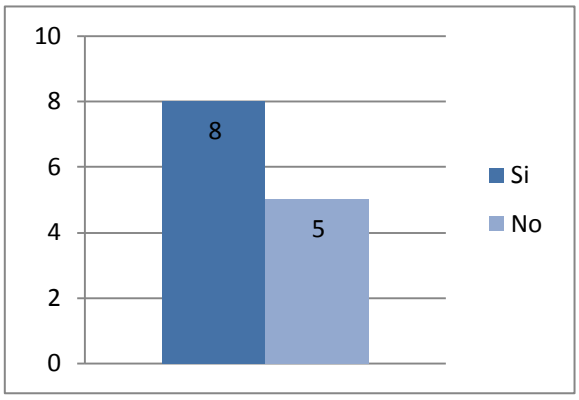
Si se tienen identificados y clasificado:

a) En los sistemas y procedimientos contingenciales se han clasificado los riesgos (2)

8. ¿Se usan criterios para identificar y clasificar los riesgos?

R/

Si	No
8	5



Si, cuales:

a) Se identifican en base a riesgos conocidos
b) A través de Monitoreo a accesos a sistemas (2)
c) Según los establecidos en los procedimientos contingenciales (2)
d) Criticidad a los cuales se expone toda actividad de la Comisión. Alta importancia en el giro de facturación de nuestros servicios/producto. Exposición de daños de cualquier tipo, evaluados por el personal idóneo/involucrado.
e) Los que tienen que ver con contraseñas, envíos de correos, procesos, etc.
f) No respondieron

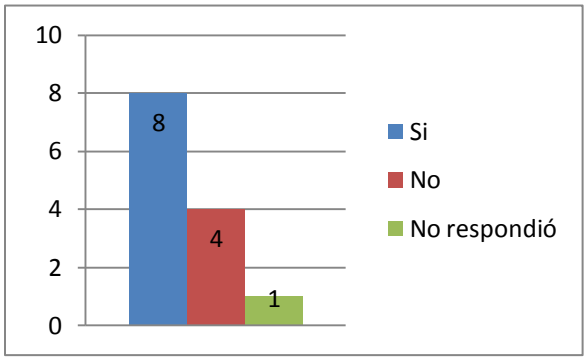
Si no se usan criterios bajo que los identifican y clasifican:

a) No se clasifican
b) No respondieron (3)
c) En forma sistemática y documentada.

9. ¿Se ha previsto el impacto que ocasionan los riesgos de la información?

R/

Si	No	No respondió
8	4	1



Si, cuales:

a) En base a los eventos de Catástrofes (2)
b) Los impactos que se detallan en los

procedimientos para contingenciales sistemas informáticos (4)

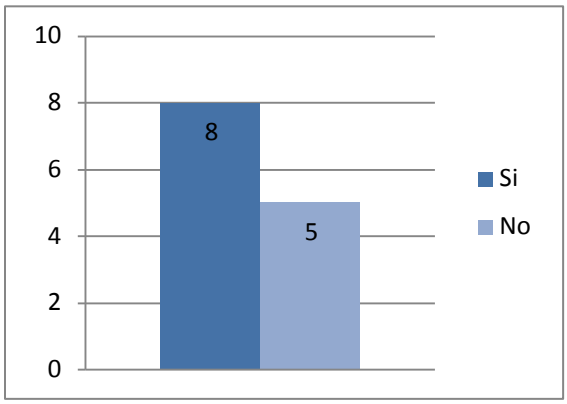
c) Pérdida total de la confidencialidad. Puesta en riesgo lo infraestructura lógica y física. Perdida de presencia en el negocio del mercado de generación de energía eléctrica. Divulgación de información propia de la Comisión de manera innecesaria.

d) Perdida de la información. Costos. Baja en la eficiencia.

10. ¿Se ha determinado un nivel de riesgo admisible?

R/

Si	No
8	5



Si, cual o cuales:

a) Definidos en documentación de sistemas (procedimientos) contingenciales (6)

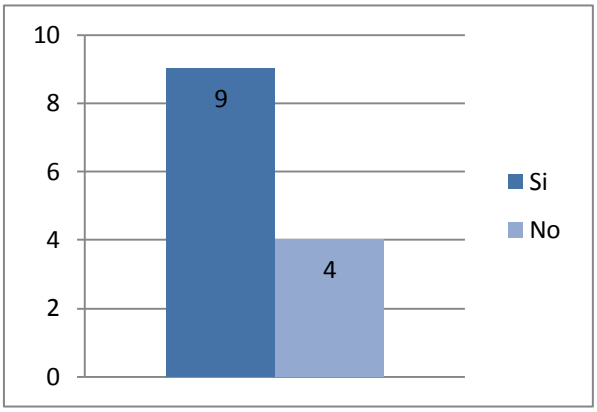
b) Aquellos que no impactan directamente a la integridad ni de la información ni a la infraestructura de la Comisión. Aquellos a los que el personal por sus labores/responsabilidades se ven expuestos sin consecuencias algunas.

c) Aquellos que posibiliten la entrada de un plan de contingencias

11. ¿Existen medidas a tomar ante la existencia de riesgos?

R/

Si	No
9	4



Si, cuales:

a) Definidas en documentación de sistemas de contingencia. Sitios y planes contingenciales para los procesos críticos de la Comisión (7)

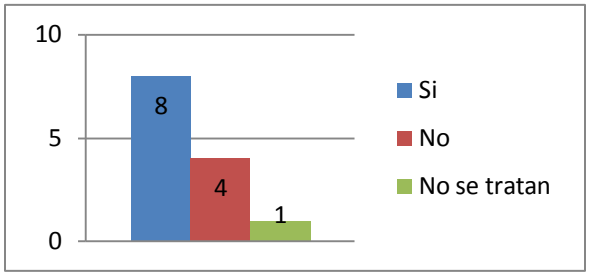
b) Generar planilla desde sitio contingencial, recuperar respaldos, etc.

c) Las concernientes a temas preventivos. Evitar cualquier tipo de esquemas que presenten riesgos en todos los ámbitos que competen a las acciones de los funcionarios de CEL.

12. ¿Existe un plan de tratamiento de riesgos?

R/

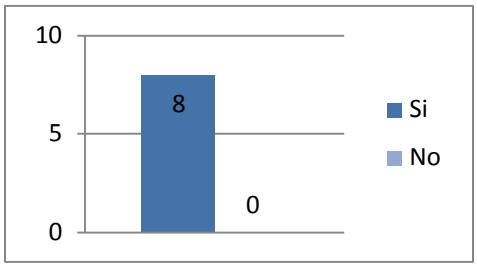
Si	No	No se tratan
8	4	1



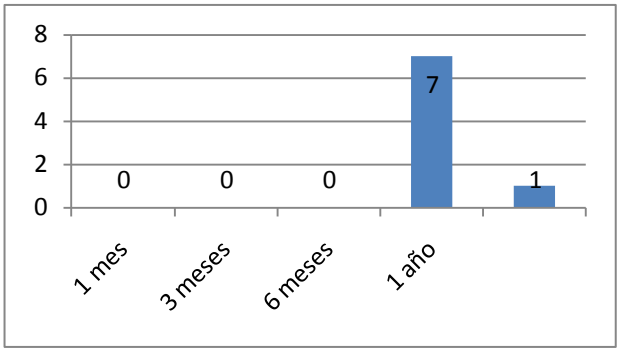
13. Si existe un plan de tratamiento de riesgos, ¿se actualiza constantemente?

R/

Si	No
8	0



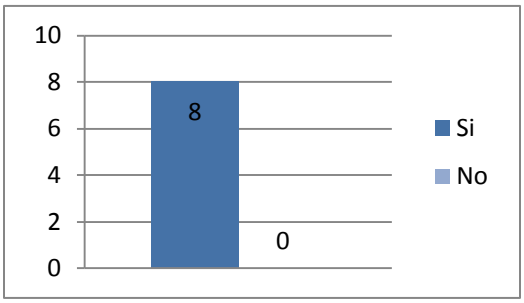
¿Cada cuánto?	
1 mes	0
3 meses	0
6 meses	0
1 año	7
Otros intervalos	1



14. ¿Se cumplen las mejoras propuestas al plan?

R/

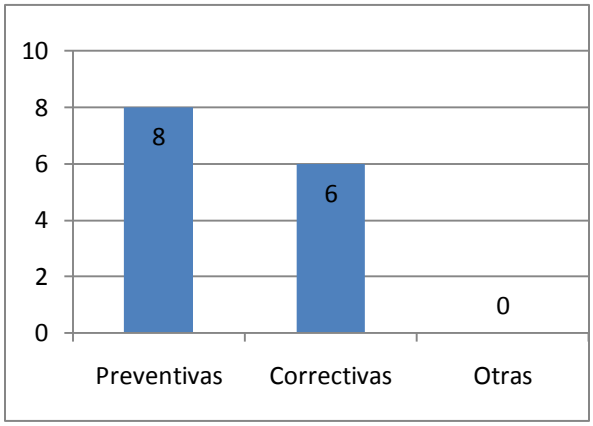
Si	No
8	0



15. ¿Qué tipo de acciones se toman?

R/

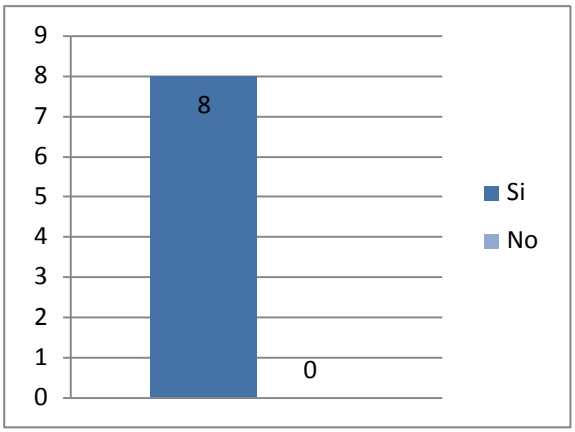
¿Qué tipo de acciones?	
Preventivas	8
Correctivas	6
Otras	0



16. ¿Existen controles para el tratamiento de los riesgos?

R/

Si	No
8	0



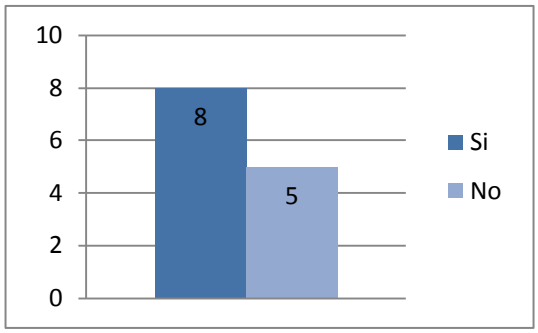
Si, cuales:

a) Entrevistas, visitas periódicas a áreas determinadas, normativas establecidas con las autoridades. Verificación constante del flujo de la información.
b) Auditorias
c) Respaldo de información, auditorias de las bases de datos, planes de contingencia (5)

17. ¿Existe capacitación al personal en cuanto al manejo y seguridad de la información?

R/

Si	No
8	5



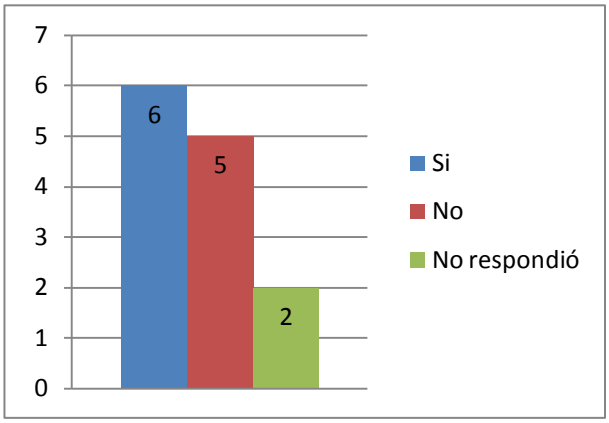
Si respondieron SI, con qué frecuencia:

- Anualmente (7)
- No respondió (1)

18. ¿Posee un mecanismo que detecte incidentes de seguridad de la información?

R/

Si	No	No respondió
6	5	2



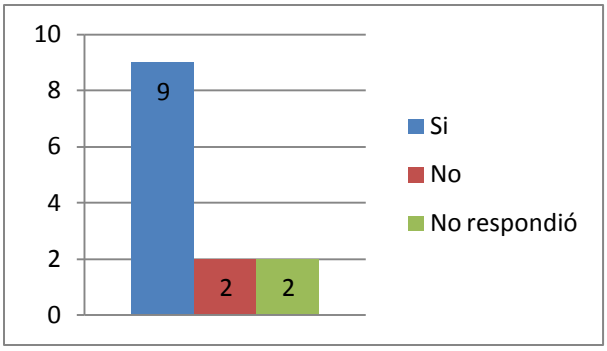
Si, Cuales:

a) Auditorías de personas y sistemas (3)
b) Observaciones de auditorías (2)
c) No respondió (1)

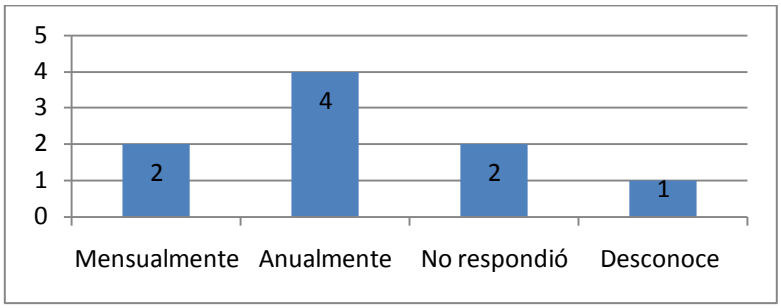
19. ¿Se ejecutan procedimientos de revisión y monitoreo dentro de las formas de manejo y seguridad de la información?

R/

Si	No	Desconoce
9	2	2



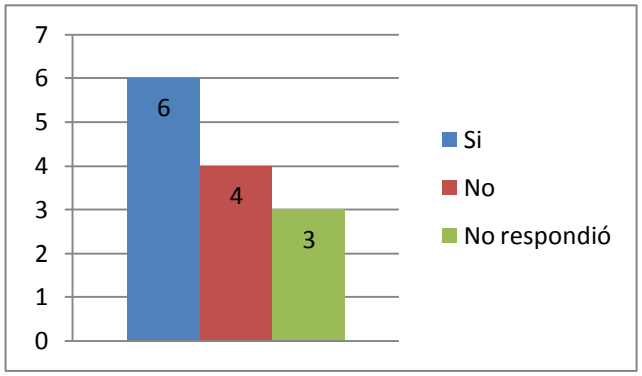
¿Cada cuánto?	
Mensualmente	2
Anualmente	4
No respondió	2
Desconoce	1



20. ¿Se revisa la efectividad de los controles existentes?

R/

Si	No	No respondió
6	4	3



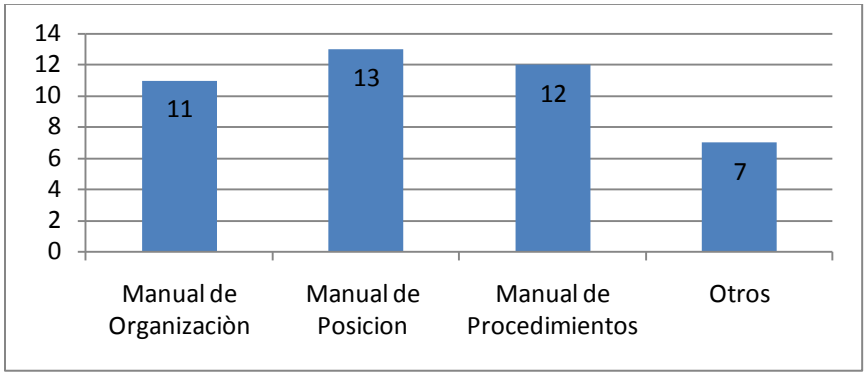
Sí, ¿cada cuánto:

- Semestralmente (1)
- Anualmente (2)
- Desconoce (1)
- No respondió (2)

21. ¿Qué tipo de documentos existen en la comisión?

R/

Tipos de Documentos	
Manual de Organización	11
Manual de Puestos	13
Manual de Procedimientos	12
Otros	7

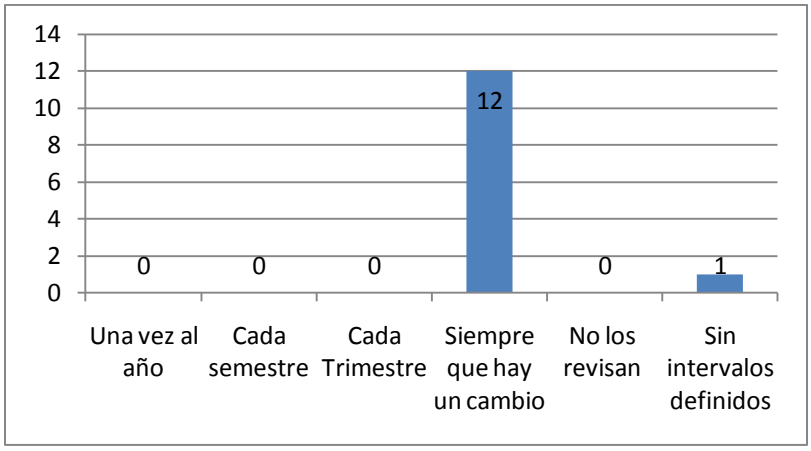


Otros: Políticas, normativas e Instructivos

22. ¿Cada cuánto tiempo se revisan y actualizan los documentos?

R/

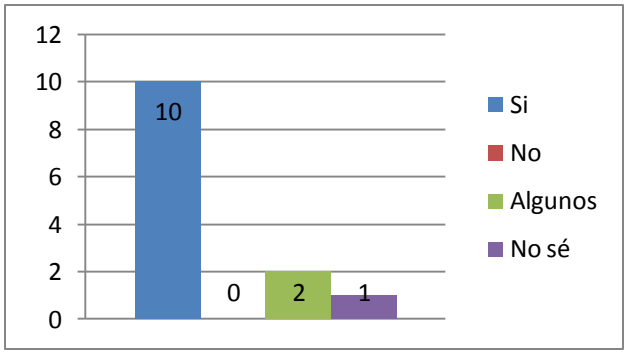
¿Cada cuánto?	
Una vez al año	0
Cada semestre	0
Cada Trimestre	0
Siempre que hay un cambio	12
No los revisan	0
Sin intervalos definidos	1



23. ¿Los documentos en uso se encuentran actualizados?

