UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

DISEÑO DE CONTROL INTERNO BASADO EN RIESGOS DE TECNOLOGÍA DE INFORMACIÓN PARA LAS DISTRIBUIDORAS DE SERVICIOS DE TELEFONÍA EN EL SALVADOR."

Trabajo de investigación presentado por:

CARLOS ALEJANDRO LÒPEZ LAZO

ANA MARCELA RAMIREZ ALEMÀN

WITHNMY MARICELA RIVAS CHACÒN

Para optar al grado de:

LICENCIADO EN CONTADURIA PÚBLICA

Diciembre, 2015

San Salvador, El Salvador, Centroamérica

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	: Licenciado José Luis Argueta Antillón.
Secretaria	: Doctora Ana Leticia Zavaleta de Amaya.
Decano de la Facultad de Ciencias Económicas	: Licenciado Nixon Rogelio Hernández Vásquez.
Secretario de la Facultad de Ciencias económicas	: Licenciado José Ciriaco Gutiérrez Contreras.
Directora de la Escuela de Contaduría Pública	: Licenciada María Margarita de Jesús Martínez Mendoza de Hernández
Coordinador de seminario	: Licenciado Mauricio Ernesto Magaña Menéndez
Asesor director	: Licenciado Daniel Nehemías Reyes López
Jurado examinador	: Licenciado Adilsó Alberto Rógel Pineda : Licenciado Henry Amílcar Marroquín : Licenciado Daniel Nehemías Reyes López

Diciembre del 2015

San Salvador, El Salvador, Centroamérica

AGRADECIMIENTO

Le doy gracias a Dios, por ser él quien guía mi camino y me dio la fortaleza para seguir adelante y de iluminarme en mis pensamientos y conocimientos, gracias a la santísima Virgen María por que también me acompaño en este camino y quien me ha protegido.

Agradecer a mis padres quienes son mis principales pilares, a los que les debo todo el apoyo que me han brindado y quienes se han preocupado por mi bienestar y el esfuerzo que han hecho de poder brindarme la educación y lograr mis metas; A mis compañeros de trabajo de graduación Carlos Alejandro López Lazo y Withnmy Maricela Rivas Chacón por compartir momentos buenos y malos y al docentes Lic. Daniel Nehemías Reyes que nos brindó el apoyo y sus conocimientos para la realización este trabajo de investigación.

Ana Marcela Ramírez Alemán

A Diosito primordialmente por haberme guiado a lo largo de mi vida; a mi madre por darme su amor y comprensión, a mi padre por su apoyo en mis estudios, a Carlos Cruz por ser esa persona que marca la diferencia en mi vida, a mis compañeros de trabajo de graduación por formar un equipo y buena amistad y a nuestro asesor Lic. Daniel Reyes por la paciencia y guiarnos en este proyecto, muchas gracias.

Withnmy Maricela Rivas Chacón

Principalmente a Dios Padre todo poderoso por haberme guiado a lo largo de mi vida y de mi carrera, gracias a él he logrado uno de mis mayores objetivos propuestos hasta este momento, a mis padres por su compresión, su confianza y apoyo incondicional, a mis compañeros de trabajo de graduación por inculcarme el trabajo en equipo, la amistad y tolerancia, por todos los momentos compartidos y vividos, gracias.

Carlos Alejandro López Lazo

ÍNDICE

RESUMEN EJECUTIVOi
INTRODUCCIÓN.iii
CAPÍTULO I: MARCO TEÓRICO, TÉCNICO Y LEGAL1
1.1 Antecedentes 1
1.1.1 La entidad y su entorno 1
1.1.2 Antecedentes nacionales sobre la protección de datos. 3
1.1.3 Antecedentes internacionales 4
1.1.4 Control interno para las tecnologías de información 6
1.2 Evaluación de los riesgos informáticos 11
1.2.1 Evaluación de los riesgos de los sistemas de gestión de la seguridad de la información 13
1.2.2 Amenazas, riesgos, vulnerabilidades y controles de tecnología de información 14
1.2.3 Componentes de un sistema de seguridad de la información 15
1.3 Evaluación de la seguridad de las tecnologías de información 16
1.4 Herramientas y técnicas para el aseguramiento de la información 18
1.4.1 Gestión de las tecnologías de información 18
1.4.2 Metodología COBIT 18
1.4.3 Metodología ITIL 20
1.5 Marco técnico 22
1.6 Marco legal 26
1.7 Diseño de un control interno informático 32
CAPÍTULO II METODOLOGÍA DE INVESTIGACIÓN Y DIAGNÓSTICO39
2.1 Tipo de estudio 39
2.2 Unidad de análisis 39
2.3 Universo y muestra 39
2.4 Instrumentos y técnicas a utilizar en la investigación 41
2.5 Procesamiento de la información 41
2.6 Análisis e interpretación de los datos 41
2.7 Diagnóstico de la investigación 41

CAPÌTULO III DISEÑO DE CONTROL INTERNO BASADO EN RIESGOS DE TECNOLOGIA DE INFORMACIÓN 48
3.1 Planteamiento del caso 48
3.1.1 Generalidades 48
3.2 Explicaciones generales, estructura y forma del diseño de control interno informático. 49
3.3 Diseño de control interno basado en riesgo de tecnología de la información. 74
CAPITULO IV CONCLUSIONES Y RECOMENDACIONES
4.1 CONCLUSIONES 113
4.2 RECOMENDACIONES 114
BIBLIOGRAFÍA 115
ANEXOS 116

ÍNDICE DE TABLAS

Tabla 1 Listado de servicios de las entidades distribuidoras de telefonía. 2
Tabla 2 Acontecimientos a nivel internacional 5
Tabla 3 Objetivos de control y sus procesos 9
Tabla 4 Riesgos, amenazas y vulnerabilidades 14
Tabla 5 Normativa técnica sobre sistemas de información. 23
Tabla 6 Marco legal aplicable a los sistemas de información. 27
Tabla 7 Diseño de control interno informàtico 35

ÍNDICE DE FIGURAS

Figura 1Componentes para el procesamiento de la información 8
Figura 2 Objetivo del negocio según COBIT 20
Figura 3Flujograma de elaboración de control interno 35
Figura 4 Matriz de priorización 83
Figura 5 Criterio de evaluacion de riesgos 89
Figura 6 Opciones de tratamiento de riesgos 91
Figura 7 Alternativa para mitigar el riesgo. 92

ÍNDICE DE ANEXOS

Anexo N° I Encuesta dirigida a los contadores públicos autorizados por el CVPCA

Anexo N° IIEncuesta dirigida a las intermediarias de las distribuidoras de telefonía

Anexo N° III Tabulación y análisis de la información procesada

Anexo N° IV Actas de Junta General de Accionistas

Anexo N° V Documento de la política de seguridad de la información

Anexo N° VI Enunciado de aplicabilidad

Anexo N° VII Plan de tratamiento de riesgo

Anexo VIII Manual de control interno basado en riesgos de tecnología de información

RESUMEN EJECUTIVO

En vista que las empresas intermediarias de las distribuidoras de telefonía en los últimos años han aumentado el grado de demanda y exigencia, tanto a nivel nacional como internacional; en la actualidad esto conlleva a aumentar la calidad que deben de implementar en sus actividades productivas, para obtener una mayor confiabilidad, rentabilidad, ventajas y excelencia sobre la competencia.

Como tal dichas entidades, que hoy en día con los avances de las tecnologías de información y comunicación optan por enviar, compartir y emigrar la información por cualquiera de los medios disponibles para la transmisión y recepción de la documentación se enfrentan a problemas con la aplicación de controles tan básicos, considerando los antecedentes tanto nacionales como internacionales en los que se han visto en vueltas estas empresas que manejan información relacionada a datos personales.

Por lo que es de mucha importancia y siendo ese el objetivo general de este trabajo "Diseño de control interno basado en riesgos de tecnologías de información para las empresas distribuidoras de telefonía en El Salvador", que proporcionará a que estas entidades implementen controles alineados a un marco técnico de referencia específico para implementar controles adecuados para mantener la integridad, confidencialidad y disponibilidad de la información.

Además a manera y para lograr el objetivo se estable objetivos específicos que van encaminados a lograr el objetivo general de este trabajo como lo son:

- Describir controles efectivos que contribuya a minimizar los riesgos de Tecnología de Información (TI) y optimizar el resguardo y aseguramiento de la información.
- Desarrollar un marco técnico y legal relacionado a la tecnología de información en conjunto con el control interno.
- Formular el control interno basados en riesgos de TI bajo la normativa técnica de COBIT 5.