R/

Si	No	Algunos	No sé
10	0	2	1



Ultima fecha de actulizacion:

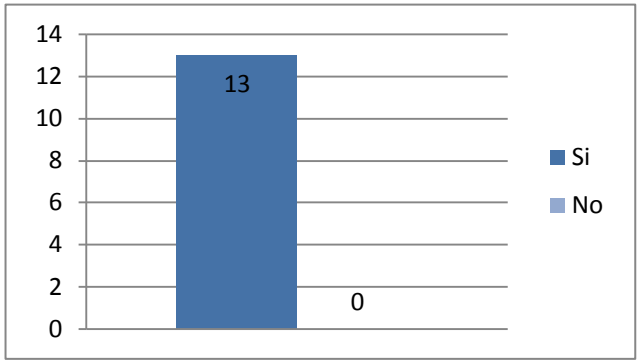
- Septiembre de 2008
- Diciembre de 2007
- 28/02/08 (para 17-01)
- Procedimientos febrero de 2008

- No respondieron (9)

24. ¿Se trabaja de acuerdo a los procedimientos establecidos?

R/

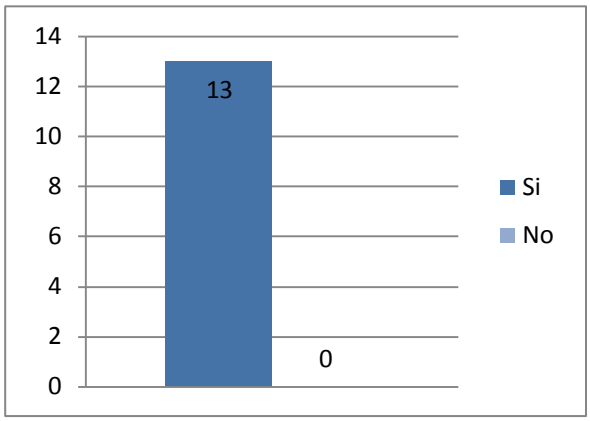
Si	No
13	0



25. ¿Los documentos están disponibles en los puntos de uso y permanecen legibles y fácilmente identificables?

R/

Si	No
13	0



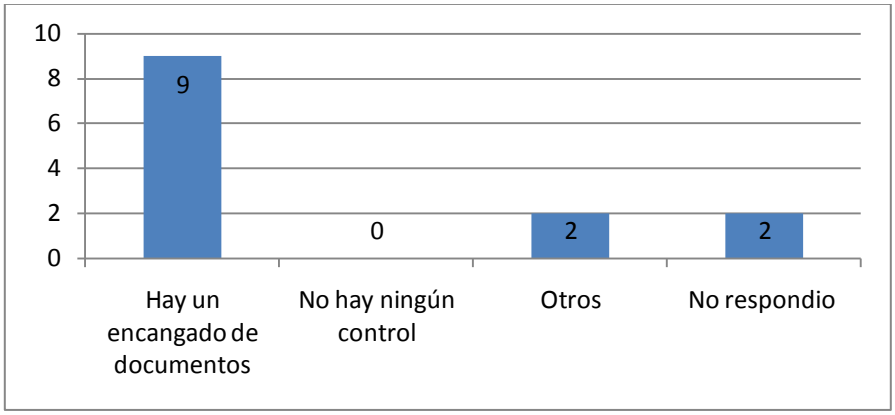
Dónde se encuentran:

- Intranet (6)
- Documentos físicos (1)
- No respondió (6)

26. ¿De qué manera se controlan los documentos del establecimiento?

R/

Control de Documentos	
Hay un encargado de documentos	9
No hay ningún control	0
Otros	2
No respondió	2

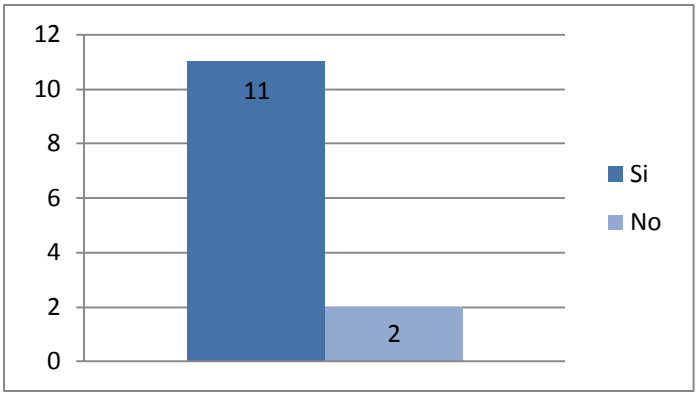


Otros: intranet y control de vensiones

27. ¿La gerencia ha expresado al personal la importancia de la seguridad de la información?

R/

Si	No
11	2



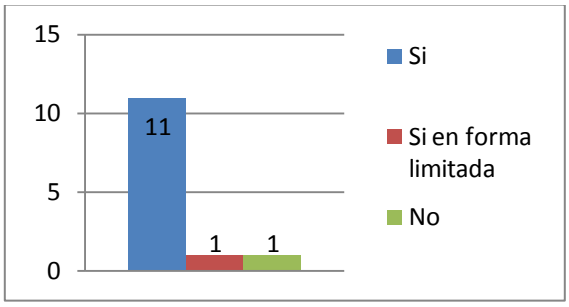
Sí, de qué forma:

a) Charlas informativas y de concientización, correos recordatorios del manejo de la información, contraseñas, encuestas.(3)
b) Despliegues informativos, procedimientos establecidos por la gestión integrada.(6)
c) Se realiza por medio de la jefatura de la unidad
d) Capacitaciones

28. ¿Se destinan recursos para asegurar la información?

R/

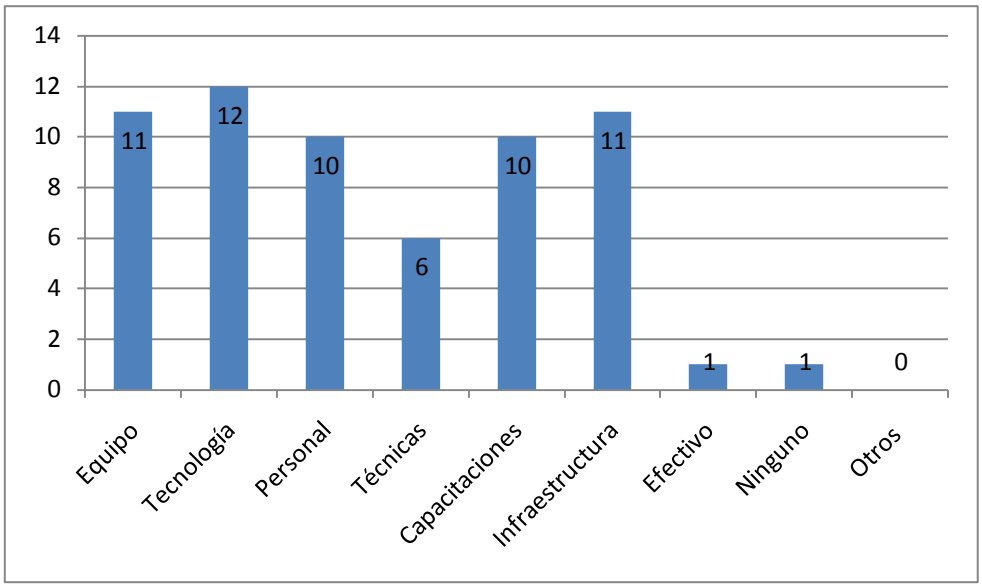
Si	Si en forma limitada	No
11	1	1



29. ¿Qué recursos se destinan para el manejo y seguridad de la información?

R/

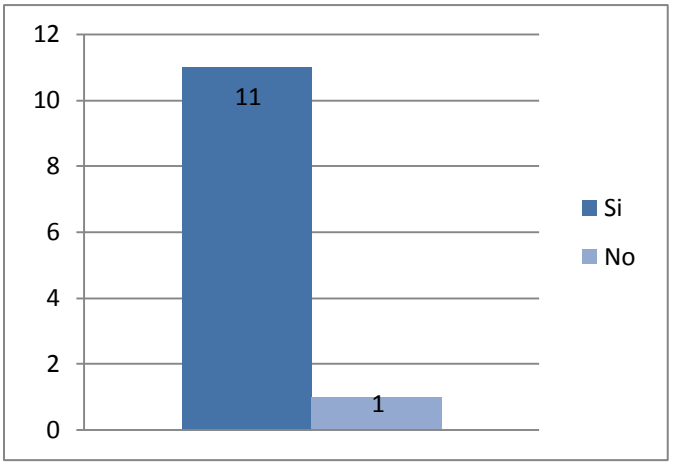
¿Qué recursos?	
Equipo	11
Tecnología	12
Personal	10
Técnicas	6
Capacita-ciones	10
Infraes-tructura	11
Efectivo	1
Ninguno	1
Otros	0



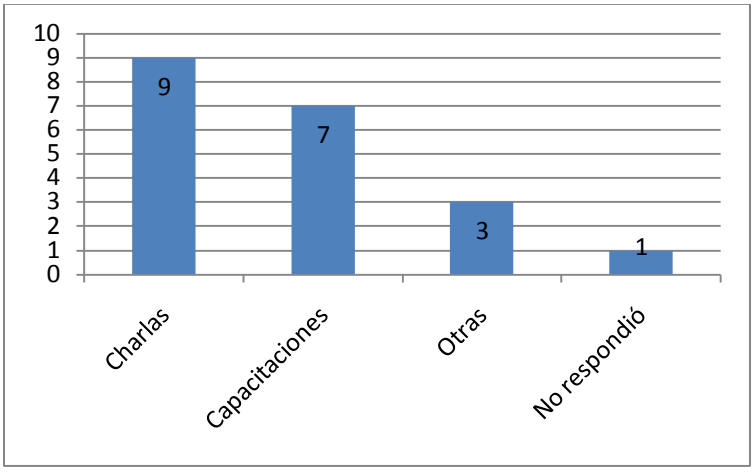
30. ¿Si se destinan los recursos, existe un adiestramiento y concientización para el uso de los mismos?

R/

Si	No
12	1



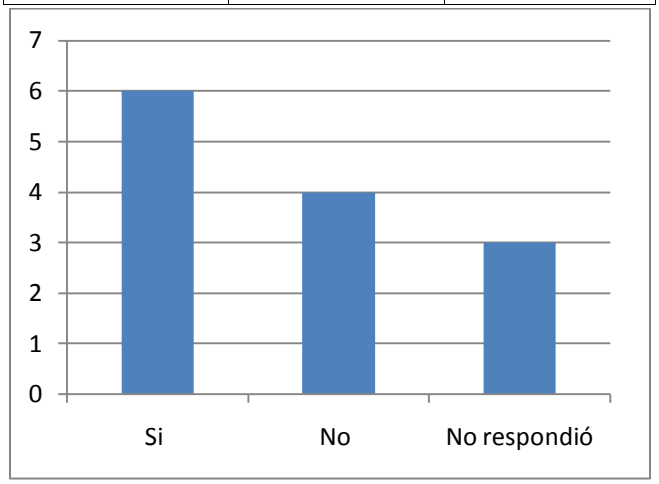
¿Cuáles?	
Charlas	9
Capacitaciones	7
Otras	3
No respondió	1



31. ¿Los recursos destinados no alcanzan a cubrir la demanda?

R/

Si	No	No respondió
6	4	3



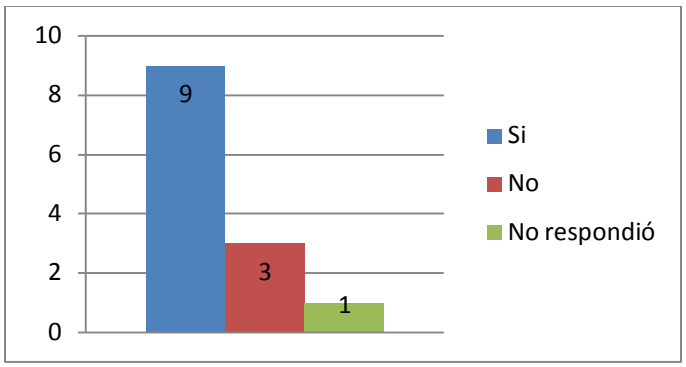
Sí, porqué:

- En materia de seguridad hay mucho que mejorar.
- Aunque existan recursos, es necesario seguir trabajando en culturización, mecanismos para hacer cumplir estatus o normativas para asegurar la información.
- No respondieron (4)

32. ¿Se realizan auditorías internas sobre el manejo y la seguridad de la información en base a requisitos internacionales?

R/

Si	No	No respondió
9	3	1



Sí, con qué frecuencia:

- Anualmente (8)
- No respondió (1)

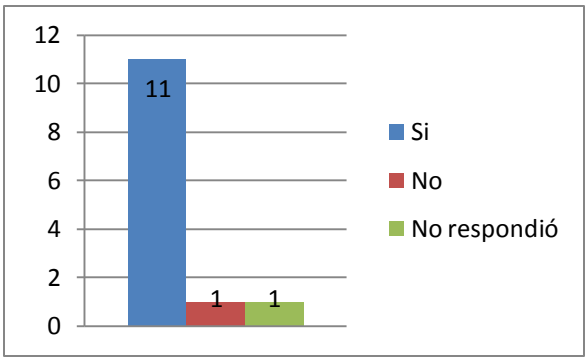
Otro tipo de auditoría (2)

- Es la que queda a criterio del auditor interno

33. ¿Existe un plan de auditorías establecido?

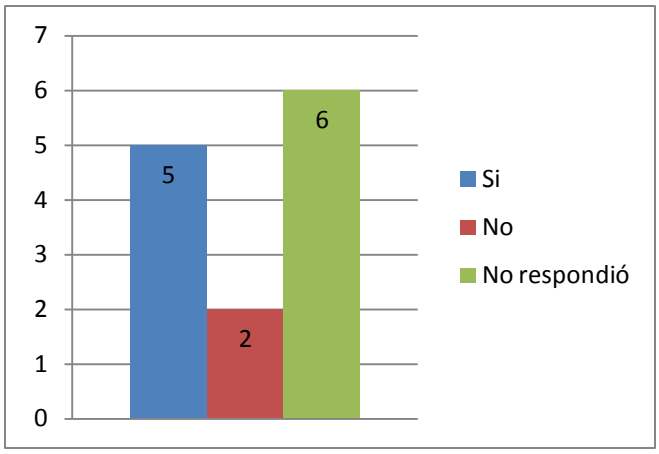
R/

Si	No	No respondió
11	1	1



¿Se aplican debidamente?

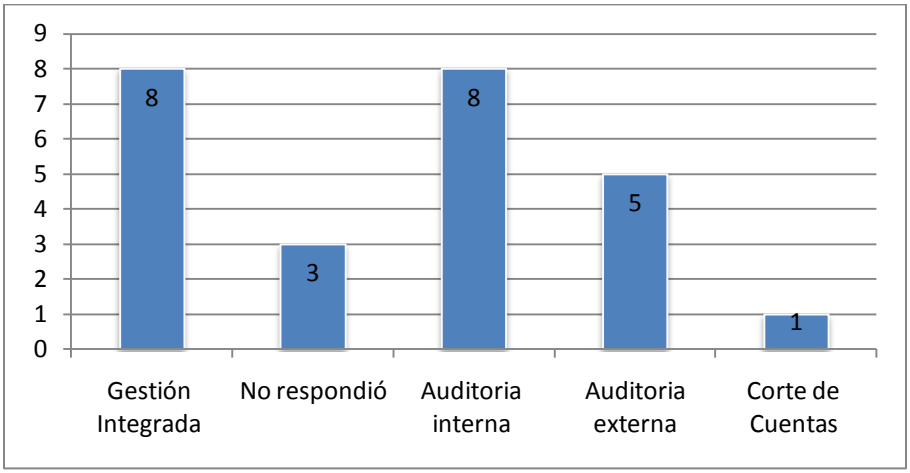
Si	No	No respondió
5	2	6



34. ¿Quien o quienes es/son él/los responsables de efectuar las auditorias?

R/

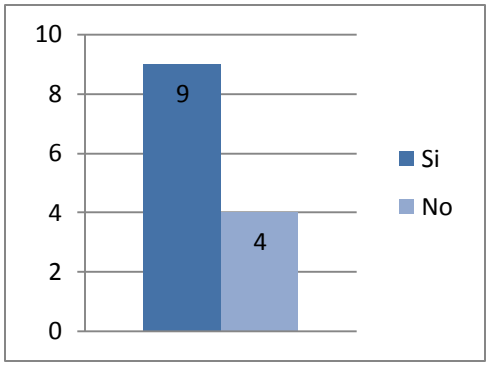
¿Responsables?	
Gestión Integrada	8
No respondió	3
Auditoría interna	8
Auditoría externa	5
Corte de Cuentas	1



35. ¿La gerencia realiza revisiones generales en cuanto al manejo y seguridad de la información?

R/

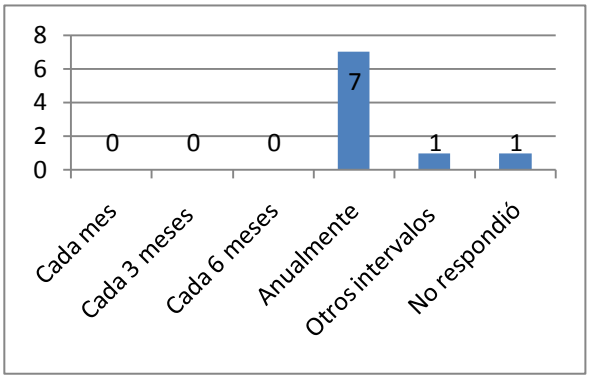
Si	No
9	4



36. Si se realizan ¿Cada cuánto tiempo se realizan?

R/

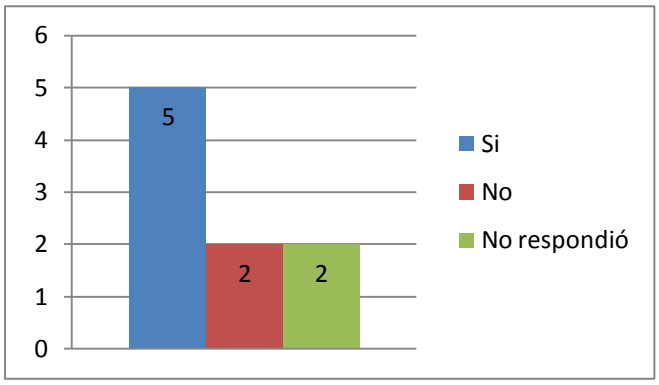
¿Cada cuánto?	
Cada mes	0
Cada 3 meses	0
Cada 6 meses	0
Anualmente	7
Otros intervalos	1
No respondió	1



37. Si se realizan revisiones ¿Estas se encuentran documentadas debidamente?

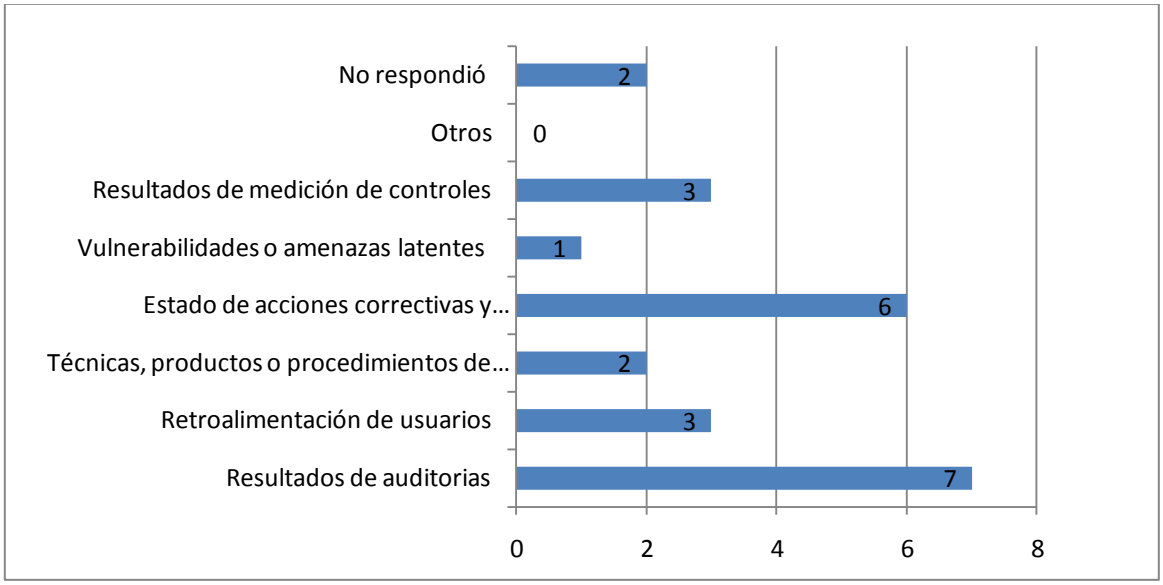
R/

Si	No	No respondió
5	2	2



38. ¿Qué insumos se utilizan para realizar las revisiones?

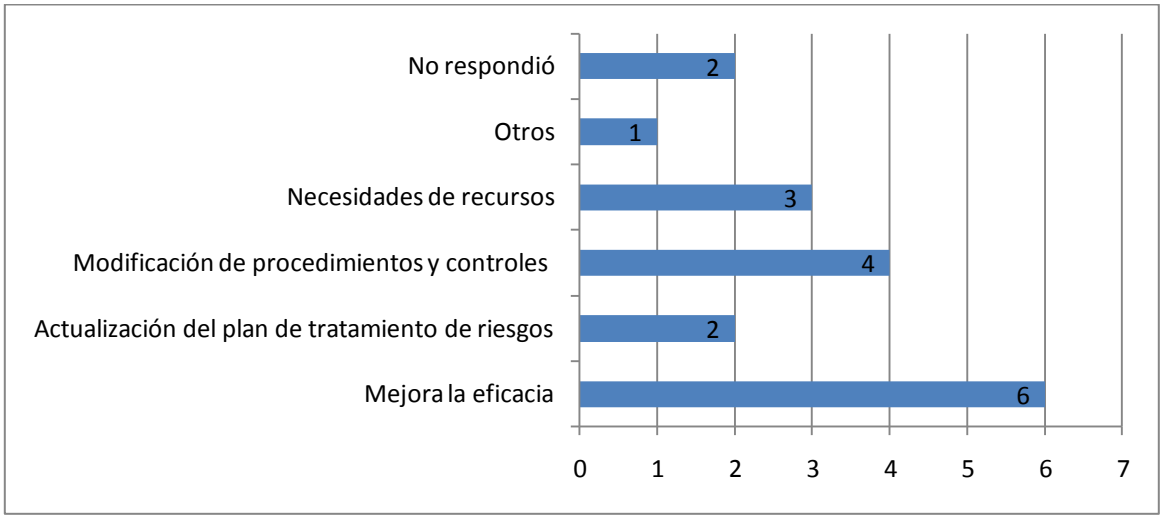
Insumos	
Resultados de auditorias	7
Retroalimentación de usuarios	3
Técnicas, productos o procedimientos de mejora	2
Estado de acciones correctivas y preventivas	6
Vulnerabilidades o amenazas latentes	1
Resultados de medición de controles	3
Otros	0
No respondió	2



39. ¿Qué tipo de resultados arrojan las revisiones?

R/

Resultados	
Mejora la eficacia	6
Actualización del plan de tratamiento de riesgos	2
Modificación de procedimientos y controles	4
Necesidades de recursos	3
Otros	1
No respondió	2



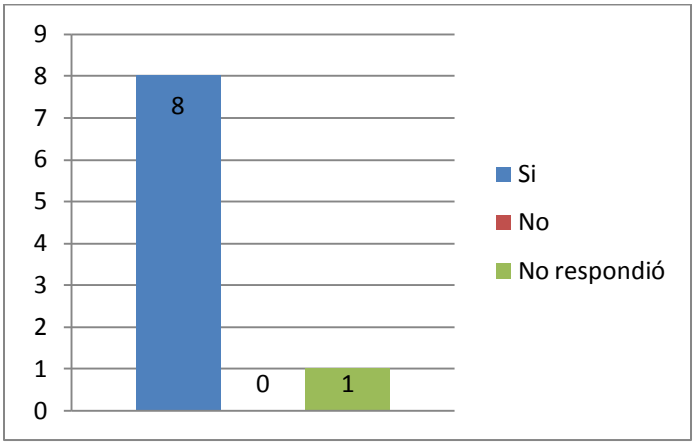
Otros:

a) Mantener alta disponibilidad.

40. ¿Existe un mecanismo establecido por la Comisión que mejore continuamente el manejo y seguridad de la información?

R/

Si	No	No respondió
8	0	1



Cuáles:

a) Sistema de Gestión integrada, control de accesos, permisos. (4)
b) Solamente seguridad informática. (1)
c) Charlas de concientización. Registro de calidad, producto de ejecutar procedimientos establecidos, los cuales producen o resultan en la continuidad, tanto, en el manejo de la información como de subsanar cualquier indicio de riesgo.
d) No respondieron. (2)

41. Ante un fallo de seguridad ¿se toman medidas o acciones correctivas para eliminar el fallo?

R/

Si	No	Desconoce
11	1	1

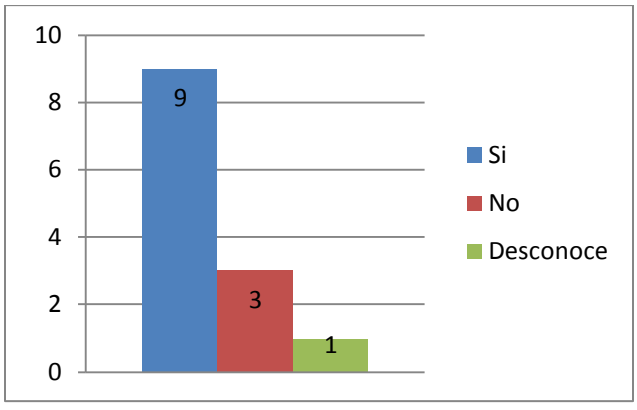
Cuáles:

a) Dependiendo el caso o falla. (2)
b) Según lo establecido en los procedimientos contingenciales. (2)
c) Se incrementa la seguridad de acceso a la red, datos o sistemas.
d) Modificación a normativas establecidas, modificación en controles del flujo o manejo de la información.
e) Solamente en el contexto informático.
f) A través de acciones correctivas y preventivas.
g) No respondieron. (3)

42. ¿Se toman acciones o medidas preventivas ante fallos de seguridad potenciales?

R/

Si	No	Desconoce
9	3	1



Cuáles:

a) Según lo establecido en los procedimientos contingenciales. (2)

b) Ejecución de procedimientos que aporten insumos para la eliminación de cualquier tipo de fallo o “hueco” por el cual se ponga en riesgo tanto el flujo de la información, así como todos los elementos que intervienen en el proceso.
c) Mejoras de los PRA´s.
d) Pruebas por la UII.
e) Depende del caso.

ANEXO 11: TABULACIÓN DE INFORMACIÓN DE ENTREVISTAS DE LA UNIDAD DE PRODUCCIÓN, COMERCIALIZACIÓN, INFORMÁTICA Y DESARROLLO HUMANO.

i. Unidad de Producción

GUÍA DE ENTREVISTA

Proceso: Proceso de Producción	**Fecha: 28/11/08**	**Hoja:**
Departamento o Área:		
Nombre del entrevistado: Ing. Cáceres		
Cargo: Gerente de Producción		
Posee personal a su cargo: SI	**Cuantos: 175**	

CONTROL:

¿Qué tipo de información o documentos maneja?

Existen dos tipos de información, Los Registros de calidad (RC) que son los datos de operación y de mantenimiento y los documentos históricos, como correspondencia, información sobre proyectos de CEL.

Existe un control para esta información

Cada procedimiento produce un RC y debe llevar un análisis tipo check list. Los RC se digitalizan para un mejor resguardo y disponibilidad de la misma, la información puede ser física o electrónica. Cada RC tiene controles de resguardo aproximadamente de 5 años.

Quien controla toda o parte de la información Cada productor de información es el dueño y responsable de la misma, por lo tanto el la controla, muchas veces la controla el personal de la misma unidad y otros pasan por la jefatura para revisión otros no.

Como se controla

Se controla a través de check list. A través de una guía de archivos que es similar a un inventario de archivos.

Cada cuanto se controla

Por ser un proceso continuo se controla diariamente

Que beneficio trae el aplicar estos controles

Los beneficios son económicos, existe un mejor manejo de la información, en términos de tiempo, efectividad, disponibilidad.

Que impacto tiene el no controlar.

Pérdidas económicas, tiempos inactivos, mala toma de decisiones.

INTEGRIDAD:

Quien manipula los documentos (durante el transporte y el proceso)

Los dueños del proceso

Quien autoriza y define las responsabilidades de manipulación

Los responsables del proceso y la jefatura.

Qué tipo de manipulación está autorizada a hacerse en esta área

Registros, revisiones,

Como se garantiza que el documento tenga únicamente alteraciones autorizadas

Ya que cada responsable de la información hace correcciones solo si proviene de la jefatura y el lleva su registro.

Como se asegura en el almacenamiento del documento el acceso al personal autorizado: Se autoriza solamente al personal de la Unidad. Y eventualmente a otras personas previa petición a la jefatura.

Que impacto genera una alteración no autorizada de la información.

En el personal puede generar amonestaciones o en el mayor de los casos despido, puede generar duplicidad de datos, datos que no son legítimos, mas trabajo, genera pérdida de tiempo.

AUTENTICIDAD:

Como se garantiza que la información suministrada es real y veraz

Se revisa previamente pero en general es confiable.

Como se respalda la información para su verificación: se hace a petición, autocontrol o como parte del proceso de emisión.

Se respalda bajo autocontrol y como parte del proceso

Que impacto genera que la información no sea veraz o real.

Puede generar atrasos en la producción, atrasos en los mantenimientos, pérdidas económicas, aumentar costos de producción, mal toma de decisiones, etc.

DISPONIBILIDAD

Como llega la información (solicitud, o flujo de proceso)

Llega como parte del proceso en el flujo de proceso, hay información que no es formal que no forma parte del proceso pero es importante asegurarla como lo es la información histórica o de proyectos de CEL.

La información llega con los tiempos establecidos y oportunos.

No, a veces hay situaciones en que el sistema de información se cae. Se tiene q recurrir a canales de comunicación diferentes, como por ejemplo vía telefónica lo cual no es efectivo como vía electrónica.

La información que necesita está disponible

No siempre.

Que canales y medios se utiliza para el manejo de la información ¿son adecuados?

Se utilizan en su mayoría canales electrónicos y de manera contingencial se tiene vía telefónico, los canales son los adecuados ya que la información es instantánea de una central a otra.

El personal autorizado al acceso de la información cuenta con la información cuando la requiere (esta área genera atrasos para poner la información a disposición de clientes)

No siempre, muchas veces no está ordenada o documentada. Los sistemas de información no son muy confiables y no generan un respaldo.

Que impacto o que dificultades le genera no disponer de la información necesaria en el tiempo preciso.

No se manda el pre despacho a la hora requerida, atrasos en el envio de reportes a la Unidad central, etc.

UTILIDAD

Como obtiene la información que necesita para desempeñar sus funciones (la obtiene por solicitud o como parte del flujo del proceso)

Se obtiene como parte del proceso de producción.

Que volumen de información demanda para su uso

En grandes cantidades pues esta Unidad representa la razón de ser de CEL la cual es producir energía eléctrica.

Utiliza toda la información que recibe, toda le es útil

Si de una manera u otra es toda utilizada,

Como la identifica si es útil o no

Si contribuye de manera directa al proceso es útil.

Qué porcentaje utiliza

90%

Con que frecuencia la utiliza

A diario.

Que impacto positivo o negativo le genera el uso o mal uso de la información

Genera que se produzca lo requerido por comercialización, o pérdidas económicas por no producir lo requerido, genera subutilización de recursos y perdidas de mercados.

CONFIDENCIALIDAD

Manipulan información confidencial

Si hay información confidencial

En porcentaje representa del total de información manipulada

El 80% de la información es confidencial y el 20% no lo es, es de uso general.

El acceso a la información confidencial es solo de la persona o grupo autorizado para hacerlo

Sí hay información que es confidencial manejada en niveles gerenciales, pero hay información que se genera que es de uso general y está en las computadoras de cada uno.

Existen otras personas o grupos que accedan a la información

No, solo con autorización.

Que medios se utilizan para el transporte de la información

Electrónico y físicos, y como correspondencia, (en sobre sellado)

Existe la posibilidad que la información llegue a la persona incorrecta, antes, durante y después de proceso (transito o flujo)

Si, si una persona ajena al proceso la toma para manipular la información o si alguien deja de laborar puede fugarse o robarse la información.

O que los RC caigan en manos de la competencia o le llegue información a los contratistas para que jueguen a su favor las licitaciones.

Que impacto genera que la información llegue a las manos equivocadas

Genera mala imagen a la institución, mal ambiente laboral si se saben medidas que el personal las considera negativas.

ii. Unidad de Comercialización

GUÍA DE ENTREVISTA

Proceso: Comercialización	**Fecha: 28/11/08**	**Hoja:**
Departamento o Área:		
Nombre del entrevistado: Juan Carlos		
Cargo: Jefe de la Unidad de Comercialización.		
Posee personal a su cargo: SI	**Cuantos: 4 Analistas y 1 Secretaria.**	

CONTROL:

¿Qué tipo de información o documentos maneja?

Básicamente se maneja información de las diferentes variables de mercado sobre ofertas, inyecciones, precios de mercado, y por otra parte la información de la Unidad de Transacciones, Pre despacho, datos de demanda inyecciones precios de mantenimiento combustibles.

En segundo lugar se maneja información como solicitudes, de mantenimiento (via FAX), reportes de fallo (impresos)

Toda la información del día anterior se proyectan día a día, toda la información está en base de datos oracle y en la página web de la UT.

La información del día anterior se toma como insumo para la del día siguiente.

Existe un control para esta información

Si se hace por medio de la página web de la UT y en las bases de dato oracle y SQL.

No está definida una política de control, solamente actualizaciones de la información, el 95% se actualizada en la base de datos vía Excel, se digita muy poco manual y se programa según la actualización de la data.

Quien controla toda o parte de la información

Los analistas de mercado son los encargados de controlar dicha información.

Como se controla

No hay controles definidos y los existentes son vulnerables, por ejemplo para controlar la información de la base de datos? Esto actualmente se hace por medio de detectar datos incoherentes por medio de intuiciones o irregularidades ya que la data posee pocas irregularidades.

No hay índices ni controles sistemáticos. Basta con apretar un botón para actualizar la data lo que la hace muy vulnerable.

Las personas que tienen acceso a la data son el director ejecutivo y los coordinadores.

Para la información física la secretaria tiene su sistema particular de archivos, los controles están en base de codificación y en base a listados de documentos, existen carpetas en las que guarda la información y se posee un fólder por cada documento.

Cada cuanto se controla

Diariamente.

Que beneficio trae el aplicar estos controles Si se posee la data actualizada y con controles debidos se hace mas fácil y oportuna la toma de decisiones, siendo esta oportuna y de una forma mas justificable y razonada. Se tiene un mejor análisis de la información.

Que impacto tiene el no controlar.

Retraso en el proceso de comercialización.

Duplicidad de datos.

Infidelidad de la información.

Impactos o pérdidas económicas.

INTEGRIDAD:

Quien manipula los documentos (durante el transporte y el proceso)

Las seis personas del área la manipulan pero en su mayoría la secretaria es la que la manipula físicamente, mucha información se encuentra en la data y no se puede manipular físicamente.

Quien autoriza y define las responsabilidades de manipulación

El jefe de la unidad lo autoriza, existen tareas rotativas que las ejecutan los analistas de mercado, así se hace por tradición, no importando si hay días festivos siempre hay una persona encargada de manipulación de la información.

Qué tipo de manipulación está autorizada a hacerse en esta área

En su mayoría son de monitoreo y algunas de modificaciones, para poder hacer modificación de datos tiene que existir una autorización del jefe de la Unidad,

Como se garantiza que el documento tenga únicamente alteraciones autorizadas

NO existen controles documentados.

Como se asegura en el almacenamiento del documento el acceso al personal autorizado.

Ya que solo existe una persona encarga y autorizada para hacer dicha tarea.

Que impacto genera una alteración no autorizada de la información.

Impactos de tipo económico, mal proceso de comercialización, mala toma de decisiones

AUTENTICIDAD:

Como se garantiza que la información suministrada es real y veraz

El mismo analista de mercado en el análisis de la información lo hace.

El 90% de la información de la data, la proporciona el usuario o el comprador, el analista detecta que la información sea confiable.

Como se respalda la información para su verificación: se hace a petición, autocontrol o como parte del proceso de emisión.

La verificación se hace como parte del análisis, Una gran parte de la información no se puede cotejar ya que es proporcionada por el usuario o el comprador, solo se puede verificar la correspondiente a la emitida por CEL como lo son los niveles de producción, los ingresos que se proyectan contra la facturaciones, existen formar de verificarla por ejemplo: si no hay rango de un 10 de desviación se puede filtrar o detectar inconsistencias.

Que impacto genera que la información no sea veraz o real.

Mal toma de decisiones, pérdidas económicas pues lo que se oferta es lo que se vende, si la red informática se cae se tiene planes contingenciales por medio de análisis históricos de ofertas.

DISPONIBILIDAD

Como llega la información (solicitud, o flujo de proceso)

La disponibilidad se encuentra en un 97 % y llega como parte del flujo de proceso, hay problemas cuando se cae la BD de la UT, las medidas alternativas son acceso vía modem o por la gprs, cuando el proveedor que es la UT esta en mantenimiento es decir cuando hay problemas de disponibilidad.

La información llega con los tiempos establecidos y oportunos.