En cuanto a la metodología utilizada se elaboró mediante el método hipotético-deductivo ya que este busca mediante la observación y análisis, establecer las diferentes hipótesis que únicamente serán comprobadas mediante la investigación; el estudio se realizó a las empresas intermediarias de las

distribuidoras de telefonía por medio del cual se determinó la muestra, la cual fue objeto de estudio, mediante la encuesta se obtuvo el resultado de la comprobación de la problemática al momento del análisis de los datos recolectados

Los resultados obtenidos demostraron que estas empresas a pesar de contar con control interno llevan controles básicos, por ende están vulnerables a diferentes incidentes de extracción y pérdida de datos, no obstante estas empresas cuentan con controles deficientes en relación a la seguridad de la información, además de considerar las entidades que no cuentan con un control interno informático están muchos más propensas a sufrir incidentes relacionados a tecnologías de información. Siendo en este sentido que muchas de las empresas mostraron interés en implementar controles de acuerdo a las necesidades de la entidad y poder dar respuesta a los riesgos a los que día con día están expuestas.

INTRODUCCIÓN.

La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; en adición de otras propiedades, como la autenticidad, responsabilidad, no-repudiación y fiabilidad. A pesar que existe la tendencia de pensar que los controles asociados a la seguridad de la información solamente están dirigidos a sistemas de "informática", es importante aclarar que estos consideran todos los aspectos relacionados con la información, los medios y los sistemas que la manejan y la soportan.

Un sistema de gestión de seguridad de la información, provee el modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de la información y los sistemas, para alcanzar los objetivos del negocio, basado en la evaluación del riesgo y los niveles de aceptación del mismo para la entidad, con el fin de gestionar de forma efectiva los riesgos; partiendo de este proceso para diseñar un modelo de control interno informático basado en los riesgos de tecnologías de información.

Hoy en día las organizaciones y sus sistemas de información están expuestos a un elevado nivel de amenazas que, aprovechando la vulnerabilidad que presentan, están propensas a diversas formas de espionaje, fraudes, sabotaje, virus informáticos, entre otros. La temática de la Tecnología de Información (TI) es importante, pues esta suele ser un valioso recurso según lo establece la ISO 27002:2005. En ese sentido el presente documento plantea un diseño de control interno orientado al resguardo y salvaguarda de la información, enfocado en las entidades que se dedican a la distribución de los servicios telefónicos.

Por lo tanto el documento contiene en su capítulo I un marco teórico en el cual se establecen conceptos, antecedentes de cómo se originó la problemática, una concepción teórica de los que conlleva el diseño de un control interno informático, las herramientas necesarias para tal efecto entre otras; además va acompañado de un marco técnico y legal relacionado a la tecnología de información, en el

que se detallan las regulaciones establecidas en los marcos de referencia adoptados para desarrollar y para el tratamiento de la información, así como de las regulaciones legales que esta conlleva

De acuerdo a lo anterior en el capítulo II se establece la metodología de la investigación, la unidad de análisis, el universo con el que se va trabajar y la determinación de la muestra sujeta a estudio; se establece como herramienta de estudio la encuesta; en la que se definen preguntas abiertas y cerradas a fin de obtener una comprensión de las características y de los problemas en estudio, con lo cual finalmente se realizó el diagnóstico de la investigación el cual extrae una serie de puntos entre los que se destacan beneficios y las limitantes del resguardo y protección de la información, consecuencias que se podrían originar y los beneficios de aplicar el modelo de control interno informático.

El presente documento se caracteriza por desarrollar una investigación novedosa y de gran utilidad social, tanto para el sector en estudio como los profesionales de la contaduría publica

Además se presenta el capítulo III el cual es la propuesta del diseño de un control interno informático basado en los riesgos de tecnologías de información para las intermediarias de las distribuidoras de los servicios de telefonía; en el cual se establecen el planteamiento del caso práctico y el desarrollo de la presente propuesta, partiendo del punto de vista del modelo PDCA establecido en la ISO 27002, de los procesos de los catalizadores establecido en Cobit en su versión 5 publicado por ISACA en el año 2012.

Finalmente en el capítulo IV se establecen las conclusiones a las que el grupo de investigación llegó luego de la comprensión, estudio y análisis de la problemática planteada estableciendo finalmente las recomendaciones pertinentes y oportunas a fin de mejorar en los niveles adecuados, la comprensión y solución de los inconvenientes establecidos a través de la investigación.

CAPÍTULO I: MARCO TEÓRICO, TÉCNICO Y LEGAL

1.1 Antecedentes

1.1.1 La entidad y su entorno

El mercado de servicios de telecomunicaciones en El Salvador se originó mediante la creación de la Administración Nacional de Telecomunicaciones (ANTEL), en el año de 1963, fue hasta el año 1996 que se dio un cambio tanto por los avances económicos, mundiales y por los desarrollos de nuevas tecnologías. Mediante la implementación de la ley de privatización de las telecomunicaciones en El Salvador se propició para que nuevas empresas invirtieran en el mercado de las telefonías, con el objetivo de ampliar el mercado.

A mediados de 1990 ANTEL concesiona a la empresa Telemòvil, los servicios de telefonía, siendo la única en prestar servicios a los usuarios que eran pocos por el alto costo de los aparatos y servicios de llamadas, debido a lo anterior y con el proceso de privatización surgieron las empresas TelefónicaMóviles,Telecom, Digicel para fomentar mayor competencia, haciendo que la telefonía celular se popularizara en El Salvador y los costos de los servicios se redujeran, además la empresas establecieron estrategias para la fidelización de clientes entre ellos el obsequiar el aparato por la firma del contrato de servicio.(Historia de las telecomunicaciones)

Posteriormente la Asamblea Legislativa aprobó la creación de la Superintendencia General de Electricidad y Telecomunicaciones entidad Institucional encargada de ejercer la función de normalización y regulador de los servicios por lo que consecuentemente la creación de la ley de servicios de telecomunicaciones.

La ley de servicios de telecomunicaciones permitió el nacimiento de nuevas empresas de telefonía tanto fija como móvil y también de televisión, dando al país un impulso importante.

Al mes de mayo del año 2013 se encuentran en operación y ofreciendo servicios de telefonía a usuarios finales operadores de telefonía fija:CTE S.A. de C.V.; El Salvador Network, S.A.; GCA Telecom S.A de C.V.;Telecam S.A. de C.V.;Telemòvil El Salvador, S.A de C.V; Digicel, S.A de C.V, Telefonía Móviles El Salvador, S.A de C.V; CTE Telecom Personal, S.A de C.V. Estas últimas cuatro empresas

prestan servicios de telefonía fija y móviles y cinco operadores de telefonía móvil: CTE Telecom S.A. de C.V.; Telefónica Móviles S.A. de C.V.; Digicel S.A. de C.V.;Telemòvil El Salvador S.A. eIntelfon S.A. de C.V. Brindan el servicio de radio digital troncalizado.

Estas entidades de telefonía empezaron con instalaciones propias de infraestructura así como prestación de todos los servicios, a medida que se daba el crecimiento de la telefonía las entidades optaron por subcontratar sus servicios empezando a través de contratos de servicio con los intermediarios de telefonía hacia las distribuidoras entre los servicios: mantenimiento de cable, instalación de antenas, telefonía fija, *call center*, venta de tarjetas de saldo prepago, recargas electrónicas entre otras.

Muchos de esos servicios son proporcionados a través de entidades intermediarias de telefonía, dado que estas empresas no solamente se encargan de los servicios mencionados anteriormente sino también de mantenimiento de redes, infraestructura, venta de celulares, contratos, entre otros.

El crecimiento de la competitividad de las intermediarias de las distribuidoras telefónicas, ha permitido que los usuarios tengan mayores opciones de elección, mayor cobertura y tarifas más atractivas. La operadoras de telefonía ofrece servicios de mensajería, imágenes, acceso a internet, cable, servicios de paquete de *voip, roaming*, servicio de prepago, distribución de saldo; con estos servicios la forma de contactar con los clientes se desarrolla mediantes contratos donde se estipulan los plazos y condiciones. A continuación se detallanen la Tabla 1 los servicios que prestan las empresas, así como la información que la entidad requiere de sus clientes.

Tabla 1 Listado de servicios de las entidades distribuidoras de telefonía.

Servicios	**Información requerida de los usuarios**
Planes prepago	• Nombre del cliente • Dirección • Teléfono • Ingreso • Lugar de trabajo • Recibo de agua y luz
Planes post-pago	
Telefonía fija	
TV cable	
Internet Residencial	
Servicios digitales	
TV cable satelital	
Video vigilancia	

Elaboración propia.

Cuando se da el caso de servicio de renovación de contrato de telefonía intervienen los *call center* entre ellos: *Sykes, Teleperformance, Stream* los cuales se encargan de suministrar información a las entidades telefónicas; la mayoría de estos manejan la información a través de bases de Excel así como las bases de datos que las entidades telefónicas le proporcionen.

Es por lo anterior y la situación de hoy en día, que la información se vuelve un dato importante, puesto que son vulnerables las bases de datos a ser extraíbles. Dado lo anterior, hasta la fecha no hay una ley que regule la protección de datos de un sistema de información, pero no obstante existen el recurso de *habeas data* que significa "que tenga los registros o conserva tus datos, es decir implica tomar conocimientos de datos propios en poder de otro" (*Habeas Data.* Derecho a la Intimidad, pág. 21) y el artículo 2 de la Constitución de la República de El Salvador que buscan normar el uso indebido de la información.