La oferta se prepara día a día, en día de semana la demanda casi es la misma, depende del clima, en verano no hay problemas no hay mucho riesgo, se puede dar el lujo de programas día a día,

Es más crítico en invierno, porque llueve, y se puede desbalancear la producción, un desbalance en los niveles de los reservorios puede cambiar las producciones (es un impacto)

La información que necesita está disponible

En condiciones normales (70%) la base de datos de la estadística, no está sistematizada no tiene back up,

Que canales y medios se utiliza para el manejo de la información ¿son adecuados?

La información llega en su mayoría de manera electrónica, por medio de correos electrónicos, base de datos de la UT, intranet y físicamente por medio de fax.

Actualmente para la demanda los canales son los adecuados.

El personal autorizado al acceso de la información cuenta con la información cuando la requiere (esta área genera atrasos para poner la información a disposición de clientes)

Si ya que los horarios son generados en la UT y es independiente de la comisión, los atrasos son mínimos y existen planes contingenciales si se da algún retraso,

Que impacto o que dificultades le genera no disponer de la información necesaria en el tiempo preciso.

Puede originar pérdidas económicas pues se vende solamente lo ofertado y según la información de recibida por la UT, pueden tomarse malas decisiones y atrasos en el proceso de comercialización.

UTILIDAD

Como obtiene la información que necesita para desempeñar sus funciones (la obtiene por solicitud o como parte del flujo del proceso)

La información se obtiene como parte del proceso y se utiliza según horarios establecidos en el reglamento de la UT, por ejemplo, la oferta de los participantes a las 7 am. La liquidación de mercado entre las 9 y 11 am, el pre despacho se publica entre 4 y 6 pm , en casos extremos a las 8 pm.

Que volumen de información demanda para su uso

Los volúmenes son grandes, pero son fijos es decir no varían de un día para otro. Se manejan en bases de datos, físicamente es poca la información.

Utiliza toda la información que recibe, toda le es útil

Toda la información es importante pero no toda se utiliza,

Se pueden dividir en datos oficiales y no oficiales.

Entre los oficiales están los que se hacen mes a mes y generan los documentos de transacciones. Solo sirve para estadística y controles de contabilidad.

La información que es más útil es la no oficial.

Como la identifica si es útil o no

Si el proceso la requiere es útil, si no la requiere no es muy trascendental.

Qué porcentaje utiliza

95%

Con que frecuencia la utiliza

Diariamente

Que impacto positivo o negativo le genera el uso o mal uso de la información Positivos son muchos ya que a partir de dicha información se elabora la oferta, lo que CEL espera producir y así comercializarla, y negativas son muchas en su mayoría pérdida de tiempo de dinero y de toma de decisiones.

CONFIDENCIALIDAD

Manipulan información confidencial

Si se maneja.

En porcentaje representa del total de información manipulada

Es información proveniente de la UT y representa el 75% de la misma.

La data de la UT posee clave y solo entran las personas de dicha unidad, en lo q corresponde a CEL 70 u 80 % es lo confidencial de la UT, la información pública son los niveles de embalse, inyecciones a nivel global, producciones generales, ofertas pasadas.

Otros datos confidenciales son precios de facturación, cuanto producto cada estación, contratos, etc.

Dentro de la data de la UT hay tres tipos de información, la pública, publica restringida que la pueden ver los usuarios y la eminentemente privada por operadores.

El acceso a la información confidencial es solo de la persona o grupo autorizado para hacerlo

Así es solamente dichas personas están autorizadas para manejarlas, además de la dirección ejecutiva.

Existen contraseñas de navegación que solo la Unidad de comercialización posee.

Existen otras personas o grupos que accedan a la información

Si existen, además de dicha unidad la alta gerencia tiene acceso a dicha información.

Que medios se utilizan para el transporte de la información

Existen medios electrónicos y físicos.

De todo lo electrónico se hacen impresiones para control, cuando se trabaja con la liquidación.

Las ofertas se guardan en el servidor, en una maquina particular, se imprimen y se guardan en un fólder por cada día. Los informes de consumo no porque se mandan para cobro debidamente resguardado y sellado vía memo.

Existe la posibilidad que la información llegue a la persona incorrecta, antes, durante y después de proceso (transito o flujo)

Es muy poco probable ya que existen sistemas de correspondencia contra firma, claves de acceso, archivos ocultos.

Que impacto genera que la información llegue a las manos equivocadas

Desde el punto de vista comercial, los medios podrían dar un mal manejo político. Hay mucha información que si se escapa puede ser crítico, otro generadores pueden sacar ventaja por saber la oferta. Hay repercusiones políticas, económicas, etc.

Dentro de la misma CEL puede tener repercusiones, en la UT en hay cuatro precios, precio de MRS, de estabilización, etc. Precios de mercado.

Las proyecciones pueden sacar información inadecuada.

iii. Unidad Informática Institucional

GUÍA DE ENTREVISTA

Proceso: Gestión de la Información	**Fecha: 25/ nov/ 08**	**Hoja:**
Departamento o Área: Unidad de Informática Institucional		
Nombre del entrevistado: Licda. Nelly de Aguilar		
Cargo: Jefe de la Unidad		
Posee personal a su cargo: SI	**Cuantos: 15**	

CONTROL:

¿Qué tipo de información o documentos maneja?

Manuales de usuarios, términos de referencia, opiniones, normativas y políticas, la mayoría de información es electrónica, existe bajo volumen de papel.

También de poseen Registros de calidad.

Existe un control para esta información

Para los físicos se llevan controles de correspondencia, de recibido y de entregado, archiveros con llave,

Quien controla toda o parte de la información

El jefe de cada área controla toda la información de la Unidad, se cuenta con tres áreas.

Como se controla

Se validan los registros completos (autorizados) a través de firmas,

Cada cuanto se controla

De acuerdo a los indicadores es una vez cada mes, además de hacer monitoreos y verificación de registros a diario.

Que beneficio trae el aplicar estos controles

Se asegura que la información este completa, q proporcione confianza y se clasifica adecuadamente dando resultados oportunos.

Que impacto tiene el no controlar.

Acceso a personas no autorizadas, mala interpretación.

INTEGRIDAD:

Quien manipula los documentos (durante el transporte y el proceso)

Los documentos de baja importancia como los memos son manipulados por los ordenanzas, y la información delicada por el personal de la unidad.

Quien autoriza y define las responsabilidades de manipulación

El jefe de la Unidad.

Qué tipo de manipulación está autorizada a hacerse en esta área

Física y digital.

Como se garantiza que el documento tenga únicamente alteraciones autorizadas

Se valida por medio de firmas o en casos más especiales con una doble firma, no es una práctica frecuente pero de esa forma de hace.

Como se asegura en el almacenamiento del documento el acceso al personal autorizado

La estructura física todo el personal puede acceder, no hay medidas que regulen que otras dependencias puedan acceder a la información, no hay una política de restricción, en otros casos solo el jefe de la unidad posee las llaves o las contraseñas donde esta almacenada la información.

Que impacto genera una alteración no autorizada de la información.

Existen penalidades en el reglamento interno y depende del nivel o valor de la información así será su impacto

AUTENTICIDAD:

Como se garantiza que la información suministrada es real y veraz

Se garantiza verificando que las firmas sean originales ya que no se maneja la firma digital, también por medio de uso de sellos.

Como se respalda la información para su verificación: se hace a petición, autocontrol o como parte del proceso de emisión. Se digitaliza como autocontrol y por respaldo.

Que impacto genera que la información no sea veraz o real.

Decisiones inadecuadas.

DISPONIBILIDAD

Como llega la información (solicitud, o flujo de proceso)

Como parte del proceso y se atienden por orden de llegada.

La información llega con los tiempos establecidos y oportunos.

Si llega oportunamente a pesar de que no están registrados los tiempos de servicio ni de respuesta.

La información que necesita está disponible

Si está disponible muchas veces el proveedor es el que no está disponible.

Que canales y medios se utiliza para el manejo de la información ¿son adecuados?

Los indicados en el proceso los cuales son por el personal de la unidad, por intranet, por email, y de manera física.

El personal autorizado al acceso de la información cuenta con la información cuando la requiere (esta área genera atrasos para poner la información a disposición de clientes)

Si internamente, no hay retrasos al solicitar a otras dependencias.

Que impacto o que dificultades le genera no disponer de la información necesaria en el tiempo preciso.

No se pueden dar resultados oportunos, se pueden minimizar pero no se pueden eliminar del todo, algunas veces son inevitables los impactos.

UTILIDAD

Como obtiene la información que necesita para desempeñar sus funciones (la obtiene por solicitud o como parte del flujo del proceso) Como parte del proceso.

Que volumen de información demanda para su uso

Mucha de la información solo se proceso, la unidad no produce mayor información.

Utiliza toda la información que recibe, toda le es útil

Si, ya que se procesa para que otras dependencias la utilicen

Como la identifica si es útil o no

Con el proceso de depuración y eliminación y también que si es solicitada continuamente por las dependencias quiere decir que si es útil.

Qué porcentaje utiliza

El 100%

Con que frecuencia la utiliza

Diariamente

Que impacto positivo o negativo le genera el uso o mal uso de la información

Se pueden mal interpretar y generar mal entendidos, pueden no apegarse a la realidad.

CONFIDENCIALIDAD

Manipulan información confidencial

Si, por ser unidad de servicios informáticos, se manejan muchas bases de datos, redes, planillas, tesorería, etc.

En porcentaje representa del total de información manipulada

No se puede precisar pero aproximadamente el 60%

El acceso a la información confidencial es solo de la persona o grupo autorizado para hacerlo

Si solamente ellos, se garantiza a través de perfiles de usuario y roles de acceso (PRA 17-17)

Existen otras personas o grupos que accedan a la información

Cada persona es responsable de la información y solo acceden las personas de la Unidad.

Que medios se utilizan para el transporte de la información

Correspondencia sellada y entregada personalmente, email, intranet con llaves.

Existe la posibilidad que la información llegue a la persona incorrecta, antes, durante y después de proceso (transito o flujo)

Si existe la posibilidad por errores humanos.

Que impacto genera que la información llegue a las manos equivocadas

Violación a la confidencialidad, se puede generar fuga de datos y pérdidas de información.

iv. Unidad de Desarrollo Humano

GUÍA DE ENTREVISTA

Proceso: Recursos Humanos	**Fecha: 27/nov/2008**	**Hoja:**
Departamento o Área: Unidad de Desarrollo Humano.		
Nombre del entrevistado: Licda. Elena de Urquilla.		
Cargo: Jefe de Unidad de Recursos Humanos.		
Posee personal a su cargo: Si	**Cuantos: 19**	

CONTROL:

¿Qué tipo de información o documentos maneja?

Se manejan documentos en copia dura, en medios electrónicos, Se manejan hojas de vida con sus documentos anexos, ofertas de servicio, Bases de datos de currículo electrónicos y físicos; Test psicológicos y sus reportes, hay un software de test de pruebas psicológicas, pruebas de conocimientos y se manejan en archivos electrónicos y en físico en el expediente respectivo, en contratación hay propuestas y notificaciones de contratación de manera física. Hay muchos formularios que se manejan ahí. Reportes de entrevistas, se imprimen memorando, recomendaciones, tablas comparativas. Es un expediente de candidato seleccionado y contratado. Luego el presidente lo acepta y se le suma el contrato individual de trabajo, un registro de inducción, se generan formularios de evaluación de desempeño anual por cada empleado, son 495 formularios en físico y se genera un consolidado, el resumen de la evaluación se genera en físico, y reportes estadísticos, a pesar de que el sistema esta mecanizado a la vez este genera reportes físicos.

El manual de descripción de puestos es un documento físico y de manera electrónica

Las acciones de personal comprende ascensos incrementos salariales, traslados, licencias con o sin goce de suelda, renuncias, amonestaciones, terminaciones de contrato, cualquier cambio que modifique el empleado, se reciben requerimientos en físico (solicitudes) por correo y por memo y si viene en internet se imprime para que las apruebe el director ejecutivo. Y luego se genera una propuesta, he ahí que existen dos documentos y requerimientos y aprobaciones, luego se hace una reforma al contrato laboral, todo incluye información personal del trabajador, todo es muy confidencial, se lleva un expediente individual por cada trabajador, y también en el sistema de recursos humanos.

Antes eran 3000 empleados ahora 496 o 498 empleados.

Existe un control para esta información

Todos los documentos están declarados en el sistema de gestión como registros de calidad, todos los procesos poseen los RC, los registros de calidad, existe control mecanizado numerando los documentos, se controla en un registro numérico ordenado ascendente, de asigna un código correlativo, cada requerimiento lleva una numeración actualmente es físico y se pretende mecanizarlo, existen 3 puntos de control, uno cuando el analista presenta la propuesta y anexa el expediente otro cuando se verifica otra vez y al final la encargada de archivar todos los documentos en el expediente revisa por última vez que vaya todo de acuerdo a la normativa de contratación, si falta algo se avisa al analista responsable para que lo complete. Existen 5 analistas

Quien controla toda o parte de la información

Los jefes de la Unidad, los analistas responsables, y los archivadores y/o colaboradores.

Como se controla

Se controlan con los registros de calidad, códigos y firmas, Existen barreras y permisos delimitados en los sistemas mecanizados.

Cada cuanto se controla

Se controla de manera continua.

Que beneficio trae el aplicar estos controles

Lograr confidencialidad en los procesos, confianza, eficiencia el trabajo, optimización de tiempos, seguridad de la información.

Que impacto tiene el no controlar.

Deficiencias en las auditorias, malos resultados en el trabajo, perdidas de información, etc.

INTEGRIDAD:

Quien manipula los documentos (durante el transporte y el proceso)

La manipula el personal que está dentro del proceso y esas mismas personas son las que la manipulan en el proceso. Cada empleado es responsable de manipular sus documentos y en algunos casos los ordenanzas.

Quien autoriza y define las responsabilidades de manipulación La responsable es la Licda. Irma Elena tanto en información física y electrónica, en el manual se establece las responsabilidades y que información puede manejar, cada uno está delimitado por sus funciones.

Qué tipo de manipulación está autorizada a hacerse en esta área

Modificaciones, actualizaciones, conteo de horas extras, contratos, solicitudes, en fin todas las definidas según los procedimientos de acción.

Como se garantiza que el documento tenga únicamente alteraciones autorizadas

Porque todo lo que se genera se valida con una firma, todo los reportes, requisiciones inscripciones, todas las prestaciones se autorizan por la Jefa de la Unidad

Como se asegura en el almacenamiento del documento el acceso al personal autorizado

Existe una normativa para poder almacenar todos los expedientes, y dicha normativa define que persona tiene acceso a la misma, si esa persona no está autorizada se procede a generar una aprobación por la Licda. Existen personas delegadas para administrar las nominas y las planillas, eso está dicho entre sus funciones, siempre se aprueba por medio de un listado a las personas que no están autorizadas para que así puedan tener acceso a la información.

El mismo personal transporta los documentos y en ocasiones se cuanta con el apoyo de los ordenanzas.

Toda acción de personal se maneja en sobe sellado, por ser confidencial. Es un criterio de confidencialidad.

Que impacto genera una alteración no autorizada de la información.

Se corre el riesgo de mal uso de los datos, datos del empleado son confidenciales, se puede caer en chambres, entra mucho en juego la práctica de valores.

.AUTENTICIDAD:

Como se garantiza que la información suministrada es real y veraz

Existen varios filtros para garantizar la veracidad, uno es el que la Jefe los revisa, otro el sistema de información tanto electrónico como físico, a la vez todo se verifica con respaldos.

Como se respalda la información para su verificación: se hace a petición, autocontrol o como parte del proceso de emisión.

Se hace como parte del procedimiento y como autocontrol (lo respalda en físico y en digital)

Que impacto genera que la información no sea veraz o real.

Se pierde la legalidad del documento, existe un reglamento interno y códigos internos que penalizan al personal si cometen una falsificación o manipulación de información.

DISPONIBILIDAD

Como llega la información (solicitud, o flujo de proceso)

De ambas formas, vienen requerimientos formales, pueden entrar por las dos vías

La información llega con los tiempos establecidos y oportunos.

Siempre hay casos extemporáneos, aun así por ser unidad de servicio al cliente externo somos de apoyo, se reciben pero se aclara que será con las medidas pertinentes, se trabaja por ser oportunos pero hay casos que externos y es ahí donde se dan los atrasos.

La información que necesita está disponible

Siempre está disponible, Pudieran darse atrasos pero no sean son 100% imputables a ellos.

Que canales y medios se utiliza para el manejo de la información ¿son adecuados?

Vía correo electrónico, intranet, físicamente, por medio de carretillas,

El personal autorizado al acceso de la información cuenta con la información cuando la requiere (esta área genera atrasos para poner la información a disposición de clientes)

Si suceden atrasos por veces, debido a fuerzas externas a la Unidad por ejemplo planillas o procesos de declaración de renta, siempre hay una justificación del proceso con un apartado que dice "no está generado o aun está en proceso".

Que impacto o que dificultades le genera no disponer de la información necesaria en el tiempo preciso.

Incumplimiento de los tiempos establecidos en el procedimiento, incumplimiento en las condiciones contractuales del trabajador, incumplimiento de la legalidad en el plan de pagos en planillas.

UTILIDAD

Como obtiene la información que necesita para desempeñar sus funciones (la obtiene por solicitud o como parte del flujo del proceso)

De ambas maneras.

Que volumen de información demanda para su uso

No se tiene definido son alrededor de 10 archivadores con su capacidad al máximo, además de gran cantidad de microfilms,

Utiliza toda la información que recibe, toda le es útil

En su mayoría es útil hay información que se procesa a diario y hay otro tipo de información que es histórica y solo sirve de referencia.

Como la identifica si es útil o no

Al revisarla y verificarla como parte del proceso.

Qué porcentaje utiliza

Al 100%

Con que frecuencia la utiliza

Diariamente.

Que impacto positivo o negativo le genera el uso o mal uso de la información

No proveer servicio a la comisión, si no se evacua el requerimiento no se podrá proveer a la dependencia o al empleado, se generan reclamos, se pueden crear perjuicios al empleado o incumplimientos a los derechos del empleado, no proveer de recurso adecuado al departamento.

CONFIDENCIALIDAD

Manipulan información confidencial

Si se maneja.

En porcentaje representa del total de información manipulada

El 90% es confidencial, y el 10% es de uso público

El acceso a la información confidencial es solo de la persona o grupo autorizado para hacerlo

Es solo para el personal de dicha Unidad y personas de alta gerencia.

Existen otras personas o grupos que accedan a la información

Que medios se utilizan para el transporte de la información

En sobre sellado y es transportado por la Jefa de la Unidad,

Existe la posibilidad que la información llegue a la persona incorrecta, antes, durante y después de proceso (transito o flujo)

Si puede darse dicha situación, pero se posee el recurso de que toda persona es responsable de la información que traslada o emite hasta ser evacuada por el mismo de buena manera.

Que impacto genera que la información llegue a las manos equivocadas

Incumplimientos, despidos por divulgación de información, publicar información para crear mala imagen a la comisión y existir señalamientos y malos entendidos, el mal uso puede afectar a título personal a cada empleado. Pueden generarse despidos o amonestaciones, y repercusiones legales hay documentos que son de trámites legales bien delimitados.

ANEXO 12: ENFOQUE BASADO EN PROCESOS Y EL CICLO PHVA APLICADOS AL SGSI

A. ENFOQUE BASADO EN PROCESOS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

1. Principio del Enfoque por Procesos

"Los resultados deseados se alcanzan más eficientemente cuando los recursos y las actividades relacionadas se gestionan como un proceso" (Norma ISO 9000)

En el apartado 0.2 de la parte introductoria de la Norma ISO 27001:2005, se promueve la adopción de un *enfoque basado en procesos* para el Sistema de Gestión de Seguridad de la Información, que tiene como objetivo aumentar la satisfacción del cliente mediante el cumplimiento de sus requisitos, tal y como se muestra a continuación.

4.2 Enfoque Basado en Procesos [32]

Esta Norma Internacional promueve la adopción de un enfoque basado en procesos durante el desarrollo, implementación y mejoramiento de la eficacia de un Sistema de Administración de Seguridad de Información.

Para que una organización funcione de manera eficaz, tiene que identificar y gestionar numerosas actividades relacionadas entre sí. Una actividad que utiliza recursos, y que se gestiona con el fin de permitir que los elementos de entrada se transformen en resultados es un proceso. Frecuentemente su resultado constituye directamente el elemento de otro proceso.
La aplicación de un sistema de procesos dentro de la organización, junto con la identificación e interacciones de estos procesos, así como su gestión, puede denominarse como ***"enfoque basado en procesos".***

Una ventaja del enfoque basado en procesos es el control continuo que proporciona sobre los vínculos entre los procesos individuales dentro del sistema, así como sobre su combinación e interacción.

[32] Tomado del Libro: "La Gestión por Procesos, su papel e importancia dentro de la Empresa"; Autor: J. R. Zaratiegui; pág. 41

Cuando un enfoque de este tipo se utiliza para la Administración de Seguridad de Información, enfatiza la importancia de:

a) La comprensión por parte de la organización de sus requerimientos de Seguridad de la Información y su necesidad de establecer una política y objetivos para garantizar la Seguridad de la Información.
b) La implementación y operación de controles para administrar los riesgos inherentes a la Seguridad de la Información de la empresa en concordancia con los riesgos del negocio.
c) El monitoreo y revisión del desempeño y la efectividad del sistema.
d) La mejora continua de los procesos con base en mediciones objetivas.

2. Entendiendo el Enfoque basado en procesos.

Los procesos se consideran actualmente como la base operativa de gran parte de las organizaciones y gradualmente se van convirtiendo en la base estructural de un número creciente de empresas.
Esto dio origen a estudios sobre las posibilidades de los procesos como base de gestión de la empresa, que fueron poniendo de manifiesto su adecuación a los mercados actuales, cada vez más cerca del mercado global y, como consecuencia, *su capacidad* de contribuir de forma sostenida a los resultados, siempre que la empresa diseñe y estructure sus procesos pensando en sus clientes.

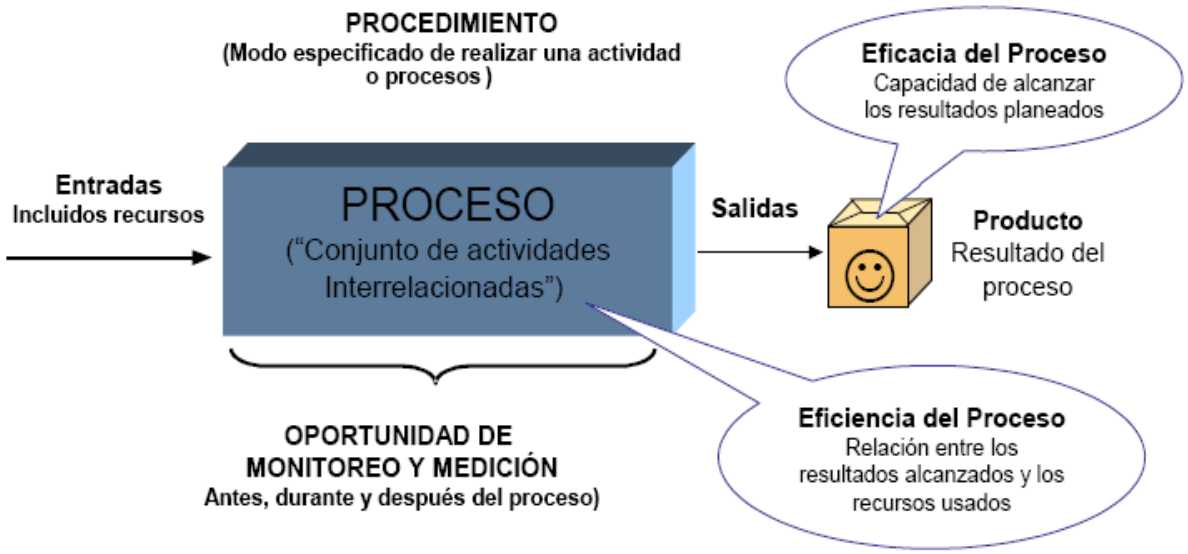
a) Definición de proceso.

La palabra proceso viene del latín *processus,* que significa avance y progreso.
Los procesos, en este contexto, se pueden definir como: Secuencias ordenadas y lógicas de actividades de transformación, que parten de unas entradas, (input) (informaciones en un sentido amplio —*pedidos datos, especificaciones*—, más medios materiales —*máquinas, equipos, materias primas, consumibles, etcétera*) —, para alcanzar unos resultados programados, (output) que se entregan a quienes los han solicitado, los clientes de cada proceso.[33]
Otra ***definición de Proceso:*** Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.[34]

[33] Tomado del Libro: "La Gestión por Procesos, su papel e importancia dentro de la Empresa"; Autor: J. R. Zaratiegui; pág. 82.

[34] Tomado del documento ISO "Orientación sobre el concepto y uso del Enfoque basado en Procesos para los sistemas de gestión", elaborado por ISO/TC 176/SC. Mayo 2004, pág. 3.

Esquema de Proceso.



b) Características del proceso.

1. Las entradas para un proceso son generalmente salidas de otros procesos
2. Los procesos de una organización son generalmente planificados y puestos en práctica bajo condiciones controladas para aportar valor.

Los elementos de entrada y los resultados previstos pueden ser tangibles (tal como equipos, materiales o componentes) o intangibles (tal como energía o información).
Los resultados también pueden ser no intencionados; tales como el desperdicio o la contaminación ambiental.
Cada proceso tiene clientes y otras partes interesadas (quienes pueden ser internos o externos a la organización) que son afectados por el proceso y quienes definen los resultados requeridos de acuerdo con sus necesidades y expectativas.
Debería utilizarse un sistema para recopilar datos, los cuales pueden analizarse para proveer información sobre el desempeño del proceso, y determinar la necesidad de acciones correctivas o de mejora.
Todos los procesos deberían estar alineados con los objetivos de la organización y diseñarse para aportar valor, teniendo en cuenta el alcance y la complejidad de la organización.
La eficacia y eficiencia del proceso pueden evaluarse a través de procesos de revisión internos o externos.

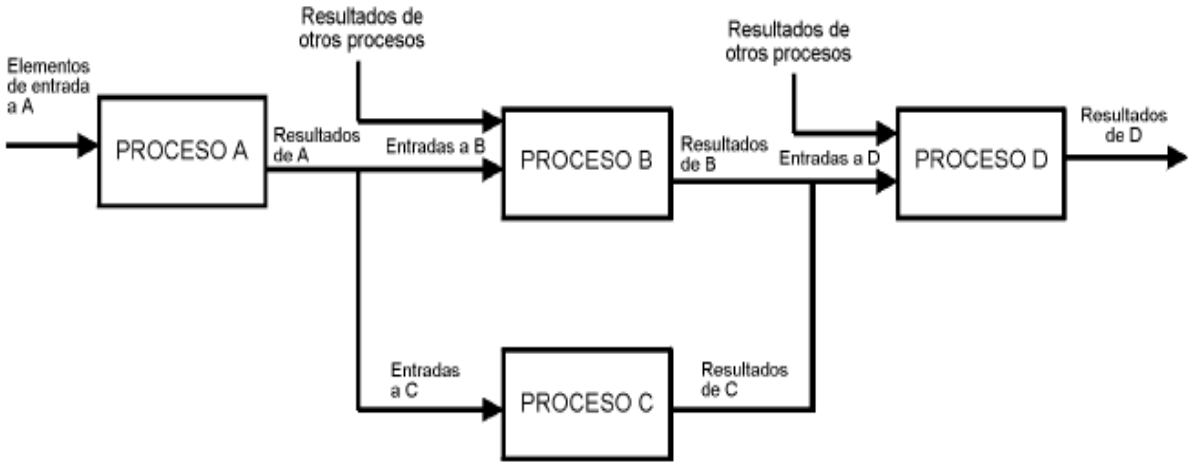
3. Tipos de procesos

Pueden identificarse los siguientes tipos de procesos:

- ***Procesos para la gestión de una organización.*** Incluyen procesos relativos a la planificación estratégica, establecimiento de políticas, fijación de objetivos, provisión de comunicación, aseguramiento de la disponibilidad de recursos necesarios y revisiones por la dirección.
- ***Procesos para la gestión de recursos.*** Incluyen todos aquellos procesos para la provisión de los recursos que son necesarios en los procesos para la gestión de una organización, la realización y la medición.
- ***Procesos de realización.*** Incluyen todos los procesos que proporcionan el resultado previsto por la organización.
- ***Procesos de medición, análisis y mejora.*** Incluyen aquellos procesos necesarios para medir y recopilar datos para realizar el análisis del desempeño y la mejora de la eficacia y la eficiencia. Incluyen procesos de medición, seguimiento y auditoría, acciones correctivas y preventivas, y son una parte integral de los procesos de gestión, gestión de los recursos y realización.

4. Relación entre procesos.

Los resultados de un proceso pueden ser elementos de entrada para otros procesos y estar interrelacionados dentro de la red global o sistema global, así:



Ejemplo de una secuencia de un proceso genérico

Así mismo estos procesos interactúan dentro de un sistema de procesos donde se interrelacionan los el resto de los procesos, en el siguiente esquema se puede visualizar la relación entre los diferentes tipos de procesos (estratégicos, de realización, de apoyo o de recursos y de medición, análisis y mejora):

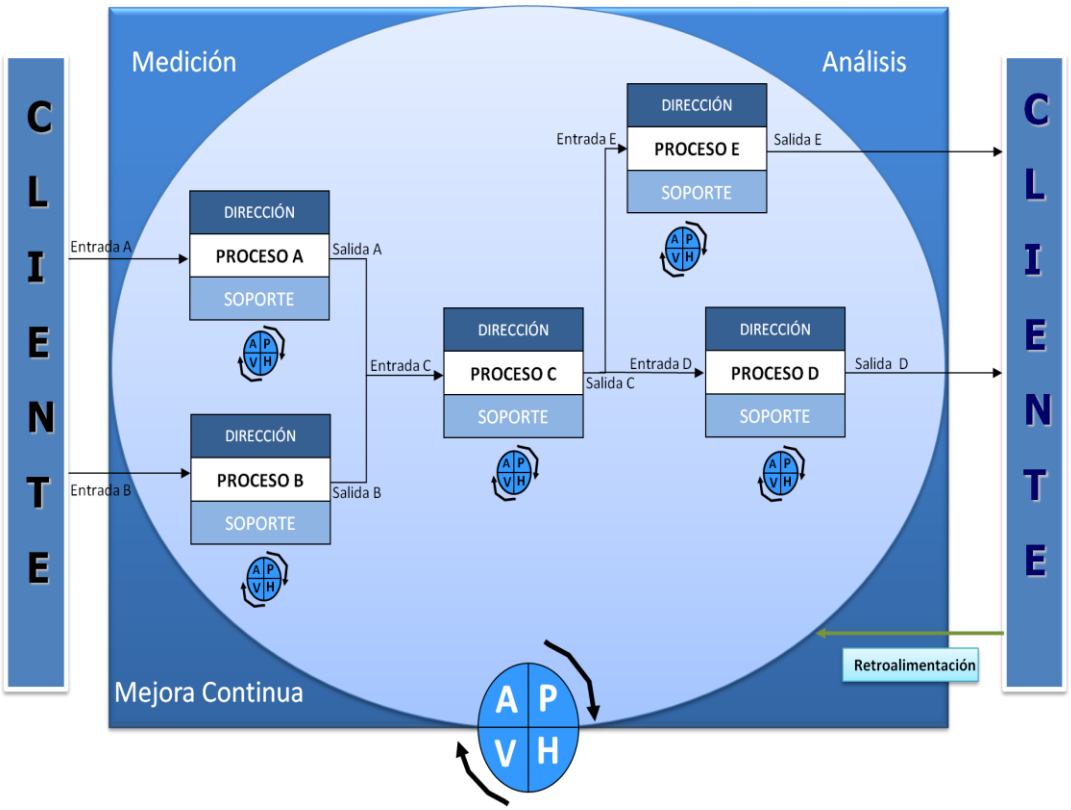
Las interacciones entre los procesos de una organización frecuentemente pueden ser complejas, resultando en una red de procesos interdependientes.

La entrada y salida de estos procesos frecuentemente pueden estar relacionadas tanto con los clientes externos como con los internos.

En la Figura siguiente se muestra un ejemplo de una red de procesos que interactúan. El modelo de la red de procesos ilustra que los clientes juegan un papel significativo en la definición de requisitos como elementos de entrada.

La retroalimentación de la satisfacción o insatisfacción del cliente por los resultados del proceso es un elemento de entrada esencial para el proceso de mejora continua del SGSI.

Red de procesos que interactúan.



Bajo este marco de referencia se puede definir el concepto de ***Enfoque basado en Procesos.***

5. Enfoque Basado en Procesos.

"La gestión por procesos (*Business Process Management*) es una forma de organización diferente de la clásica organización funcional, y en el que prima la visión del cliente sobre las actividades de la organización. Los procesos así definidos son gestionados de modo estructurado y sobre su mejora se basa la de la propia organización."[35]

Otra definición de Enfoque basado en Procesos:

"Es una forma de conducir o administrar efectivamente las actividades, interrelaciones y recursos de una organización concentrándose en el valor agregado para el cliente y las partes interesadas."[36]

El enfoque basado en procesos introduce la gestión horizontal, cruzando las barreras entre diferentes unidades funcionales y unificando sus enfoques hacia las metas principales de la organización. También mejora la gestión de las interfaces del proceso.

El desempeño de una organización puede mejorarse a través del uso del enfoque basado en procesos. Los procesos se gestionan como un sistema, mediante la creación y entendimiento de una red de procesos y sus interacciones.

La gestión de procesos aporta una visión y unas herramientas con las que se puede mejorar y rediseñar el flujo de trabajo para hacerlo más eficiente y adaptado a las necesidades de los clientes. No hay que olvidar que los procesos lo realizan personas y los productos los reciben personas, y por tanto, hay que tener en cuenta en todo momento las relaciones entre proveedores y clientes.

6. Ventajas del Enfoque por Procesos.

Proporciona a la dirección de la organización:

1. Una visión integrada de las actividades que la empresa/organización necesita para cumplir sus obligaciones ante el mercado.
2. Una ayuda imprescindible para planificar nuevas estrategias o el despliegue de nuevas políticas. Este aspecto se hace especialmente relevante cuando la innovación (tecnológica o de reingeniería) tiene un papel destacado en esas nuevas políticas.

[35] Tomado del documento: "La Gestión por Procesos", Universidad de Toledo, España.

[36] Tomado del documento: "Sistemas de Gestión con Enfoque por Procesos" por la escuela de Ingeniería de Antioquia.

- **¿Por qué la Gestión por Procesos?**

1. Existen cambios en las expectativas y necesidades del *cliente haciéndose cada día más exigente.* (Mercados más desarrollados, clientes con mas conocimiento y sobreoferta en mercados globalizados)
2. *Necesidad de eficiencia* en las organizaciones (Entorno de elevada competencia que exige mayor control de costos)
3. *Estructuras que no se adaptan* a las necesidades de la organización.

Gráficamente se puede describir el Enfoque por Procesos basado en el ciclo PHVA de la forma siguiente:

B. EL CICLO PDCA Y EL ENFOQUE BASADO EN PROCESOS

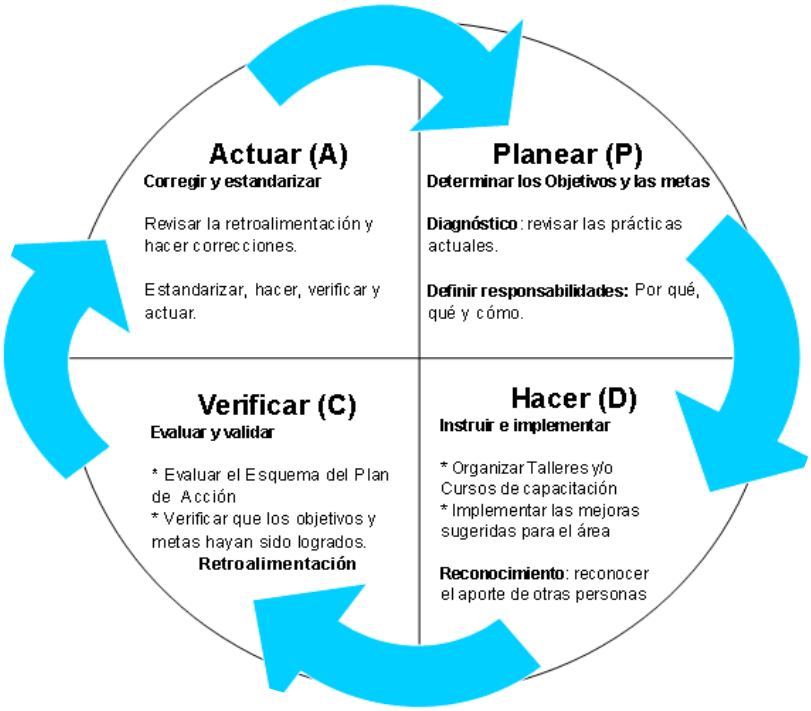
Las siglas "PDCA", tiene como significado al idioma inglés: "PLAN, DO, CHECK and ACT"; palabras que a su vez se traducen al idioma español como: "PLANIFICAR, HACER, VERIFICAR Y ACTUAR",
El ciclo "PDCA" de las normar ISO 27000 no es más que una representación fiel del denominado ciclo de Deming, el cual lleva por nombre en el idioma español ciclo "PHVA" que significa: "PLANEAR, HACER, VERIFICAR Y ACTUAR", ciclo desarrollado inicialmente en la década de 1920 por el Dr. Walter A. Shewhart en los Laboratorios Bell, de Western Electric en Cleveland, Ohio, Estados Unidos, y que fue popularizado luego por el Dr. W. Edwards Deming; es por esa razón que frecuentemente se le llama ciclo de Deming.