1.1.2 Antecedentes nacionales sobre la protección de datos.

Habeas data en El Salvador

El *Habeas data* es una acción constitucional que asiste a toda persona identificada o identificable a solicitar judicialmente la exhibición de los registros públicos y privados, en los cuales están incluidos sus datos personales o los de su grupo familiar para tener conocimientos de su exactitud; a requerir la rectificación, la suspensión de datos inexactos u obsoletos. Constituye un mecanismo o instrumento que protege al individuo contra el uso ilegal o indebido de sus datos personales por parte de entidades públicas o privadas.(Alvarez, 2011)

Países como México, han desarrollado normas de protección de datos personales por parte de empresas e instituciones públicas. Uruguay Argentina, Bolivia, Brasil, Colombia, España, Venezuela, Perú y panamá son los que han adoptado tal disposición en sus cartas magnas, debido a lo anterior el habeas data ha venido experimentado auge paralelamente a los avances tecnológicos, ya que trata de brindarle a las personas la privacidad de los datos, en este sentido son los avances tecnológicos en materia de informática para registrar y almacenar datos, lo que repercute en la intromisión de los datos privados manejados por las entidades.

En El Salvador no existe tal nivel de desarrollo en dicho tema, al igual que en el resto de Centroamérica. El asunto sólo puede ser analizado por la Corte Suprema de Justicia al no existir una ley

especial que regule la protección de datos. Pese a esto la Corte reconoció el año 2004 el derecho fundamental de todos los salvadoreños para la protección de datos o la autodeterminación informativa. Algunos de los tratados internacionales que El Salvador ha ratificado contienen disposiciones relativas al derecho a la intimidad, pero no un derecho y un procedimiento para hacer valer el *Habeas data.*

En la actualidad con el desarrollo de las telecomunicaciones y el ámbito tecnológico el 1 de octubre de 2015 se aprobó la ley de firmas electrónicas, siendo un reconocimiento al citado artículo 2 de la Constitución de la República, en este sentido dicha ley es un acontecer; donde la tecnología por medios electrónicos está jugando un papel importante. Fundamentalmente lo que busca esta ley es contar con un sistema que brinde la seguridad de las operaciones electrónicas, acompañado de la confianza para los usuario al efectuar dichas operaciones, además de brindar certeza jurídica al dar un valor igual a la firma autógrafa y a mecanismos tecnológicos que aseguren la identidad y contenido, dicha ley consta de cinco títulos que establece objeto y alcance, principales definiciones, tratamiento de datos personales, la emisión y recepción de los mensajes de datos, infracciones y sanciones entre otros aspectos.
Una de las principales características de la firma es la integridad de los mensajes electrónicos lo que busca es que los documentos no firmados no sean alterados basándose en una función hash que es un algoritmo que resume un gran conjunto de datos que da como resultado otro conjunto de datos finito. Los principales principios que la ley de firmas electrónicas establece son: la autenticidad, integridad, confidencialidad, equivalencia funcional y el no repudio.

1.1.3 Antecedentes internacionales

A nivel internacional los hechos de robo de información se han dado en mayor escala que en el ámbito nacional, la Tabla 2 detalla algunos de los sucesos más representativos del robo y comercialización de datos así como una breve descripción del acontecimiento e impacto que tuvo el hecho.

Tabla 2 Acontecimientos a nivel internacional

Acontecimientos a nivel internacional		
Entidad	**País**	**Suceso**
Adobe	Varios países	Robo de código fuente y datos de 38 millones de usuarios; debido a una brecha de ciber seguridad que propicio que los delincuentes pudiesen acceder a nombres de usuarios y contraseñas cifradas almacenadas en una base de daos; así como también a información de sus tarjetas de crédito.
Vodafone	Alemania	Robo de datos; según la operadora móvil fue uno de sus propios empleados quien efectuó el ataque, robando los datos personales de dos millones de clientes; incluyendo nombres, direcciones, fechas de nacimiento y número de cuentas bancarias
Centro de llamadas	India	En el año 2012 trabajadores del centro de llamadas, vendieron información confidencial de Alrededor de unos 500,000 ciudadanos británicos entre la información que se comercializo se mencionan: nombres, direcciones, números de teléfonos y números de tarjetas de crédito.
Grupo TJX	Varios países	La empresa TJX fuero quienes publicaron el robo de 45.6 millones de números de tarjetas de crédito y débito, alrededor del mundo.
HeartlandPaymentSystems	Estados Unidos	La empresa reveló una filtración de 1000 millones de registros de sus usuarios alrededor del mundo; por lo que tuvo que pagar cerca de 140 millones de dólares para procesar nuevamente las tarjetas de crédito.
Compañía de publicidad	Varios países	Sufre una filtración de millones de nombres y

por correo electrónico Epsilon		direcciones de correo electrónico de las bases de datos de clientes como BestBuy, Marks & Spencer o Chase Bank. Los costos iníciales de retención y reparación previstos alcanzaron los 225 millones de dólares.
Sony Corp	Varios países	Sufrió filtraciones que pusieron en peligro las cuentas de 100 millones de clientes, con un costo para la empresa que alcanzo 2000 millones de dólares.

Fuente: Adaptado de Revista especializada en seguridad (redseguridad.com)

1.1.4 Control interno para las tecnologías de información

Tradicionalmente el control interno se adoptaba a un enfoque contable y administrativo, en la actualidad se sabe que el manejo de controles internos son puntos claves de las actividades operativas de las empresas, esto con el fin de prevención de riesgos efectivos y potenciales ya que se observan importantes cambios en las empresas y los controles.

Principalmente el enfoque que se le dará al control interno será en el entorno de las tecnologías de información, así como contemplar de manera específica la seguridad de la información siendo este uno de sus objetivos fundamentales y finalmente formar un modelo de control interno más completo dentro del área sistemas de información y tecnologías. Este tendrá que estar orientado a los administradores del área de tecnología de información, usuarios y auditores involucrados en el proceso de operaciones de las entidades intermediarias de las distribuidoras de telefonía en El Salvador.

Entre los objetivos que tienen el control interno de tecnología de información están los siguientes:

- Procesar atributos de la información
- Apoyar a la protección del activo
- Apoyar la eficiencia operativa
- Emplear los recursos de tecnología de información del área de los sistemas y tecnologías
- Brindar apoyo competitivo para el sector de las entidades intermediarias de las distribuidoras de telefonía en el país

- Mantener una cultura informática adecuada en el sector en estudio
- Habilitar mecanismos de equilibrio en las operaciones
- Mantener la continuidad y consistencia de las operaciones
- Preservar las condiciones de la información

El establecimiento de procedimientos de control es responsabilidad directa del área de sistemas, dichos procedimientos deben permitir la instrumentación necesaria para lograr los objetivos.

Procedimientos de control en tecnología de información

Los procedimientos de control son mecanismos de administración que una empresa establece con la intención de lograr sus objetivos de control. El conjunto de lineamientos, prácticas y estándares a tomar en cuenta para el desarrollo del modelo de control interno debe estar orientado en cuatro aspectos fundamentales la Figura 1 ilustra los componentes y las características a considerar para un adecuado control interno en el área de un sistema de información.