En el vocabulario utilizado a lo largo del desarrollo de los términos y definiciones de la serie de Normas ISO 27000 como parte del proceso de adaptación de las mismas al idioma español, se han utilizado palabras sinónimas a las originales, que describen más ampliamente el ciclo "PDCA" o ciclo "PHVA" esta traducción es la siguiente: "PLANIFICAR, IMPLEMENTAR, SEGUIMIENTO Y MEJORA CONTINUA".

En el contexto de la aplicación de la Norma ISO 27001, y conociendo el valor que tienen los procesos para las organización ya que en estos se encuentra la fuerza productiva de la mismas, es allí donde la participación activa del ciclo PHVA dinamiza la ejecución de esos procesos, en este sentido y por la naturaleza misma del ciclo PHVA éste es aplicable a todos los procesos individuales dentro de la empresa, así como al sistema de procesos que conforma la misma empresa.
Es decir, la aplicación del ciclo PHVA tiene la capacidad de hacer funcionable cada proceso sumergiéndolo en una dinámica de mejora continua, este mismo efecto se potencializa en el sistema de procesos que opera a toda la organización.

El ciclo PHVA tiene la capacidad de ver a la organización como un todo.

Ciclo "Planificar, Hacer, Verificar y Actuar":



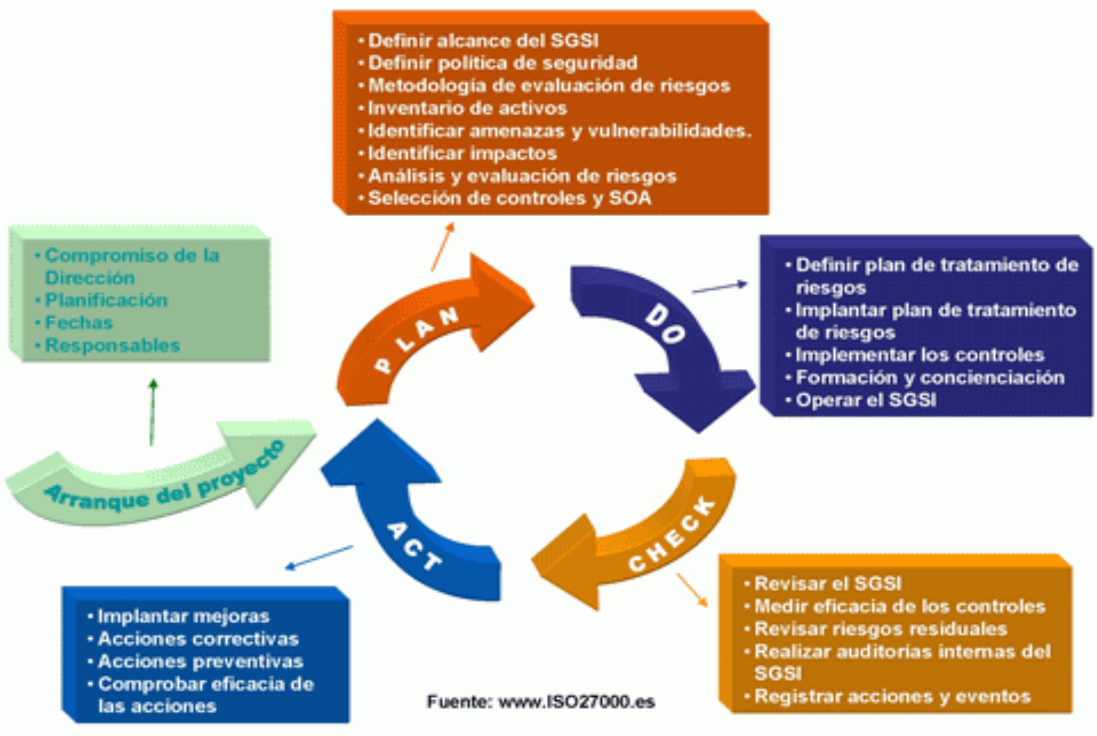
Esta representación grafica ayuda a comprender con más claridad los términos específicos que comprenden cada una de las etapas del ciclo, encontrando en cada apartado del ciclo procedimientos que indican ***"el como hacer"*** cada etapa; estos procedimientos se desagregan de un ya establecido proceso que indica ***"el que hacer".***

En el apartado 0.2 de la parte introductoria de la Norma ISO 27001, describe mediante un cuadro la aplicación del ciclo PHVA en los procesos del SGSI.

4. Descripción de la aplicación del ciclo PHVA como parte del SGSI

Planear (Establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (Implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.
Verificar (Monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Ciclo "Planificar, Implementar, seguimiento y Mejora Continua" según ISO 27000:



5. Etapas del ciclo PHVA aplicadas al SGSI

a) Arranque del Proyecto

- ***Compromiso de la Dirección:*** una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la organización. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.
- ***Planificación, fechas, responsables:*** como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

b) Requisitos de la etapa de Planificación

- ***Definir alcance del SGSI:*** en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado.
- ***Definir política de seguridad:*** que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección, por lo que no pasará de dos o tres páginas.

- ***Definir el enfoque de evaluación de riesgos:*** definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente se deberá, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla (en el futuro, ISO 27005 proporcionará ayuda en este sentido). El riesgo nunca es totalmente eliminable –ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.
- ***Inventario de activos:*** todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
- ***Identificar amenazas y vulnerabilidades:*** todas las que afectan a los activos del inventario.
- ***Identificar los impactos:*** los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- ***Análisis y evaluación de los riesgos:*** evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.
- ***Identificar y evaluar opciones para el tratamiento del riesgo:*** el riesgo puede reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).
- ***Selección de controles:*** seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.
- ***Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI:*** hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).
- ***Confeccionar una Declaración de Aplicabilidad:*** la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

c) Requisitos de la etapa de Implementación

- ***Definir plan de tratamiento de riesgos:*** que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- ***Implantar plan de tratamiento de riesgos:*** con la meta de alcanzar los objetivos de control identificados.
- ***Implementar los controles:*** todos los que se seleccionaron en la fase anterior.

- ***Formación y concienciación:*** de todo el personal en lo relativo a la seguridad de la información.
- ***Desarrollo del marco normativo necesario:*** normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

d) Requisitos de la etapa de Seguimiento

- ***Ejecutar procedimientos y controles de monitorización y revisión:*** para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
- ***Revisar regularmente la eficacia del SGSI:*** en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.
- ***Medir la eficacia de los controles:*** para verificar que se cumple con los requisitos de seguridad.
- ***Revisar regularmente la evaluación de riesgos:*** los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.
- ***Realizar regularmente auditorías internas:*** para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.
- ***Revisar regularmente el SGSI por parte de la Dirección:*** para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.
- ***Actualizar planes de seguridad:*** teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

e) Requisitos de la etapa de Mejora continúa

- ***Implantar mejoras:*** poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- ***Acciones correctivas:*** para solucionar no conformidades detectadas.
- ***Acciones preventivas:*** para prevenir potenciales no conformidades.
- ***Comunicar las acciones y mejoras:*** a todos los interesados y con el nivel adecuado de detalle.

- ***Asegurarse de que las mejoras alcanzan los objetivos pretendidos:*** la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

6. Modelo PHVA como enfoque de procesos aplicado al SGSI

El esquema que se muestra a continuación ilustra el Sistema de Gestión de Seguridad de la Información basado en el enfoque de procesos descrito en la norma ISO 27000.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

ISO 27000 adopta el modelo ***"Planear-Hacer-Verificar-Actuar"***, el cual es aplicado en todos los procesos del sistema. La figura muestra como el Sistema de Gestión de la Seguridad de la Información toma como insumos los requerimientos en materia de Seguridad de la Información así como las expectativas de las partes interesadas para a través de las acciones necesarias, producir como salida elementos de Seguridad de la Información que satisfacen los requerimientos y expectativas de la empresa.

De la figura anterior, también debemos destacar la entrada al Sistema de Gestión, que no es otra cosa que los Requisitos y Objetivos para el SGSI. Estos los debe definir la organización antes de empezar la implementación del SGSI.

:

ANEXO 13: PRUEBA PILOTO DEL ANÁLISIS Y EVALUACIÓN DEL RIESGO

➢ ANÁLISIS DEL RIESGO

En la siguiente tabla se demuestra el método que se utilizo para calcular el riesgo en la comisión.

RIESGO		FACTORES DEL RIESGO		MEDICIÓN DEL RIESGO	PRIORIZACIÓN DEL RIESGO
Activos de información	Amenaza	impacto de la amenaza	probabilidad de ocurrencia		
Base de datos clientes	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	50%	80%	40%	1
Base de datos de empleados	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	50%	80%	40%	1
Base de datos financieras	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	50%	80%	40%	1
Base de datos de producción	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	50%	80%	40%	1
Base de datos proveedores	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	50%	80%	40%	1
Equipo de computo	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	95%	20%	19%	2
Internet	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	80%	50%	40%	1
Servicio de archivos	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.	50%	10%	5%	5
Copias de respaldo	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.	50%	10%	5%	5
Líneas telefónicas	Amenazas naturales como Terremotos	50%	10%	5%	5
Cámaras	Amenazas naturales como Terremotos	20%	10%	2%	6
Correspondencia interna	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	80%	20%	16%	3
Correspondencia externa	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	80%	20%	16%	3
Información intelectual	Amenazas humanas como huelgas, epidemias, perdidas de personal clave	80%	10%	8%	5
Correos electrónicos	Amenazas tecnológicas como virus, hacking, fallas de	50%	80%	40%	5

RIESGO		FACTORES DEL RIESGO		MEDICIÓN DEL RIESGO	PRIORIZACIÓN DEL RIESGO
Activos de información	Amenaza	impacto de la amenaza	probabilidad de ocurrencia		
	software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones				
Intranet	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	50%	80%	40%	1
Documentos en papel impreso	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.	80%	10%	8%	5
Documentos en medio digital	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	50%	80%	40%	1
Manuales de usuarios,	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.	80%	10%	8%	5
Documentos legales	Amenazas operacionales como crisis financieras, aspectos regulatorios	80%	20%	16%	3
Software de sistemas	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	80%	20%	16%	3

Una vez calculada la medición del riesgo (multiplicando los valores obtenidos del impacto de la amenaza y la probabilidad de ocurrencia), se procede a priorizar en orden, con base en su factor de exposición del riesgo. En una escala del 1 al 6, representado los riesgos con prioridad 1, 2 y 3 los de mayor peligrosidad para CEL (ver ISO 27001:2005 4.2.1 (e)).

- **EVALUACIÓN DEL RIESGO**

Una vez efectuado el cálculo del riesgo por cada activo, en relación con su amenaza, se debe determinar cuales son aquellas amenazas cuyos riesgos son los mas significativos. A todo este proceso se le denomina evaluación del riesgo.

TOTAL = ((Impacto económico del riesgo) x (Tiempo de recuperación) x (Probabilidad de ocurrencia del riesgo) x (Probabilidad de interrumpir las actividades)) / 100

RIESGO		CRITERIOS PARA EVALUAR LA IMPORTANCIA DEL RIESGO				
Activos de información	**Amenaza**	**Impacto económico del riesgo**	**Tiempo de recuperación**	**Probabilidad de ocurrencia del riesgo**	**Probabilidad de interrumpir las actividades**	**TOTAL**
Base de datos clientes	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	4	4	40%	50%	3.2
Base de datos de empleados	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	3	4	40%	50%	2.4
Base de datos financieras	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	4	3	40%	80%	3.8
Base de datos de producción	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	4	3	40%	50%	3.8
Base de datos proveedores	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	3	4	40%	50%	3.8
Equipo de computo	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	3	4	19%	50%	1.14
Internet	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	3	2	40%	50%	1.2
Servicio de archivos	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.	3	3	5%	50%	0.2
Copias de respaldo	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.	2	5	5%	20%	0.1
Líneas telefónicas	Amenazas naturales como Terremotos	3	3	5%	80%	0.4
Cámaras	Amenazas naturales como Terremotos	3	3	2%	50%	0.1
Correspondencia interna	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	2	3	16%	50%	0.5
Correspondencia externa	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	2	2	16%	10%	0.06
Información intelectual	Amenazas humanas como huelgas,	4	4	8%	95%	1.2

RIESGO		CRITERIOS PARA EVALUAR LA IMPORTANCIA DEL RIESGO				
	epidemias, perdidas de personal clave					
Correos electrónicos	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	3	2	40%	50%	1.2
Intranet	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	4	3	40%	50%	2.4
Documentos en papel impreso	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.	3	2	8%	50%	0.3
Documentos en medio digital	Amenazas tecnológicas como virus, hacking, fallas de software y hardware, perdidas de datos, fallas en líneas telefónicas y falsificaciones	3	4	40%	50%	2.4
Manuales de usuarios,	Amenazas sociales como motines, protestas, vandalismo, violencia laboral.	2	3	8%	50%	0.2
Documentos legales	Amenazas operacionales como crisis financieras, aspectos regulatorios	5	4	16%	50%	1.6
Software de sistemas	Amenazas a las instalaciones como Incendios, explosiones, caídas de energía, perdidas de acceso	5	3	16%	80%	1.95

Si el puntaje total de los criterios para la importancia del riesgo es menor que 1.0 se define un nivel de riesgo aceptable, para valores mayores o iguales de 1.0 se define que los riesgos son de relevancia para La Comisión por lo que se deberán tomar en cuenta para la elaboración del plan de tratamiento de riesgos.

ANEXO 14: RESUMEN EJECUTIVO DE LA EVALUACION ECONOMICA FINANCIERA

Costos de inversión

COSTO DE INVERSIÓN	
RUBRO	COSTO
Costos de Capacitación a las Autoridades de CEL	$ 577.4
Costos de Capacitación al personal de las aéreas involucradas	$6,672.0
Costo de Equipo, materiales, servicios e instalaciones	$30,205
Costo de Documentación	$560.24
Costos del Sistema de Información Gerencial	$ 480.0
Costos de la estructura organizativa de la Administración del proyecto	$ 38,557.5
Costos de la Certificación	$ 27,830
TOTAL	**$ 104,882.14**

Costos operativos

COSTOS DE OPERACIÓN	
RUBRO	COSTO ANUAL
Costo de Formularios del Sistema	$ 50.0
Costo de Equipo de Protección Personal	$80,424.00
TOTAL	**$80,474.0**

Beneficios esperados de acuerdo a la reducción de pérdidas

Año	% esperado de Reducción de perdidas	Pérdidas promedio ocasionadas por el mal manejo y falta de seguridad de la información. (2007-2008)	Pérdidas proyectadas ocasionadas por el mal manejo y falta de seguridad de la información.	Ahorro Anual estimado	Beneficios Esperados del SGSI
2010	83%	$818,250.00	$139,102.50	$679,147.50	$540,045.00
2011	93%	$818,250.00	$57,277.50	$760,972.50	$703,695.00
2012	100%	$818,250.00	$0.00	$818,250.00	$818,250.00

Beneficios – Costo de la implantación

AÑO	BENEFICIO	COSTO	B/C	Tiempo de recuperacion
2010	$540,045.00	$80,474.00		
2011	$703,695.00	$80,474.00		
2012	$818,250.00	$80,474.00		
TOTALES	$2061,990.00	$241,422.00	**8.36**	1.5 meses

Escenarios económicos

ESCENARIO	Año	% esperado de Reducción de perdidas	TMAR	B/C	TRI	FACTIBLE?
1	2010	78%	**7.50%**	**8.12**	**0.13**	**SI**
	2011	90%				
	2012	100%				
2	2010	85%	**7.50%**	**8.89**	**0.12**	**SI**
	2011	95%				
	2012	100%				

Análisis probabilístico

anos/ Escenarios	2010 P (X)	2011 P (X)	2012 P (X)	Valor Esperado
1	83.00	93.00	100.00	92.0000
2	78.00	90.00	100.00	89.3333
3	85.00	95.00	100.00	93.3333

Anos/ Escenarios	2010	2011	2012	Valor esperado	Varianza	Desviacion estandar	Coeficiente de variacion
1	83.00	93.00	100.00	92.0000	73.000	8.5440	9.286960593
2	78.00	90.00	100.00	89.3333	121.333	11.0151	12.33038182
3	85.00	95.00	100.00	93.3333	58.3333	7.6376	8.183170884

CRITERIOS DE EVALUACION:		NO EXITOSO	INDIFERENTE	EXITOSO			
		1	3	5			
ESCENARIO	EVALUADOR	CRITERIOS PARA EL EXITO O FRACASO DE LOS ESCENARIOS						
		EXPERIENCIAS ANTERIORES	NOVEDOSO DEL PROYECTO	APOYO DE LA GERENCIA	ESTRUCTURA ADMINISTRATIVA	AMBIENTE DE ESTABILIDAD	INTERES DEL PERSONAL	TOTAL
1	1	3	5	5	3	3	3	38.55 %
	2	5	1	5	3	5	3	
	3	5	5	1	1	3	5	
Prom		4.33	3.67	3.67	2.33	3.67	3.67	3.56
2	1	5	3	3	5	1	3	31.33 %
	2	3	3	1	3	5	1	
	3	1	1	3	3	5	3	
Prom		3.00	2.33	2.33	3.67	3.67	2.33	2.89
3	1	5	1	1	3	1	3	30.12 %
	2	1	5	5	1	5	1	
	3	1	1	3	5	3	5	
Prom		2.33	2.33	3.00	3.00	3.00	3.00	2.78

Escenario	Análisis del coeficiente de variacion	Analisis de probabilidad de ocurrencia
1	9.28%	38.55%
2	12.33%	31.33%
3	8.18%	30.12%

De lo anterior el escenario que resulta mas factible es el numero 1 pues es el que posee mayor probabilidad de ocurrencia y el que posee un coeficiente de variación promedio, es decir se encuentra entre los límites del mismo.

ANEXO 15: COTIZACIÓN DE CAPACITACIONES Y EL MONTO QUE INSAFORP ABSORBE DE LA MISMA

Antiguo Cuscatlán, 04 de septiembre de 2009

No. Documento 86395
Solicitud No. 1366/2009
TDR No. 03000541012009

IRMA ELENA DE URQUILLA/CARMEN DE VASQUEZ
COMISION EJECUTIVA HIDROELECTRICA DEL RIO LEMPA (CEL)
Presente.