Dominios, objetivos y características para el procesamiento de la información

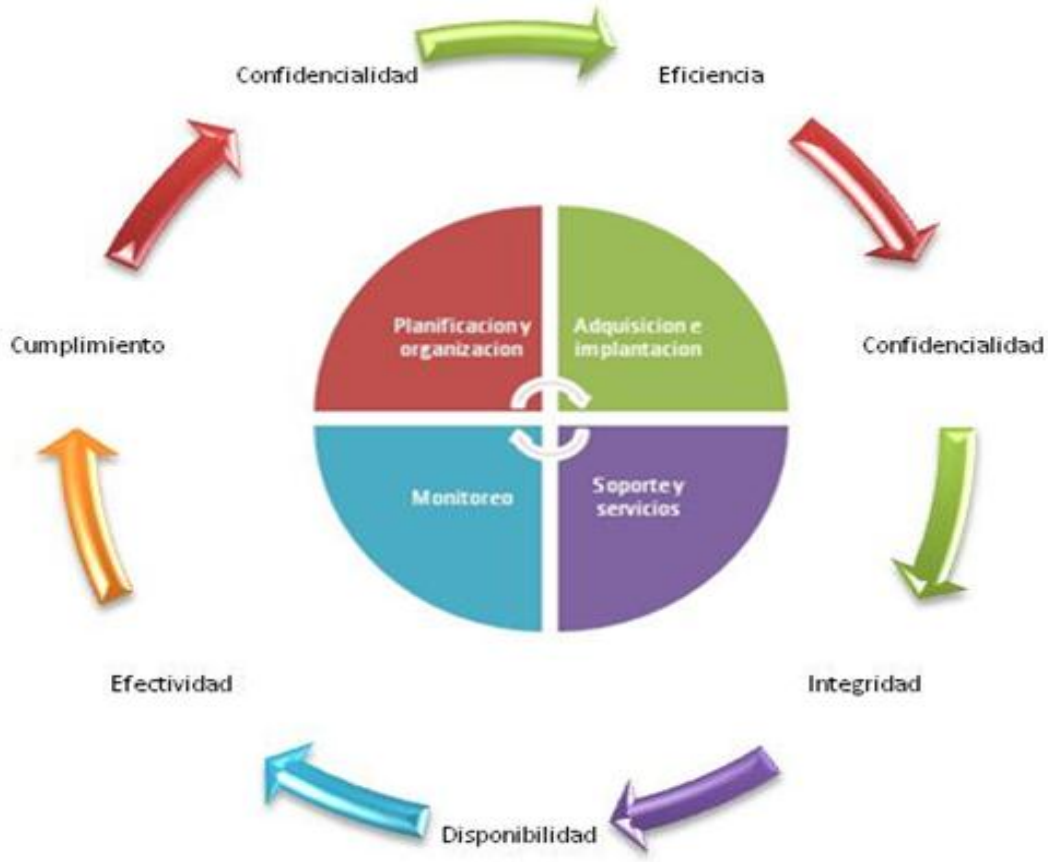


Figura 1 Componentes para el procesamiento de la información

Fuente: Adaptado de COBIT 5

Detalles de los componentes de dominio necesarios para el procesamiento de la información

Para determinar los procesos a seguir encaminados al cumplimento de los objetivos que establece Cobit conjuntamente con los procesos catalizadores se detallan en la Tabla 3 los 34 procesos necesarios para mantener la información integra, confidencial y disponible para los usuarios a cargo del manejo y uso de las bases de datos.

Tabla 3 Objetivos de control y sus procesos

Objetivos de Control	Procesos
Planear y organizar	• Definir el plan estratégico de TI • Definir la arquitectura de la información • Determinar la dirección tecnológica • Definir procesos, organización y relaciones de TI • Administrar la inversión en TI • Comunicar las aspiraciones y la dirección de la gerencia • Administrar recursos humanos de TI • Administrar calidad • Evaluar y administrar riesgos de TI • Administrar proyectos • Administración de Calidad
Adquirir e implantar	• Identificar soluciones automatizadas • Adquirir y mantener el software aplicativo • Adquirir y mantener la infraestructura tecnológica • Facilitar la operación y el uso • Adquirir recursos de TI • Administrar cambio
Monitorear y evaluar	• Monitorear y evaluar el desempeño de TI • Monitorear y evaluar el control interno • Garantizar cumplimiento regulatorio • Proporcionar gobierno de TI
Prestación y soporte	• Definir y administrar niveles de servicio • Administrar servicios de terceros • Administrar desempeño y capacidad • Garantizar la continuidad del servicio • Garantizar la seguridad de los sistemas

	• Identificar y asignar costos • Educar y entrenar a los usuarios • Administrar la mesa de servicio y los incidentes • Administrar la configuración • Administrar los problemas • Administrar los datos • Administrar el ambiente físico • Administrar las operaciones

Fuente: Adaptado de Cobit 5(ISACA, 2012)

Recursos necesarios para alcanzar los objetivos de control interno para el área de tecnología de información

- Datos: dentro de estos se debe considerar la información tanto interna como externa, estructurada o simple, gráficos, informes, estadísticos en fin deben considerarse todos los objetos de información

- Aplicaciones: se debe considerar los tipos de sistemas de información que integran las entidades intermediarias de las empresas distribuidoras de telefonías ya sea que por la magnitud o simplicidad de las operaciones se lleven por medios sistemáticos o manuales

- Tecnología: se incluye hardware o software dentro de la entidad, los sistemas con los que cuenta ya sean operativos o administrativos, multimedia, bases de datos u otros recursos propiamente involucrados en los activos de la entidad

- Instalaciones: se deben asegurar de la existencia y debida adecuación de los recursos tecnológicos de la entidad, que sean capaces de alojar de forma segura y oportuna la información, así como de dar soporte a los sistemas de información

- Recurso humano: se debe considerar el factor más importante y complejo ya que el personal administrativo, operativo o cualquier otro usuario debe poseer ciertas características fundamentales para la productividad de los sistemas de información; estos

deben ser capaces de cumplir un perfil de personal capaz de planear, adquirir y prestar servicios, dar soporte y monitorear los procesos de las tecnologías de información

1.2 Evaluación de los riesgos informáticos

En los últimos años los riesgos informáticos se han enmarcado dentro del diario vivir de las diversas gestiones de los negocios, siendo particularmente abordados por técnicos debido a la complejidad de los mismos; sin embargo saber administrar los riesgos informáticos dentro del entorno de las gestiones de las entidades es el factor clave en las empresas, debiendo involucrar cada área de la empresa, ya que un impacto en la parte informática podría afectar a cualquier parte integral de la entidad. Es por lo anterior que la administración de dichos riesgos juega un papel importante en la protección de la información de las empresas.

Dado lo anterior se establece que la seguridad de la información clasificada como aceptable como tal requiere los siguientes elementos:

- Integridad: se refiere a la protección de la información de cualquier inconsistencia o alteración que podría verse afectada y cuya malversación pudiese causar fraudes, imprecisiones o malas decisiones empresariales.

  Es la cualidad de un mensaje, comunicación o archivo, que permite comprobar que no se ha producido manipulación alguna en el original, es decir, queno ha sido alterado.
  Cuando un usuario, programa o proceso modifica o borra los datos importantes que son parte de la información, se registra esta modificación para asegurar la confiabilidad de los datos.

  La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la información.

  Para que la información sea integra debe de estar completa y libre de errores. Del mismo modo concordar con las metas de calidad de la información las cuales son: la completitud y la precisión.

- Disponibilidad: este elemento enmarca la importancia que la información pueda siempre estar disponible para ser usada, ya que la falta de disponibilidad pudiese ocasionar retrasos, pérdida de tiempo y en ocasiones causar un incumplimiento en las funciones de los usuarios que manipulan dicha información. Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. Supone que la información pueda ser recuperada en el momento en que se necesite, evitando su pérdida o bloqueo.

  Hay que tener en cuenta que, tanto las amenazas como los mecanismos para contrarrestarlas, suelen afectar a estas tres características de forma conjunta. Así por ejemplo, fallos del sistema que hacen que la información no sea accesible pueden llevar consigo una pérdida de integridad. Generalmente tienen que existir los tres aspectos descritos para que haya seguridad.

  Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de seguridad. Por ejemplo, en un servidor de archivos en red, se priorizará la disponibilidad frente a la confidencialidad. En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

  Como tal la disponibilidad es uno de los fines que persigue la calidad de la información, ya que para que la información esté disponible debe ser accesible y cumplir con los estándares de seguridad.

- Confidencialidad: dentro de este se establece el acceso de la información, ya que solo puede ser usada una vez se tenga la debida autorización de los responsables del manejo de las bases de datos, puesto que la falta de confidencialidad resultaría en una pérdida de confianza, mala reputación para el ente garante de la conservación de la información, acciones legales que podrían emprender los afectados, entre otros. Requiere que la información sea accesible únicamente por la entidades o personas autorizadas, de esta manera, se dice que un documento o información es confidencial si y solo si puede ser comprendido por la persona o

entidad que va dirigida o este autorizada. Por ejemplo una medidas de seguridad podemos mencionar cifrado asimétrico o cifrado simétrico.

Un método eficaz para proteger la información es en primer lugar establecer los responsables de la gestión de la información en cada entidad, es por lo tanto que la alta dirección conjuntamente con los directores y personal operativo del área de tecnología de información, administradores del área de negocios son los responsables de garantizar la salvaguarda oportuna y secreta de la información dentro de sus instalaciones y es por lo anterior que la legislación Salvadoreña debe estar obligada a velar porque la protección de la información se realice de manera apropiada.

Para que exista confidencialidad debe existir un acceso restringido a la información de calidad, esto se logra a través de accesos restringidos, políticas de controles de accesos y estándares de la seguridad de la información, evitar la divulgación de información clasificada.

1.2.1 Evaluación de los riesgos de los sistemas de gestión de la seguridad de la información

La evaluación del riesgo es una actividad que forma parte del modelo PDCA (Planear, Hacer, Chequear y Actuar) este modelo está según la ISO/IEC 27002: 2005 que define que la evaluación del riesgo debe ir en la fase del chequeo. Dentro del proceso de los requerimientos generales para un sistema de gestión de la seguridad de la información, al establecer dicho sistema se debe dejar en claro dos aspectos fundamentales; el primero la identificación de los riesgos, es en este sentido que se procede a la identificación de los activos dentro del alcance de la entidad, las amenazas a las que están expuestos dichos activos, las vulnerabilidades que pueden surgir de las amenazas, los impactos que puedan desencadenar las perdida de la confidencialidad, integridad o disponibilidad de los activos; y el segundo aspecto debe ser el análisis y evaluación de riesgos orientados a calcular el impacto que podría darse debido a una falla de seguridad, así como también efectuarse el cálculo sobre la probabilidad que ocurran fallas producidas por las vulnerabilidades que están dentro de la entidad y finalmente se debe hacer un cálculo de los niveles de riesgo determinando el riesgo aceptable o aquellos que requieran tratamiento.