En relación a solicitud de capacitación de fecha 14/07/2009 para desarrollar el tema de capacitación **" MANEJO DE CRISIS EN CASOS DE EMERGENCIA",** hacemos de su conocimiento que nuestra institución, de conformidad a lo exigido en la Ley de Adquisiciones y Contrataciones "LACAP", invitó a ofertar a los siguientes proveedores: GILBERTO ANTONIO PAZ FLORES, HECTOR OSVALDO BONILLA CHAVARRIA, REYNALDO ALEXANDER VALLEJO MONGE, ROBERTO ANTONIO ESQUIVEL, ROMEL GIOVANNI CUESTAS PACHECO, CARLOS ROBERTO SANCHEZ ESPAÑA, EDWIN MAURICIO CHAVARRIA IGLESIAS, OSCAR ANTONIO ZAMORA TOBAR, de los cuales ofertaron: EDWIN MAURICIO CHAVARRIA IGLESIAS, CUATRO MAS ENVIARON NOTA DE EXCUSA, luego de la evaluación técnica-económica, los proveedores que califican para impartir la acción formativa son los siguientes:

Nombre Empresa	Monto Ofertado $	Monto de Apoyo	% Apoyo
EDWIN MAURICIO CHAVARRIA IGLESIAS Teléfono: 22746645 Fax: 2784972 @mail: 8883390@tigo.com, e.m.chavarria@gmail.com, edwin.m.chavarria@hotamil.com	1,200.0	840.00	70.0%

Les agradeceremos contactar directamente a los proveedores propuestos, a efecto de que evalúen y seleccionen el más conveniente en calidad y precio para su institución, pudiendo con toda libertad solicitarles la información adicional que consideren necesaria (Hoja de Vida del facilitador, carta didáctica, otra).

Asimismo, deberán remitir a la UACI: Formulario de Acción Formativa (F8), lista de participantes y esta notificación firmada y sellada, a más tardar **diez (10) días hábiles** después de recibida ; considerando además para programar el inicio de la capacitación **5 DIAS HABILES**, contados a partir de la presentación correcta y completa de estos documentos.

Atentamente,

Unidad de Adquisiciones y Contrataciones Institucional

UACI INSAFORP

Tomar en cuenta:

1. Si requieren de más tiempo para dar una respuesta en el plazo indicado, favor enviar correo a la dirección electrónica **gaguiluz@insaforp.org.sv**, haciendo referencia a nombre de la capacitación, números de la solicitud y del término de referencia.

ANEXO 16: FORMULARIO DE ACCION FORMATIVA F-8 INSAFORP

I. GENERALIDADES

Nombre de la Empresa: _____Tel.:_____

Número de Empleados en total: _____ Fax: _____

Persona Contacto: _____ Correo Electrónico: _____

Nombre del Evento: _____ ___

_____ Duración por Grupo (horas): _____En Total: _____

Lugar de Realización del Evento (Dirección Exacta): _____

_____

_____ Nombre del Proveedor Seleccionado: _____

Nombre del Facilitador/Instructor: _____

II. CALENDARIZACION

GRUPO(S) DE PARTICIPANTES	HORARIOS	FECHAS DE REALIZACION
UNO O UNICO		
DOS		
TRES		

III. NIVEL ORGANIZACIONAL DE PARTICIPANTES

No. Del Grupo	Nivel de los Participantes										Total por Sexo		Total
	Gerentes o Directores		Mandos Medios Administ		Mandos Medios Técnicos		Personal Administ		Personal Operativo				
	M	F	M	F	M	F	M	F	M	F	M	F	
1													
2													
3													

Nota: Mayor número de Grupos, favor anexar información en hoja adicional.

F. _____

_____

Responsable de la Empresa Sello

F. _____

_____

Empresa Capacitadora Sello
Ó Consultor

ANEXO 17: PROGRAMA DE CAPACITACIONES PARA EL PERSONAL DE CEL

PERFIL DE PARTICIPANTES.

• Personal superior y funcionarios que necesitan conocer la problemática y soluciones en cuanto a seguridad de la información y su trascendencia en los riesgos de negocios.

• Gerentes y cuadros medios de Sistemas, Computación y Tecnología, administradores de redes y seguridad de la información que necesitan adecuar a criterios de confiabilidad internacional el nivel de seguridad en operaciones de ecommerce, accesos remotos e inalámbricos.

• Auditores informáticos y de sistemas, auditores internos y externos.

• Auditores de diferentes sistemas de gestión corporativos.

1. CAPACITACIÓN A LAS AUTORIDADES DE CEL

OBJETIVOS

- Capacitar e instruir al personal de las áreas involucradas en el proyecto asi como al personal que se encargada de la implementación del mismo en materia de Gestión y manejo de la seguridad de la información y la norma ISO 27000.

- Capacitar al personal en materia de uso de documentación, formatos, procedimientos normativos, Análisis y gestión del riesgo para que puedan administrar y Gestionar debidamente la Seguridad de la información

- Conocer los fundamentos y conceptos generales para la gestión de la seguridad de la información a partir de la visión general de la normativa internacional agrupada en la Serie 27000 de ISO/IEC, familia de estándares relacionados con la gestión de seguridad de la información.

- Conocer los conceptos generales y las acciones que permiten implementar un Sistema de Gestión de la Seguridad de la Información basado en la Norma ISO/IEC 27001 e ISO/IEC 17799.

- Estándares y modelos internacionales y nacionales relacionados: CobiT®, ITIL, normativas de seguridad aplicadas al ámbito privado, gubernamental y entidades financieras nacionales.

- Realizar talleres participativos para dinamizar los conceptos y asegurar el entendimiento de los mismos.

PROPÓSITO:

Proporcionar al personal herramientas y bases teóricas sobre la normativa ISO 27000 además de concientizar sobre la importancia del manejo y seguridad de la información generando una visión hacia el futuro comprometida con una adecuada Gestión de la Seguridad de información.

PARTICIPANTES

- Jefe de Gestión Integrada
- Jefe de la Unidad de Producción
- Jefe de comercialización
- Jefe de Gestión de la Información
- Jefe de RRHH

CONTENIDO TEMATICO:

Unidad I: FUNDAMENTOS DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SEGÚN LA SERIE ISO/IEC 27000.

- Introducción a la seguridad de la información y a su gestión según la Serie ISO/IEC 27000.
- Conceptualización de un Sistema de Gestión de Seguridad de la Información (SGSI) según la Norma ISO/IEC 27001. Alcance. Entendimiento de los términos y definiciones asociados.
- Requerimientos del Sistema de Gestión de Seguridad de la Información (SGSI):
- Modelo Plan- Do- Check-Act (PHVA).
- Planificación, Implementación, revisión, mantenimiento y mejora continua del SGSI.
- Evaluación y Gestión de riesgos.
- Documentación requerida, Responsabilidad de la Alta Dirección y Gestión de recursos.

Unidad II: SEGURIDAD DE LA INFORMACIÓN: NORMA ISO/IEC 17799

- Introducción a la norma: origen y evolución.
- Contenido de la Norma: Las buenas prácticas para la Gestión de la Seguridad de la Información.
- Capítulos, objetivos de control y controles:
- Política de seguridad
- Aspectos organizativos para la seguridad

- Clasificación y Control de Activos
- Seguridad ligada al Personal
- Seguridad física y del entorno
- Gestión de Comunicaciones y Operaciones
- Control de Accesos
- Desarrollo y Mantenimiento de Sistemas
- Gestión de Continuidad del negocio
- Conformidad
- Consideraciones para la implementación de la norma. Casos prácticos.

2. CAPACITACIÓN A LAS ÁREAS INVOLUCRADAS EN EL PROYECTO

OBJETIVOS:

- Capacitar e instruir al personal de las áreas involucradas en el proyecto asi como al personal que se encargada de la implementación del mismo en materia de Gestión y manejo de la seguridad de la información y la norma ISO 27000.
- Capacitar al personal en materia de uso de documentación, formatos, procedimientos normativos, Análisis y gestión del riesgo para que puedan administrar y Gestionar debidamente la Seguridad de la información
- Realizar talleres participativos para dinamizar los conceptos y asegurar el entendimiento de los mismos.
- Comprender la integración de la norma ISO 27001 con otros estándares y normativas aplicables.
- Profundizar los conocimientos sobre la norma ISO 27001 y comprender el proceso de auditoría y evaluación de la eficacia de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Reconocer, revisar, analizar y articular:

• La evaluación de seguridad, el análisis y gestión de riesgos, y las herramientas para su tratamiento.
• Los riesgos organizacionales, operacionales, físicos y de sistemas IT, y las metodologías para su determinación.
• Las normas ISO 27002 (antes 17799) y 27001 que rigen la seguridad de la información. Complementación, selección e implementación de controles.
• El aporte de integración de la familia de normas 27000 a la problemática de riesgos y seguridad.

• El Sistema de Gestión de Seguridad de la Información certificable de la ISO
27001, armonización con los sistemas de gestión de Calidad (ISO 9001) y Ambiental (ISO 14001).
• Análisis de un caso real de implementación de amplio alcance de la ISO 27001.
• La participación activa en un taller de implementación.

PROPÓSITO:

Proporcionar al personal herramientas y bases teóricas sobre la normativa ISO 27000 además de concientizar sobre la importancia del manejo y seguridad de la información generando una visión hacia el futuro comprometida con una adecuada Gestión de la Seguridad de información.

PARTICIPANTES:

- Técnico en seguridad de información de la unidad de producción
- Técnico en seguridad de información de la unidad de comercialización
- Técnico en seguridad de información de la unidad de RRHH
- Técnico en seguridad de información de la unidad de Gestión de Información
- Coordinador del SGSI
- Asesor interno

CONTENIDO TEMÁTICO:

UNIDAD I: INTRODUCCION A SEGURIDAD DE LA INFORMACION.

0.1 ¿Qué es seguridad de la información?
0.2 ¿Por qué se necesita seguridad de la información?
0.3 ¿Cómo establecer los requerimientos de seguridad?
0.4 Evaluando los riesgos de la seguridad
0.5 Selección de controles
0.6 Punto de inicio de la seguridad de la información
0.7 Factores de éxito críticos
0.8 Desarrollo de sus propios lineamientos

UNIDAD II: SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN LOS REQUISITOS DE LA NORMA ISO 27000

1. Introducción

    a. General
    b. Enfoque del Proceso
2. Modelo PHVA aplicado a los procesos SGSI
    a. Compatibilidad con otros sistemas de gestión
3. Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de
4. seguridad de la información – Requerimientos
5. Alcance
    a. General
    b. Aplicación
6. Referencias normativas
7. Términos y definiciones
8. Sistema de gestión de seguridad de la información
    a. Requerimientos generales
    b. Establecer y manejar el SGSI
        i. Establecer el SGSI
        ii. Implementar y operar el SGSI
        iii. Monitorear y revisar el SGSI
        iv. Mantener y mejorar el SGSI
    c. Requerimientos de documentación
        i. General
        ii. Control de documentos
        iii. Control de registros
9. Responsabilidad de la gerencia
    a. Compromiso de la gerencia
    b. Gestión de recursos
        i. Provisión de recursos
        ii. Capacitación, conocimiento y capacidad
10. Auditorías internas SGSI
11. Revisión Gerencial del SGSI
    a. General
    b. Insumo de la revisión
    c. Resultado de la revisión
12. Mejoramiento del SGSI
    a. Mejoramiento continuo
    b. Acción correctiva
    c. Acción preventiva
13. Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar
14. Internacional
15. Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este
16. Estándar Internacional ISO 27000

UNIDAD III: TÉCNICAS DE SEGURIDAD – CÓDIGO PARA LA PRÁCTICA DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMATION

11.4.6 Control de conexión a la red

11.4.7 Control de routing de la red

11.5 Control del acceso al sistema operativo

11.5.1 Procedimientos para un registro seguro

11.5.2 Identificación y autenticación del usuario

11.5.3 Sistema de gestión de claves secretas

11.5.4 Uso de las utilidades del sistema

11.5.5Cierre de una sesión por inactividad

11.5.6 Limitación del tiempo de conexión

11.6 Control de acceso a la aplicación y la información

11.6.1 Restricción del acceso a la información

11.6.2 Aislar el sistema confidencial

11.7 Computación y tele-trabajo móvil

11.7.1 Computación y comunicaciones móviles

11.7.2 Tele-trabajo

12 Adquisición, desarrollo y mantenimiento de los sistemas de información

12.1 Requerimientos de seguridad de los sistemas de información

12.1.1 Análisis y especificación de los requerimientos de seguridad

12.2 Procesamiento correcto en las aplicaciones

12.2.1 Validación de la input data

12.2.2 Control del procesamiento interno

12.2.3 Integridad del mensaje

12.2.4 Validación de la output data

12.3 Controles criptográficos

12.3.1 Política sobre el uso de controles criptográficos

12.3.2 Gestión de claves

12.4 Seguridad de los archivos del sistema

12.4.1 Control del software operacional

12.4.2 Protección de la data del sistema

12.4 3 Control de acceso al código fuente del programa

12.5 Seguridad en los procesos de desarrollo y soporte

12.5.1 Procedimientos del control del cambio

12.5.2 Revisión técnica de la aplicación después de cambios en el sistema

12.5.3 Restricciones sobre los cambios en los paquetes de software

12.5.4 Filtración de información

12.5.5 Desarrollo de software abastecido externamente

12.6 Gestión de la Vulnerabilidad Técnica

12.6.1 Control de las vulnerabilidades técnicas

13 Gestión de un incidente en la seguridad de la información

13.1 Reporte de los eventos y debilidades de la seguridad de la información

13.1.1 Reporte de eventos en la seguridad de la información

13.1.2 Reporte de las debilidades en la seguridad

13.2 Gestión de los incidentes y mejoras en la seguridad de la información

13.2.1 Responsabilidades y procedimientos

13.2.2 Aprender de los incidentes en la seguridad de la información

13.2.3 Recolección de evidencia

14 Gestión de la continuidad del negocio

14.1 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

14.1.1 Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio

14.1.2 Continuidad del negocio y evaluación del riesgo

14.1.3 Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información

14.1.4 Marco Referencial de la planeación de la continuidad del negocio

14.1.5 Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio

15 Cumplimiento

15.1 Cumplimiento de los requerimientos legales

15.1.1 Identificación de la legislación aplicable

15.1.2 Derechos de propiedad intelectual (IPR)

15.1.3 Protección de registros organizacionales

15.1.4 Protección de la data y privacidad de la información persona l

15.1.5 Prevención del mal uso de los medios de procesamiento de la información

15.1.6 Regulación de controles criptográficos

15.2 Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico

15.2.1 Cumplimiento con las políticas y estándares de seguridad

15.2.2 Chequeo del cumplimiento técnico

15.3 Consideraciones de auditoria de los sistemas de información

15.3.1 Controles de auditoría de los sistemas de información

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

TALLERES Y TRABAJOS A REALIZAR

1) Reconocimiento del esquema y cronograma de los pasos del proyecto.

2) Activos primarios. Clasificación. Asignación de niveles, discusión.

3) Vulnerabilidades. Clasificación y niveles, discusión. Vulnerabilidades Físicas, Organizacionales y Operacionales. Vulnerabilidades Técnicas. Vulnerabilidades totales y por niveles. Nivel relativo de vulnerabilidad total, activos más vulnerables.

4) Ensayos de la aplicación del método Delphi para la determinación de vulnerabilidades organizacionales y operacionales.

5) Amenazas. Clasificación. Asignación de niveles, discusión.

6) Matrices de riesgos. Comparaciones.

7) Riesgos potenciales en activos. Amenazas vs. Activos. Amenazas vs. Vulnerabilidades.

8) Cálculo de riesgos en activos seleccionados:Riesgo promedio; por cada amenaza, cantidad de vulnerabilidades y máximo riesgo; cruces totales amenazas -vulnerabilidades.

9) Resumen de riesgos y total de cruces amenazas-vulnerabilidades de diferentes tipos de activos. Máximos por tipo y ubicación.

10) Discusión de totales de riesgo por activo, máximos, promedios y factor de importancia.

11) Cálculo de pérdidas en productividad e ingresos.

12) Análisis Gap. Discusión sobre varios controles de la ISO 27002. Resultados, cumplimiento.

13) Revisión de las métricas de gestión.

14) Alcance del SGSI. Condiciones y discusión sobre un modelo. Escenarios de daños.

15) Política General. Condiciones y discusión sobre los puntos a definir, objetivos y normas de uso.

16) Normas de Uso. Modelo, discusión. Desarrollo de una norma a elección.

17) Foro de gestión. Participantes y operación.

18) Controles. Requisitos y formatos.

19) Lista de controles según recomendaciones de la norma ISO 27002. Condiciones, redacción y discusión de casos característicos de controles y procedimientos.

20) Métricas de gestión.

21) Concientización y capacitación. Discusión sobre temarios para diferentes tipos de usuarios.

22) Organización del área de seguridad. Perfiles del personal de seguridad de la información: administración de seguridad, analista de seguridad y CISO.

ANEXO 18: MANUAL DE FUNCIONES PARA LA OPERACIÓN DEL SGSI.

SISTEMA DE GESTION PARA EL MANEJO Y SEGURIDAD DE LA INFORMACION

Manual de funciones de Operacion del SGSI

OCTUBRE 2009

CATALOGO DE PUESTOS AUTORIZADOS

El campo de aplicación de este manual, comprende la Unidad de Gestión de Seguridad de Información.

Dentro de esta Area se involucran los siguientes puestos de trabajo:

- Alta gerencia de CEL
- Jefe de Unidad de Seguridad de la Informacion
- Coordinador/a del SGSI
- Tecnico de SGSI de Produccion
- Tecnico de SGSI de Comercializacion
- Tecnico de SGSI de Informatica
- Tecnico de SGSI de Desarrollo Humana

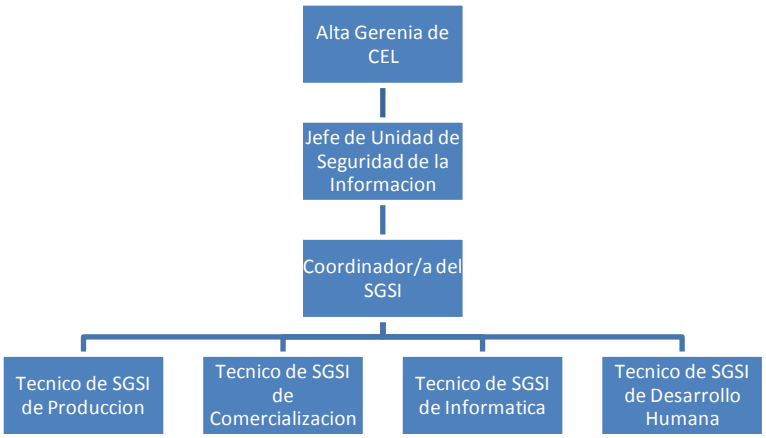
INTRODUCCIÓN

El presente manual nos describe las principales funciones que desempeñaran cada una de las personas involucradas en la operación del SGSI. De igual forma se han definido las líneas de autoridad por medio de un diagrama organizacional.

OBJETIVO:

Proporcionar la estructura organizativa de la Unida responsable de la operación del SGSI, las líneas y grados de autoridad, responsabilidades y funciones de cada uno de los puestos de trabajo.

ESTRUCTURA ORGANIZATIVA PROPUESTA.