Para el tratamiento de los riesgos que han sido identificados dentro del análisis de aceptación del riesgo se debe tomar en cuenta lo siguiente:

- La aplicación de controles adecuados
- Aceptar los riesgos de una manera congruente y objetiva
- En la medida de lo posible evitar los riesgos
- Y en situaciones que se permitan realizar una transferencia del riesgo a otras entidades

1.2.2 Amenazas, riesgos, vulnerabilidades y controles de tecnología de información

Las amenazas se refieren a cualquier circunstancia susceptible de lograr que la información o los sistemas que la soportan sufran una pérdida de confidencialidad, integridad o disponibilidad. La vulnerabilidad por su parte se refiere a debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un activo del sistema, mientras que el riesgo sería la probabilidad de que la amenaza actúe sobre el activo. La Tabla 4 hace referencia a los riesgos a los cuales están expuestos las diversas entidades, así como también los métodos de control que pudieren utilizar y los controles que mitigarían el riesgo.

Tabla 4 Riesgos, amenazas y vulnerabilidades

Riesgos, amenazas y vulnerabilidades	Controles			
	Métodos de Control		Controles de seguridad preventivos	Controles operativos
	Técnicos	No técnicos		
Procesamiento incorrecto de datos ya sea por errores en la operación de los medios informáticos	-Mecanismos de control de acceso. -Mecanismos de autenticación	-Políticas de seguridad -Procedimientos operativos	Asignar responsabilidades de seguridad para los sistemas	Controlar el acceso y destrucción de medios físicos
Ataques externos.	Métodos de encriptación	Seguridad física, del personal y ambiental	Mantener un plan de seguridad de sistemas	Limitar la distribución de datos a terceros

Accesos no autorizados. Fuga de información por mal uso de dispositivos externos.	Sistemas de detección de "intrusos"		Implementar controles de seguridad de personal segregación de funciones	Implementar herramientas de control de virus informáticos
Debilidad para garantizar la recuperación de la infraestructura de TI Espionaje industrial Ataques internos Hacker, Cracker Crimen cibernético Terrorismo				Asegurar los centros de cómputo. Procedimientos para y recuperación de información. Proteger las computadoras personales y móviles

Elaboración propia

1.2.3 Componentes de un sistema de seguridad de la información

Un sistema integral de seguridad al menos debe de comprender componentes que garanticen la seguridad de la información y que estén de acuerdo al marco de gestión que la entidad implementa a la vez que sus controles sean realizados de conformidad a lo estipulado en este.

Los siguientes son los componentes necesarios para garantizar la seguridad de información:

- Elementos administrativos
- Definición de una política de seguridad
- Segregación y organización de funciones y responsabilidades
- Seguridad física y lógica
- Prácticas de seguridad de empleados de todas las áreas que comprenden la entidad

- Elementos y procedimientos técnicos y legales
- El correcto gestionamiento de controles por parte de los profesionales a cargo

1.3Evaluación de la seguridad de las tecnologías de información

El uso inadecuado de las gestiones de la seguridad de la información comienza desde la utilización de los métodos de entrada de la información que son operados por la parte humana y estos están a expensas durante todo el procesamiento de la misma; es por ello que el factor humano es visto como el eslabón más débil en la parte de las tecnologías de información y a la vez se visualiza la necesidad de implantar un sistema que documente con metas claras de seguridad y evaluación de riesgos a los que están expuestos las entidades.

Al definir el enfoque para el desarrollo de la evaluación de riesgos se debe principalmente establecer la metodología adecuada para dicha evaluación de los sistemas de gestión de la seguridad de la información, sin dejar de lado las necesidades de la entidad; se debe contar con el desarrollo de criterios para la aceptación de riesgos y para la determinación del nivel aceptable de riesgo.

Los enfoques relacionados a la evaluación de la seguridad de la información a pesar de estar orientados primordialmente en la protección y salvaguarda de la información, estos también deben orientarse a la adecuada y correcta gestión de la información y es, en este sentido que se debe evaluar a través de los siguientes fundamentos:

- Formación y desempeño del personal
- Políticas de la entidad
- Procedimientos a realizar en la gestión de la seguridad de la información
- Herramientas a utilizar para la conservación de la información
- Valoración (acreditación) que posean o aspiren las entidades
- Evaluación (certificación) que posean o aspiren las entidades

Dentro de la evaluación de la seguridad debe existir un monitoreo y revisión de las estipulaciones, procedimientos y políticas que han establecido las entidades previamente en este sentido se deben abordar los siguientes elementos:

Lo siguiente son las acciones que deben estar encaminadas a la evaluación de la seguridad a través de controles y políticas de seguridad de acuerdo con la ISO/IEC 27002, mejores prácticas generalmente aceptadas, ITIL entre otras.

Principalmente las evaluaciones se deben orientar en lo siguiente:

- La protección y la no divulgación de datos personales
- Protección de la información interna
- Protección de los derechos de propiedad intelectual
- La política de seguridad de la información
- Asignación de la responsabilidad de seguridad de la información
- Escalamiento de problemas
- Gestión de la continuidad del negocio

Relacionado a lo anterior deben gestionárseles las evaluaciones de los siguientes apartados a fin de poder realizar una evaluación objetiva de la seguridad de la información que maneja la entidad.

- Organización de la información de seguridad
- Administración de recursos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Administración de las comunicaciones y operaciones
- Control de accesos
- Adquisición de sistemas de información, desarrollo y mantenimiento
- Administración de los incidentes de seguridad
- Administración de la continuidad de negocio
- Cumplimiento (legales, de estándares, técnicas y auditorías)

Evaluación del tratamiento de los riesgos

Esta evaluación corresponde al hecho de realizar una verificación de las acciones que a continuación se detallan:

- Aplicación de los controles apropiados y necesarios para el proceso
- Aceptación de los riesgos, siempre que se hayan realizado los procedimientos estipulados según las políticas de cada entidad
- En la medida de lo posible evitar los riesgos
- Transferencia de riesgos comerciales hacia otras entidades como aseguradoras y/o proveedores

1.4 Herramientas y técnicas para el aseguramiento de la información

1.4.1 Gestión de las tecnologías de información

La gestión de la tecnología de información consiste en la aplicación de los procesos de la administración (planificación, ejecución, seguimiento y control) a los diversos aspectos relacionados a los bienes y servicios de tecnología de información lo cual incluye aspectos como: gestión de procesos relacionados con la infraestructura de tecnologías de información, gestión de proyectos de infraestructura de tecnologías de información, gestión de proyectos de desarrollo de información, y gestión de requerimientos relacionados a los sistemas de información en la producción.

Por lo que en la actualidad existen diversos marcos técnicos para salvaguardar mediante controles los activos de la entidad así como también la salvaguarda de la información que se maneja.

1.4.2 Metodología COBIT

COBIT 5 provee un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y gestión de las tecnologías de información corporativas es decir, beneficiando a las entidades en la creación de un valor optimo, manteniendo el equilibrio entre la generación de costo-beneficios.

Los objetivos de control para la información y la tecnología de información, brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas del COBIT representa el consenso de los expertos. Están enfocados principalmente en el control.

Criterios de control de metodología

Para satisfacer las necesidades de la entidad, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos a COBIT como requerimientos de información de calidad y de seguridad, ya que este Marco define los siguientes criterios de información: la eficacia, la eficiencia, la integridad, la fiabilidad, la disponibilidad, la confidencialidad, y conformidad.

A continuación se presenta mediante la Figura 2 el conjunto de lineamentos y estándares internacionales, bajo el enfoque COBIT 5, con el objeto de mostrar el marco de referencia, que clasifica los procesos de las unidades de tecnología de información de las organizaciones o entidades, enfatizando los cuatro dominios que hace referencia el marco de gestión.

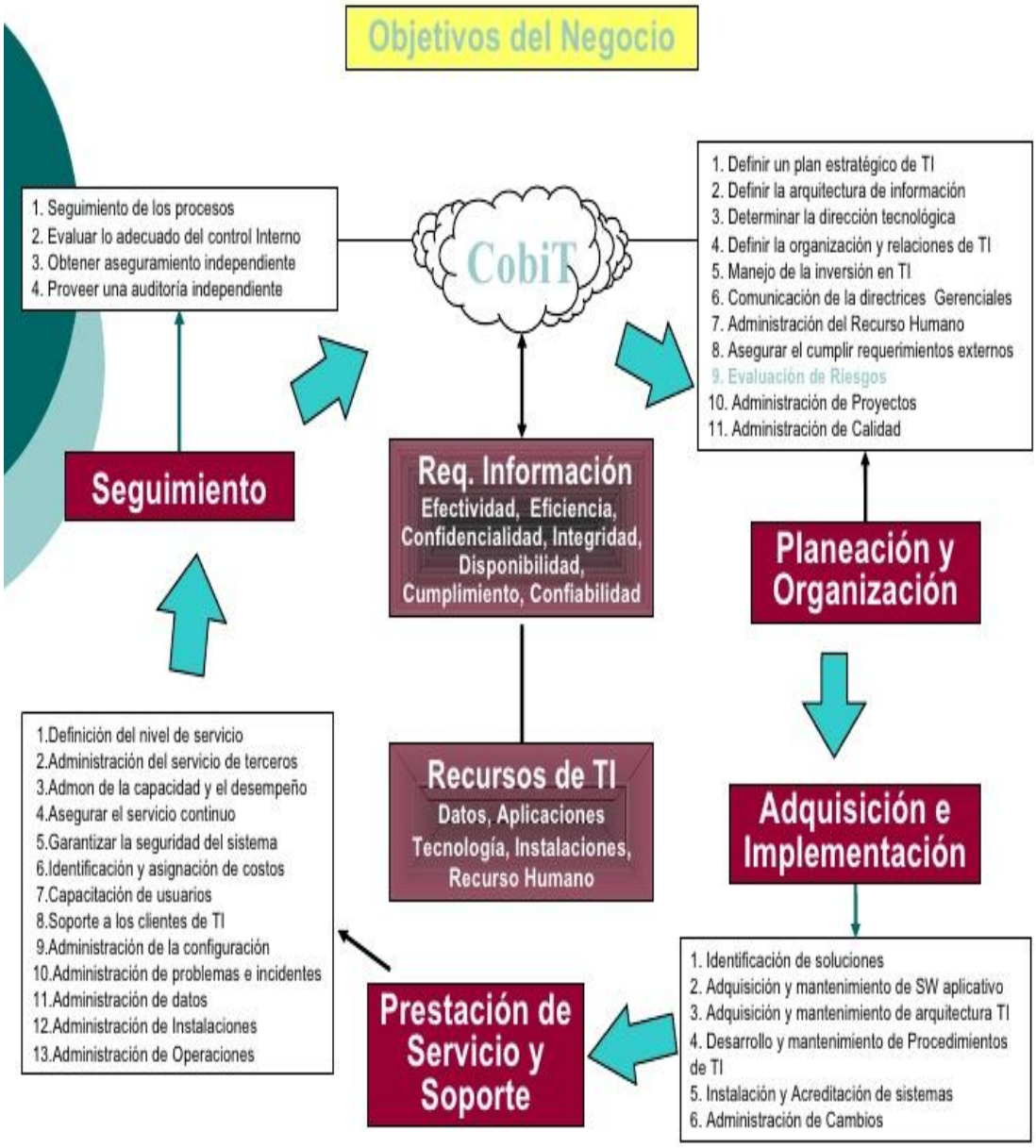


Figura 2 Objetivo del negocio según COBIT

Fuente: capturado de http//cobit.isaca.org(Todos los derechos reservados)

1.4.3 Metodología ITIL

Librería de Infraestructura de Tecnologías de Información (en adelante ITIL) es un modo sistemático de planear la prestación de servicios de tecnologías de información y constituye la estructura utilizada por

la mayoría de las organizaciones que se identifican con la práctica de la gestión de servicios. Dicho marco describe el modo de dirigir las tecnologías de información como un negocio desde la creación de una estrategia de servicios hasta el diseño de los negocios: la planificación, creación continua de los servicios de forma constante. Proporciona las herramientas que tecnologías de información necesita para convertirse en una ventaja competitiva para cualquier organización.(Huercano, 2007)

Objetivos de la metodología

ITIL como metodología propone el establecimiento de estándares que nos ayuden en control, operaciones y administración de los recursos. Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos los necesiten, lo que nos lleva a una mejora continúas además, otra de las cosas que propone es que para cada actividad que se realice se debe de hacer la documentación pertinente, ya que esta puede ser de gran utilidad para otros miembros del área.

Fases de la metodología

Fase 1: Gestión de incidentes

Son objetivos primordiales es restablecer el servicio lo más rápido posible para evitar que el cliente se vea afectado, con la finalidad de que se minimicen los efectos de la operación.

Se manejan cuatros procesos básicos que son: propiedad, monitoreo, manejo de secuencias y comunicaciones.

Fase 2: Gestión de problemas

El objetivo de este proceso es prevenir y reducir el máximo los incidentes, y estos nos lleva a una reducción en el nivel de incidencia. Por otro lado nos ayuda a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos.

En este proceso lo que se busca es que se pueda tener pleno control del problema, lo cual se lograra dando un seguimiento y monitoreo al problema.

Se manejan dos fases: la primera está relacionada con lo que es control del problema y la segunda es con el control del error.

Fase 3: Gestión de cambios

El objetivo de este proceso es reducir los riesgos tanto técnicos, económicos y de tiempo al momento de la realización de cambios.

Se tiene un registro y clasificación del cambio a realizar, se pasa a la fase de monitoreo y planeación, si el rendimiento es satisfactorio se da la aprobación del cambio, en caso de que el rendimiento sea malo se pasa a la fase de reingeniería hasta que el proceso funcione adecuadamente.

Fase 4: Gestión de los activos los servicios y configuración

Su objetivo es proveer con información real y actualizada de lo que se tiene configurado e instalado en cada sistema del cliente.

Este proceso es de lo más complejo, ya que se mueve bajo cuatro vértices que son: administración de cambios, administración de liberaciones, administración de configuraciones y la administración de procesos diversos.

El nivel de complejidad de este modelo es alto, ya que influyen muchas variables y muchas de ellas son dinámicas, por lo que al cambiar una o varias de ellas afectan al sistema en general, por lo que no fácilmente se puede manipular.

Fase 5: Gestión del catálogo de servicios (entregas)

Su objetivo es planear y controlar exitosamente la instalación de software y hardware bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas, ambiente real.

Este proceso marca la transición que se da de acuerdo a los ambientes por los que se va dando la evaluación del proyecto.

En el ambiente de desarrollo se tiene que realizar liberaciones de las políticas, la liberación de la planeación, el diseño lógico de la infraestructura que se va implementar y la adquisición de software y hardware están entre los ambientes de desarrollo y de pruebas controlada.

En el proceso de entrega del servicio es el punto en que el usuario hace uso del servicio y no sabe que detrás del servicio que está recibiendo hay un sin fin de actividades y decisiones.

1.5 Marco técnico

Existen diversidad de estándares, marcos de integración, enfoques entre otros aplicables a las tecnologías de información; dado lo anterior para el diseño de un control interno basado en riesgos de tecnologías de información, se establece los estándares y marcos de trabajos más relevantes considerados en el marco Cobit 5. La siguiente tabla detalla la normativa técnica aplicable para el diseño de un control informático.

Tabla 5 Normativa técnica sobre sistemas de información.

	Normativa	Descripción
NORMAS ISO	ISO 27000	Contiene conceptos y definiciones que se emplean en toda la serie 27000. Cuenta con un vocabulario para la aplicación de cualquier estándar para evitar distintas interpretaciones de conceptos técnicos y de gestión
	ISO 27001	Suministra las fases para la implementación de la seguridad de la información en una organización: establece que esta división se hace en cuatro fases: planificación; implementación; revisión y mantenimiento; y mejora.
	ISO 27002	Define una serie de objetivos de control y gestión, por medio de dominios: 1. La política de seguridad. 2. Los aspectos organizativos de la seguridad de la información. 3. La gestión de activos. 4. La seguridad ligada a los recursos humanos. 5. La seguridad física y ambiental. 6. La gestión de las comunicaciones y de las operaciones. 7. Los controles de acceso a la información. 8. La adquisición, desarrollo y mantenimiento de los sistemas de información. 9. La gestión de incidentes en la seguridad de la información.