DESCRIPCION DE FUNCIONES:

A continuación se presentan las funciones para los siguientes puestos de trabajo:

1. Jefe de la Unidad de Seguridad de la información
2. Coordinador del SGSI
3. Técnico de SGSI

JEFE DE LA UNIDAD DE SEGURIDAD DE LA INFORMACION.

Nombre de la Unidad: Gestión de Seguridad de Información

Dependencia jerárquica: Alta Gerencia de CEL

Unidad subordinada: Procesos claves y de apoyo de CEL

Cantidad de plazas: 1

ES RESPONSABILIDAD DEL JEFE DE LA UNIDAD DE SEGURIDAD DE LA INFORMACIÓN :

- Identificar los procesos claves que serán sujetos a inspección de Seguridad de la Información.
- Aprobar las Fichas de Proceso de Seguridad cuando sea necesario.
- Investigar junto con su personal, las causas que originan la No Conformidad y proponer Acciones Correctivas o Preventivas necesarias para solventarla, evitar su repetición o prevenirla, detallándolas en la Hoja de No Conformidad, Acciones Correctivas o Preventivas.
- Identificar oportunidades de mejora continua, proponer acciones y realizar el respectivo seguimiento.
- Velar por el fiel cumplimiento de los procedimientos normativos
- Revisar las actualizaciones propuestas por el personal.
- Elaborar propuestas de actualización de los procedimientos normativos

  Tomar las acciones correctivas cuando le sean notificados:

  i. Incidentes o debilidades de seguridad en los sistemas de información.
  j. Infracciones, problemas de seguridad informática, daños, pérdidas y mal funcionamiento de hardware, software.
  k. Condiciones que pudieran llevar a una interrupción de las actividades del negocio.
  l. Divulgación de la información confidencial o sensible y de uso interno.
  m. Alertas y advertencias de vulnerabilidades relacionadas a personas no autorizadas, incluyendo: la pérdida o cambios en los datos de producción y el uso cuestionable de archivos, bases de datos o redes de comunicación.
  n. Solicitudes inusuales de información efectuadas por personas externas.
  o. Conducta atípica del sistema.
  p. Fallas o indisponibilidad de los controles que aseguran la integridad de la información.
- Autorizar el acceso a la información de los sistemas informáticos.
- Actuar y aplicar lo establecido en las disposiciones legales y técnicas vigentes, según corresponda cuando se detecten incidentes de seguridad producidos de forma deliberada por empleados de La Comisión o terceros.
- Elaborar, revisar, aprobar y mantener un proceso de gestión de incidentes y problemas de seguridad de la información, el cual debe contar con la tipificación de incidentes y niveles de impacto.
- Revisar mensualmente los informes de incidentes y problemas de seguridad, resultado de dicho proceso de gestión, elaborado por los Encargados de Seguridad de la Información.
- Tomar en cuenta las acciones preventivas o correctivas que provengan del análisis de incidentes para incorporarlas al plan de seguridad o plan de calidad.
- Gestionar el acceso y permisos a los sistemas informáticos al personal bajo responsabilidad o terceros.
- Solicitar inmediatamente al área o unidad de informática según corresponda, el aislamiento de la estación de trabajo y mantenerla intacta hasta que se presente el encargado de seguridad de

su dependencia, cuando la misma este involucrada en una violación o incidente de seguridad con el fin de recabar evidencia o proteger la información contenida en ella.

- Revisar y remitir a la Dirección Ejecutiva el informe anual de incidentes, problemas y violaciones a la seguridad de la información

- Coordinar y Convocar a reuniones al menos una vez al año con los jefes y Gerentes de los Procesos en aplicación para dar seguimiento a sus actividades.
- Presidir las reuniones.
- Aprobar el informe anual de la revisión del Sistema de Gestión de Seguridad de la Información.
- Aprobar o Ajustar los Planes de Acción formulados por Jefes de las Unidades en estudio.
- Dar seguimiento de acuerdos establecidos en reuniones anteriores Jefes de las Unidades en estudio
- Definir cursos de acción necesarios para solventar cualquier desviación en el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información, además en aquellos casos en que los jefes de las Unidades en estudio no han definido acciones correctivas o preventivas al respecto.
- Proporcionar los datos referentes a las auditorias de seguridad de la información, así como acciones correctivas, preventivas producto de las mismas, para ser incluidas en las partes del Informe Anual de Revisión del SGSI de La Comisión.
- Brindar apoyo en la preparación del Informe Anual de Revisión del SGSI de La Comisión

COORDINADOR DE SEGURIDAD DE LA INFORMACIÓN

Nombre de la Unidad: Gestión de Seguridad de Información

Dependencia jerárquica: Jefe de la unidad de seguridad de la informacion

Unidad subordinada: Procesos claves y de apoyo de CEL

Cantidad de plazas: 1

ES RESPONSABILIDAD DEL COORDINADOR DE SEGURIDAD DE LA INFORMACIÓN:

- Asegurar que los Documentos del Sistema de Gestión de Seguridad de la Información cumplan con los requisitos establecidos en la Norma UNE-ISO/IEC 27001:2007 y lo regulado en este procedimiento en lo aplicable para cada Dependencia.
- Evaluar el cumplimiento y validez de los Documentos del SGSI.
- Asesorar a las Unidades Organizativas en las diferentes Dependencias en la elaboración de los Documentos del SGSI
- Evaluar el cumplimiento y validez de los Documentos del SGSI.
- Revisar, actualizar, aprobar, distribuir, controlar o someter a aprobación los Documentos correspondientes del SGSI,.
- Publicar en los enlaces dentro del SGSI, los Documentos Originales del Sistema de Gestión de Seguridad de la Información.
- Comunicar a través de correo electrónico a los Directores y Subdirectores; Jefes de Unidades Organizativas, Encargados de Seguridad de cada Dependencia, usuarios de CEL; según corresponda, cuando existan cambios o nuevos Documentos del SGSI.
- Realizar inducciones de los Documentos de carácter normativo a los Encargados de Seguridad de la Información de cada Dependencia.
- Realiza inducciones de los Documentos de carácter operativo a los Técnicos de Seguridad de la Información.
- Verificar la aplicación efectiva de los procedimientos normativos.
- Coordinar la ejecución del monitoreo o inspección.
- Informar los resultados de los monitoreos o inspecciones periódicamente a las unidades organizativas de cada Dependencia.
- Efectuar la actualización en la documentación del SGSI cuando ocurran cambios en los requisitos internos, externos y legales en materia de seguridad de la información.
- Efectuar la actualización en la documentación del SGSI cuando sea requerido por las Unidades Organizativas, debido a cambios en los requisitos internos, externos y legales en materia de seguridad de la información identificados por las mismas.
- Elaborar propuestas de actualización del Procedimiento.
- Es el responsable de verificar la correcta ejecución de este procedimiento.
- Sugerir las acciones correctivas inmediatas cuando le sean notificados:
    j. Incidentes o debilidades de seguridad en los sistemas de información.
    k. Infracciones, problemas de seguridad informática, daños, pérdidas y mal funcionamiento de hardware, software.
    l. Condiciones que pudieran llevar a una interrupción de las actividades del negocio.
    m. Divulgación de la información confidencial o sensible y de uso interno.
    n. Alertas y advertencias de vulnerabilidades relacionadas a personas no autorizadas, incluyendo: la pérdida o cambios en los datos de producción y el uso cuestionable de

archivos, bases de datos o redes de comunicación.

o. Solicitudes inusuales de información efectuadas por personas externas.
p. Conducta atípica del sistema.
q. Fallas o indisponibilidad de los controles que aseguran la integridad de la información.
r. Problemas asociados con sistemas informáticos en diseño y desarrollo, que no se han abordado adecuadamente por los proyectos existentes o planificados.

- Informar al Coordinador de Tecnología de la Información, cuando La Comisión haya sido víctima de un delito de computación o comunicación, con suficientes datos para tomar acciones que prevengan o reduzcan tales incidentes.
- Elaborar el informe anual de incidentes, problemas y violaciones a la seguridad de la información.
- Actualizar las variables del análisis de riesgo tomando como base los resultados de los informes sobre incidentes.
- Preparar agenda para cada reunión.
- Moderar y mantener las discusiones dentro del tema y nivel técnico.
- Redactar y gestionar las firmas de las actas de reuniones.
- Realizar seguimiento a los acuerdos tomados en reuniones anteriores.
- Coordinar la recopilación de información que debe ser sometida a consideración de la dirección Ejecutiva.
- Consolidar el Informe de Revisión del Sistema de Gestión de Seguridad de la Información, considerando para ello los informes correspondientes de los Encargados de Seguridad de la Información de cada Unidad.
- Proponer los requisitos de manejo de la información
- Proponer la clasificación del marcado de la información.

TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN

Nombre de la Unidad: Gestión de Seguridad de Información

Dependencia jerárquica: Coordinador de seguridad de la información

Unidad subordinada: Procesos claves y de apoyo de CEL

Cantidad de plazas: 4

ES RESPONSABILIDAD DEL TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN:

- Efectuar la actualización y mantenimiento en la estructura del SGSI, por los cambios de estructura en las Unidades Organizativas y/o Jefaturas o cada vez que se emita, anule o modifique un Documento del SGSI.
- Cuando el cambio de estructura implica insertar un enlace, se efectúa siguiendo el número correlativo del ramal principal afectado.
- Cuando las unidades soliciten la eliminación de un área, el número de dicha área queda fuera de uso y no se utiliza dentro de ese ramal, ya que esto ocasionaría cambios en toda la estructura de los enlaces.
- Comunicar por un requerimiento en el Sistema al Jefe de la Unidad Organizativa responsable, la disponibilidad de los Documentos vigentes en el SGSI.
- Actualizar y archivar magnéticamente los Documentos del SGSI
- Identificar y almacenar los Documentos del SGSI que han sido sustituidos o eliminados, guardándolos en la carpeta Documentos Ediciones Anteriores (Word y Excel) sin firmas o rubricas y (PDF de Adobe) con firmas o rubricas, respectivamente; manteniéndolos por un período de 3 años, en los casos que las leyes fijen un período mayor de resguardo, se atiende lo señalado en ellas.
- Actualizar las matrices de los Documentos del SGSI.
- Asegurar que los Documentos del SGSI sean legibles.
- Revisar la Ficha de Proceso de Seguridad.
- Colocar en las carpetas del SGSI los informes y registros de monitoreo e inspección conforme a lo establecido en el Control de Documentos del SGSI.
- Actualizar los enlaces dentro de la INTRANET del SGSI correspondientes a cada Unidad Organizativa, de a cuerdo con el Control de Documentos del SGSI; cada vez que se emita, anule o modifiquen los requisitos internos, externos y legales.
- Cumplir con lo establecido en este procedimiento.
- Elaborar propuestas de actualización del Procedimiento.
- Actualizar las Carpetas Compartidas del Portal institucional “Intranet” del Sistema de Gestión de Seguridad de la Información correspondiente de cada Unidad Organizativa, cada vez que se emitan Planes e Informes de Auditorías de Seguridad y/o Seguimiento, conforme a un procedimiento que se debe establecer llamado Procedimiento para la Conversión de Formato, Publicación, Almacenamiento y Control de Documentos del SGSI.
- Mantener en las Carpetas Compartidas del Portal institucional “Intranet” del Sistema de Gestión de Seguridad de la Información el archivo de planes e informes de auditoria de seguridad y/o seguimiento (en formato PDF), durante un período mínimo de 3 años, por considerarse Registros de Seguridad de la Información.
- Dar apertura a la No Conformidad a través de la Hoja de No Conformidad, Acciones Correctivas o Preventivas y darle seguimiento a la ejecución de dichas acciones para verificar su eficacia, en

cuanto a la eliminación de las causas que originan la No Conformidad; asimismo, efectuar el cierre de dicha hoja.

- Mantener en las carpetas compartidas del Portal Corporativo “Intranet” del Sistema de Gestión de Seguridad de la Información, el archivo de las Hojas de No Conformidad, Acciones Correctivas o Preventivas por No Conformidades establecidas (en formato PDF), durante un período mínimo de 3 años, por considerarse Registros de Seguridad.
- Archivar magnéticamente en **documentos ediciones vigentes**, las Hojas de No Conformidad, Acciones Correctivas o Preventivas, en formato de Word.
- Eliminar archivo en formato de Word de las Hojas de Acciones Correctivas o Preventivas cuando han sido cerradas.
- Concientizar al personal de La Comisión sobre medidas para la prevención de incidentes de seguridad de la información.
- Ejecutar las acciones que le hayan sido delegadas por el Coordinador de Seguridad de la Información.
- Asesorar en la clasificación y marcado de la información cuando los Jefes de las Unidades Organizativas o a quien delegue se lo solicite.

ANEXO . 19: SOLICITUD DE CERTIFICACIÓN

Solicitud de Certificación

Muy Sr./a. nuestro/a:
Con el fin de poder iniciar los trámites de certificación de su empresa, le rogamos cumplimenten este impreso y lo envíen a la dirección de AENOR EL SALVADOR que figura al final del documento.

Datos generales de la entidad solicitante:

Entidad: .....

..... NIT: .....

Con Domicilio Social: .....

Dirección centro a certificar: .....

Ciudad: ..... Departamento: .....

C.P.: ..... País: .....

☐ Si su empresa dispone de más de un centro cumplimente el anexo CASO DE SOLICITAR MÁS DE UN CENTRO

Identificación de cargos:

Persona que va a firmar el contrato (Representante Legal):

Apellidos y Nombre: .....

Cargo: ..... D.U.I.: .....

Persona de contacto para la comunicación y envío de correspondencia:

Apellidos y Nombre: .....

Cargo: .....

Dirección: ..... C.P.: .....

Ciudad: ..... Departamento: .....

País: ..... Telf.: ..... Fax: .....

E-mail: .....

Persona de contacto para la facturación:

Apellidos y Nombre: .....

Cargo: .....

Dirección: ..... C.P.: .....

Ciudad: ..... Departamento: .....

País: ..... Telf.: ..... Fax: .....

E-mail: .....

Solicitud de certificación de Sistemas de gestión

Solicita la certificación del sistema de gestión:

Gestión de la calidad: ☐ UNE-EN ISO 9001 ¿Incluye diseño de productos? SI ☐ NO ☐
☐ UNE 66174 Gestión Avanzada 9004

Gestión ambiental: ☐ UNE-EN ISO 14001 ☐ Verificación medioambiental (EMAS) ☐ Ecodiseño

Gestión integrada: ☐ UNE-EN ISO 9001 + ☐ UNE-EN ISO 14001 + ☐ OHSAS 18001

Referenciales del automóvil: ☐ UNE-EN ISO/TS 16949

Seguridad y salud laboral: ☐ OHSAS 18001 La vigilancia de la salud está asumida por la organización: SI ☐ NO☐
Modalidad preventiva: .....

Aeroespacial: ☐ UNE EN 9100 (fabricación) ☐ prEN 9110 (Mantenimiento) ☐ prEN 9120 (Almacenaje)

Gestión de la accesibilidad: ☐ Accesibilidad global

Agroalimentaria: ☐ UNE ISO 22000 ☐ BRC Alimentación ☐ IFS ☐ SAL ☐ EUREPGAP

Otras certificaciones: ☐ Seguridad de la información (S.G.S.I.) ISO 27001 ☐ Gestión de I+D+I
☐ Acuerdo de Reconocimiento (IQNet)

Otro no indicado:
.....
.....
.....

Certificación de productos y/o servicios:

¿Desean la certificación de algún producto o servicio simultáneamente con alguno de los sistemas anteriores? Sí ☐No☐

En caso afirmativo, cite cuáles:

Las condiciones económicas para la prestación del servicio solicitado son las establecidas en la oferta Nº: .....

Actividades objeto de certificación: Por ejemplo: producción de, transporte de, comercialización de, instalación de, diseño y producción de, para cada sistema de gestión:

Indique, si lo conoce, el código CNAE de la actividad que desea certificar: .....

Estructura de la organización:

Nº total de empleados de la organización: .....

Nº de personas de la organización a los que aplica el sistema objeto de la certificación:

Propias: ..... Subcontratadas: ..... Personal / Nº Turnos: .....

Información adicional:

Fechas aproximadas en las que se desearía:

Realizar la auditoria: ..... Disponer del certificado: .....

¿Dispone de algún tipo de certificación? Sí ☐ No ☐

Cuál y quién certifica: .....

Solicitud de certificación de Sistemas de gestión

Indique el nombre de las entidades asesoras que han participado en la implantación de cada sistema de gestión en los últimos tres años: .....
.....

La firma de la Solicitud implica:

- El pago de las facturas generadas durante el proceso de certificación solicitado, de acuerdo a lo establecido en la oferta correspondiente.
- El cumplimiento en todo momento de la legislación vigente aplicable a las actividades y centros de trabajo indicados en la presente solicitud de certificación de sistemas.
- En cumplimiento de la Ley de Prevención de Riesgos Laborales vigente en materia de coordinación de actividades empresariales. El firmante (cliente) se compromete a facilitar el intercambio de información preventiva (plan de prevención de riesgos laborales, medidas de prevención y emergencia, información) en relación a los riesgos a los que pudiera estar expuesto, durante su estancia en sus instalaciones, el personal de AENOR en la prestación de los servicios encomendados.
- La empresa solicitante se compromete a informar de forma inmediata los cambios organizativos (legales, comerciales, de propiedad, etc.), y de su sistema de gestión (procesos, líneas de fabricación, productos) a partir de la presentación de la solicitud y mientras la empresa se encuentre certificada por AENOR.
- La aceptación de las condiciones particulares de cada certificación especificadas en el anexo correspondiente.

En ..... a …… de ..... de 20 .....

Nombre y Firma:

(Director General/Representante Legal de la Empresa)

AENOR EL SALVADOR tratará, como responsable, sus datos de carácter personal con el fin de llevar a cabo la prestación del servicio objeto de este documento, remitirles documentación y realizar estudios. Los datos personales son voluntarios, impidiéndose, si no los facilita, la correcta prestación de los servicios contratados. Si se facilitan durante la prestación del servicio contratado datos de terceras personas deberá informar previamente a estas del contenido de esta información y recabar su consentimiento para el tratamiento de sus datos. Podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición de sus datos dirigiéndose a AENOR EL SALVADOR.

Sus datos podrán ser cedidos, cuando sea necesario, a las entidades titulares de las certificaciones que haya solicitado a AENOR EL SALVADOR y que ésta gestione conjuntamente con dichas entidades, con el fin de que emitan las certificaciones y licencias de uso, consintiendo esta cesión de sus datos con la firma de este contrato, y absteniéndose de contratar estos servicios si no consiente esta cesión de sus datos.

Nota importante: Rellene los datos del ANEXO correspondiente a cada sistema solicitado.

AENOR EL SALVADOR
Edificio Valencia. Cl. Llama del Bosque, Pte. y Pje. S
Urb. Madreselva. Antiguo Cuscatlán. El Salvador
Tel.: +503 22 43 23 77 / Fax: 503 22 43 23 88
aenor@aenorelsalvador.com
www.aenorelsalvador.com