		10 .La gestión de la continuidad del negocio. 11 .Los aspectos de cumplimiento legal y normativo.
	ISO 27003	Constituye una guía de implementación de SGSI e información acerca del uso del modelo PDCA (planear, Hacer, Verificar y Actuar) y de los requerimientos de sus diferentes fases que comprenden desde la producción del proyecto hasta la creación del modelo para la autorización de la gerencia.
	ISO 27004	Especifica las métricas y las directrices aplicables para determinarla eficacia de un SGSI y de los controles relacionados.
	ISO 27005	Establece las políticas para la gestión del riesgo en la seguridad de la información. Brinda un apoya los conceptos generales especificados en la norma ISO 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
	ISO 27006	Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información
COBIT 5		Provee una base para crear un valor óptimo de TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los riesgos y el uso de recurso permitiendo abarcar diversas áreas de TI de

		una entidad permitiendo que la información sea de calidad, fiable y eficiente, así como mantener los riesgos a un nivel aceptable. Además la importancia del COBIT radica en : Dar más énfasis a las entidades sobre qué es lo que esperan de la información y tecnologías. Tratar en qué medida la información que se va recopilando se va resguardando de forma íntegra. Generar confidencialidad, qué medidas se toman para mantener el acceso restringido de la información. ✓ Eficiencia de la obtención de la información,
	SERIE ISO/IEC 31000	Esta serie proporciona procesos relativos a la gestión de riesgos en los dominios, por lo que es un estándar que provee servicios y directrices sobre la gestión de riesgo.
	SERIE ISO/IEC 38500	Esta serie establece directrices básicas de orientación a la alta dirección para favorecer el correcto gobierno de las tecnologías de información.
ITAF 3ª Edición.		Define procedimientos de auditoría y aseguramiento de SI, por lo que se tomara en cuenta en la investigación, por proporcionar una guía para el cumplimiento del control interno a los sistemas de información.
		Este modelo introduce novedades al Marco

COSO III E l a b o		Integrado de Gestión de Riesgos las cuales son: • Mejora de la agilidad de los sistemas de gestión de riesgos para adaptarse a los entornos • Mayor confianza en la eliminación de riesgos y consecución de objetivos • Mayor claridad en cuanto a la información y comunicación. Por otra parte incluye 17 principios que conllevan sus cinco componentes u se debe implementar en toda organización.
rITIL (Information aTechnologies tnfrastructure Library). i ó		Brinda un enfoque sistemático del servicio de TI centrado en los procesos y procedimientos, y establecimiento de estrategias para la gestión operativa de la infraestructura de TI.
n COSO P r o p i a		Es una comisión de control interno orientado a proporcionar liderazgo intelectual frente a tres temas interrelacionados: 1. La gestión del riesgo empresarial (ERM), 2. El control interno, y 3. La disuasión del fraude

1.6 Marco legal

Con los precedentes de los riesgos relacionados con las tecnologías de información en El Salvador, existen en materia legal, leyes generales y específicas relacionadas a los sistemas de información, con el objeto de normar el uso y manipulación de datos, así también establece lineamientos legales de las

entidades que manipulan dicha información. La siguiente Tabla establece la normativa legal relacionada con el manejo y aseguramiento de la información.

Tabla 6 Marco legal aplicable a los sistemas de información.

NORMATIVA	DESGLOSE	DESCRIPCIÓN
LEY DE TELECOMUNICACIONES	CAPÍTULO ÙNICO Art.1 Regulaciones del sector de telecomunicaciones en cuanto al servicio de telefonía	Toda entidad que realice operaciones en el sector de telecomunicaciones, estará regulada por la Superintendencia general de electricidad y comunicaciones que tendrá por objeto de velar por el cumplimiento de las obligaciones de tanto las operaciones que realicen como del manejo de la información.
	Art. 2 Fines que persigue la ley	Aplicación de normas en cuanto al acceso de las comunicaciones a todos los sectores de la población, así como conservación de los derechos de los usuarios, operadores, proveedores de servicios en general y la mejora del servicio a través de la competitividad en el sector de telecomunicaciones.
	Art. 5 A Lineamientos en cuanto a los servicios de telecomunicación basada en normas de calidad.	Los operadores de telecomunicaciones están en la obligación de disponer de sistema que permita acreditar la calidad de sus servicios, quienes tendrán que informar a la Superintendencia general de electricidad y comunicaciones para su verificación de acuerdo a sus reglamentos establecidos, asimismo los servicios con respecto a duración de llamadas, servició de datos, mensajería texto multimedia, pliego tarifario, coberturas, atención al cliente entre otras.

		Esto con el fin de aplicar métodos de control en cuanto al manejo de la información así como de sus procesos.
	TÌTULO 2 Art. 7 Concesión de servicio	Establece los requisitos de los operadores en cuanto a la explotación de servicios de telefonía que es autorizada por la Superintendencia general de electricidad y telecomunicaciones para un periodo de treinta años.
	TÌTULO IV Art. 29 Derechos de los usuarios.	Estipula los derechos que tiene los usuarios entre los que enfatizan: El acceso a los servicios públicos de telefonía manteniendo la comunicación sin interferencia ni intervenciones, confidencialidad de datos personales como de protección, asimismo como de recibir compensación en cuanto a la desconexión de servicio de manera arbitraria sin previa autorización de las operadoras.
	Art.30-A Obligaciones del operador	Menciona que las operadoras deben llevar un registro de todos los usuarios, en relación a información de datos así como de la entrega de información con fin de cooperar con instituciones de seguridad pública en caso de delitos.
	CAPÌTULO V-BIS Art.42-D Encriptación de la información	Es obligación de los operadores de redes de telecomunicación de emplear sistema que mediante técnica o programas se cifre o se codifique información de los usuarios con el fin que sea inaccesible e ilegible para personas no autorizadas.

LEY DE ACCESO A LA INFORMACIÓN	Art.6 Datos personales	Se refiere a la información concerniente a sus datos con respecto a su nacionalidad, domicilio, patrimonio, dirección electrónica, numero de telefónica entre otros.
	Información reservada	Es la información pública cuyo acceso se restringe de manera expresa que ponga en peligro la vida, la seguridad, la integridad de las personas, en razón de un interés general.
	Información confidencial	Es toda aquella información cuyo acceso se limita por mandato constitucional o legal en razón de un interés jurídicamente protegido que pueda afectar el derecho a la intimidad personal, al honor, imagen cuya revelación será considerada como invasión a la privacidad de la persona.
	Art. 35 Lista de registro o sistemas de datos personales	Las empresas que manejen por cualquier título, registros o sistema de datos deberán notificar dicha información al Instituto de acceso a la información pública, esto con el fin de mantener una actualización del mismo y manteniendo un protocolo de seguridad como medida de confidencialidad.
CÓDIGO DE COMERCIO	Art. 455 Resguardo de la información en medios electrónicos	El código de comercio hace énfasis en el resguardo de la información por cualquier medio; esto queda a juicio profesional el uso.

CONSTITUCIÓN DE LA REPUBLICA DE EL SAVADOR	Art. 2 Derechos individuales	Señala de los derechos que tienen la población en cuanto a la protección de su integridad y conservación y defensa de los mismos, garantizando el derecho a la intimidad personal
LEY DE FIRMA ELECTRÓNICA		Esta ley busca contar con un sistema que brinde la seguridad de las operaciones electrónicas, acompañado de la confianza para los usuarios al efectuar dichas operaciones, además de brindar certeza jurídica al dar un valor igual a la firma autógrafa y a mecanismos tecnológicos que aseguren la identidad y contenido.
	Art. 4 principios generales	Establece los principios por la cual las entidades reguladas por esta ley deberá cumplir, las cuales son: autenticidad, integridad, confidencialidad, equivalencia funcional, no repudiación y neutralidad tecnológica.
	Art. 5 tratamiento de datos personales	Establece las reglas los cuales están sujetas los prestadores de servicios de almacenamiento tecnológico para el tratamiento de los datos personales
	Art. 7 equivalencia funcional	Determina que los mensajes de datos se tendrá por jurídicamente equivalente al contenido de aquellas que son emitidos de manera convencional
	Art. 12 formas de conservación de documentos	Establece que la obligación de conservar documentos, registros e información en documentos electrónicos lo puede realizar a cuenta propia, o a través de terceros, lo cual

		debe registrarse ante la SIGET
	Art. 13 requisitos para la conservación de documentos.	Determina que la información contenida conste por escrito, si la información está disponible para consulta, además de cumplir los requisitos de: que la información pueda ser consultada, que se mantenga el formato en que se generó y que conserve todo dato de origen y el destino.
	Art.14 Garantías mínimas que debe cumplir el sistema de almacenamiento tecnológico.	Establece que el procedimiento utilizado para el almacenamiento de documentos electrónicos debe garantizar que mantenga en forma íntegra, nítida y segura, la fecha en que fue almacenado, la recuperación del documento y que cumpla con los reglamentos de la SIGET
	Art. 15 Declaración de prácticas de almacenamiento de documentos	Establece que toda persona jurídica que realice el almacenamiento de documentos electrónicos para terceros, debe redactar una declaración de prácticas de almacenamiento con la información que se detalla en este artículo.
	Art. 18 Supervisión y control	Los prestadores de servicios de almacenamiento tecnológico quedara sujeto a las facultades de supervisión y control de la unidad de firma electrónica de la SIGET
	Art. 28 Uso de la firma electrónica certificada por representantes de personas jurídicas.	Determina que los certificados electrónicos de personas jurídicas para los dispositivos electrónicos utilizados en una empresa, como computadoras, servidores, entre otros deberán ser solicitados por medio de administradores y representantes legales

	Art. 48 Medidas para garantizar los servicios de certificación	Establece que la SIGET podrá adoptar medidas preventivas para garantizar la confiabilidad de los servicios, para tal efecto podrá dictar las normas y reglamentos técnicos necesarios

Elaboración Propia

1.7 Diseño de un control interno informático

Las entidades dentro del proceso de diseñar controlesinternos, tienen que elaborar sus procedimientos integrales, los cuales son la base primordial para poder desarrollar adecuadamente sus operaciones o actividades, establecer responsabilidades de los funcionarios, información, medidas de seguridad y objetivos que participen en el cumplimiento con la misión institucional propuesta. (Mejia Guardado, 2008)

El control interno aparte de ser una política de gerencia, se constituye en las directrices principales de cualquier empresa para modernizarse, cambiar y producir los mejores resultados, con calidad y eficiencia. Por lo que al diseñar un modelo de control interno informático se debe considerar lo siguiente:

- Objetivos del control interno, estableciendo como prioridad la seguridad y protección de la información del sistema y de los recursos informáticos de la entidad.
- Promover la confiabilidad, integridad y disponibilidad de la recepción de los datos, su procesamiento en el sistema.
- Implementar los métodos, técnicas y procedimientos necesarios para obtener el eficiente desarrollo de las funciones, actividades y tareas.
- Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.

Además, se debe considerar elementos fundamentales del control interno.

- Controles internos sobre la organización del área de informática
- Controles internos sobre el análisis y desarrollo del sistema
- Controles sobre operaciones del sistema
- Controles sobre los procedimientos de entradas de datos, el procesamiento de la información

- Controles sobre seguridad

Consideraciones preliminares:

El proceso de evaluación involucra la identificación de las debilidades potenciales, así como el diseño o implementación de los controles adecuados que la mitigan. La evacuación de los controles existentes en entornos informáticos dentro de una entidad, normalmente se realizan para determinar la eficacia u eficiencia de esos controles.

Una estrategia para conocer y comprender los controles existentes en el ambiente informático en una organización es entrevistar al personal usuario del sistema, pues son los que tiene mayor conocimiento de las operaciones que realizan.

Estudio inicial: conocer las características del sistema

Un sistema de información interactúa entre sí para procesar la información y distribuirla de la mejor manera a través de todos los niveles de la organización en función de sus objetivos. Para que sea un verdadero sistema informático, debería existir varios sistemas interconectados entre sí, que se comuniquen unos con otros a través de grupos de reglas y condiciones: protocolos.

Por lo que las características de los sistemas informáticos que debemos conocer están para el conocimiento del sistema de información:

- Procesamiento uniforme de las transacciones
- Posibilidades de errores e irregularidades no detectadas
- Posibilidad de mayor supervisión gerencial
- Rastreo de las transacciones
- Segregación de funciones incompatibles
- Iniciación automática de eventos
- Los controles manuales dependen de la confiabilidad del procesamiento de datos
- Los controles de aplicación depende de los controles generales

Identificación de riesgos

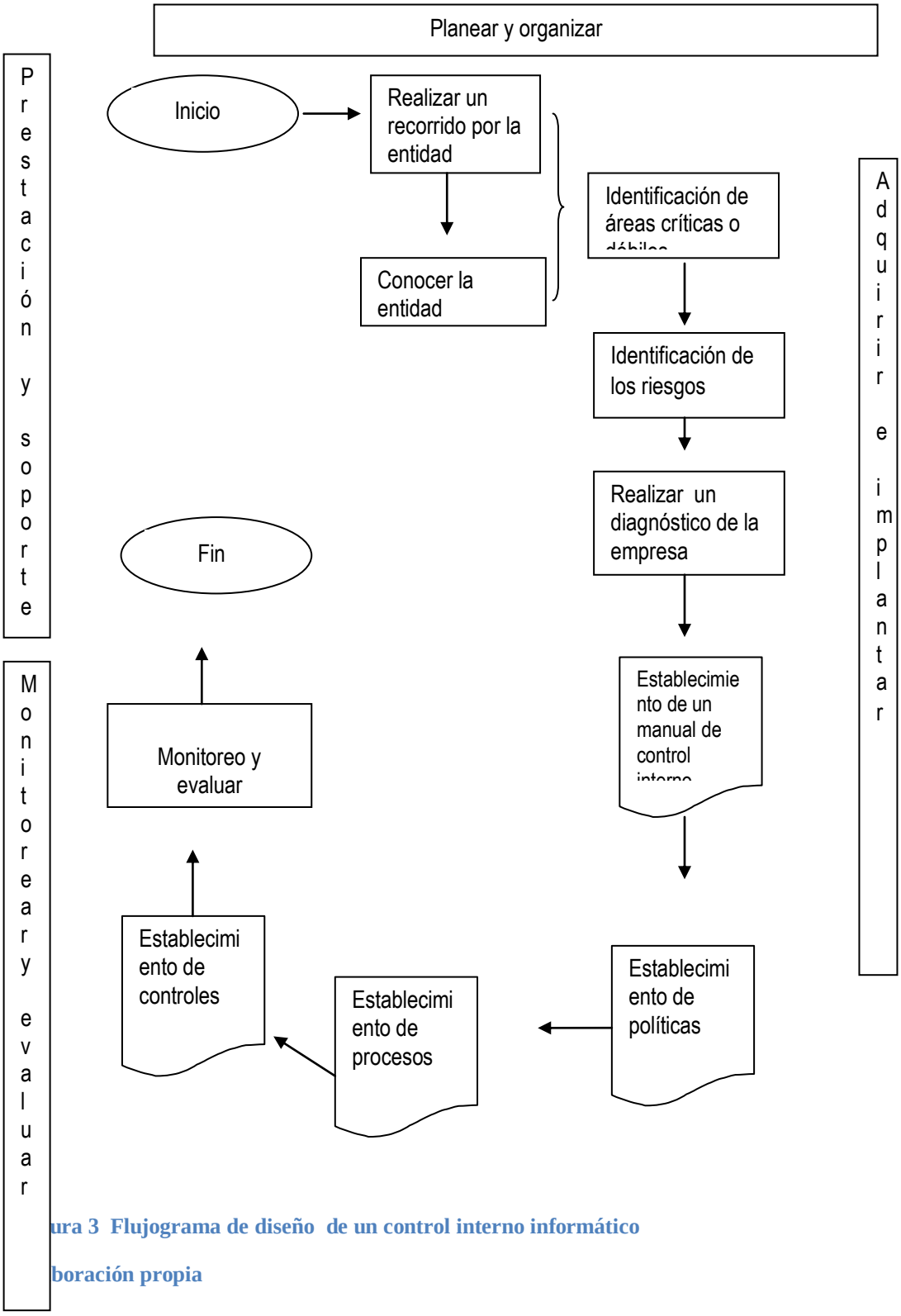
Este constituye uno de los elementos más importantes para propiciar que la entidad alcance una categoría.Se debe identificar y conocer detalladamente cada factor de riesgo, tanto interno como externo y por cada área de responsabilidad, por lo que es necesario obtener información precisa para cada factor de riesgo, con sus características y niveles asociados, así como las causas que originan el mismo.Algunos

tipos de riesgos asociados a las tecnologías de información son componentes del universo de riesgos a los que se encuentran propensas las entidades. Relacionados a estos riegos se encuentran tanto los riesgos estratégicos, los ambientales, riesgos de mercado, de crédito, operacionales y de cumplimiento.

- Riesgos de mercado: el cual está asociado a que un activo disminuya de valor, producto de variaciones y cambios en las condiciones de mercado. Asociado a este tipo de riesgo se encuentra la información que manejan las entidades por ello la necesidad de realizar una gestión apropiada para el tratamiento de los activos tecnológicos que se convierte en un factor clave para la gestión de las empresas.
- Riesgo operativo: Está orientado a producir pérdidas financieras producto de fallas o insuficiencias relacionadas a la entidad como lo son el personal, los sistemas la parte de tecnologías de información. De igual manera se asocia con la parte externa como lo son imprevisto a nivel de mercado de competidores y de otras circunstancias.
- Riesgos de cumplimiento: orientados a afectar la reputación de la entidad, respecto a fraudes, lavado de dinero, prestigio entre otros

En la figura 3 se establecen los procesos y documentos a seguir para el diseño de un control interno informático; se detalla el flujograma y la secuencia que se deberá llevar para lograr diseñar un control interno como tal, hasta llegar a la parte final del monitoreo y evaluación. Es importante aclarar que para efectos del desarrollo de la propuesta que se elaborará se llegará hasta la etapa del establecimiento de controles.

Flujograma



ura 3 Flujograma de diseño de un control interno informático

boración propia

Para el diseño de un control interno informático es necesario considerar las condiciones para que se pueda lograr la determinación e implantación de los procesos, procedimientos y políticas a seguir en una entidad con el fin de lograr que la información cumpla con las características principales de integridad, confidencialidad y disponibilidad y así lograr agregar valor a la entidad. La Tabla 7 detalla los pasos a seguir para lograr el diseño de un sistema de gestión de la seguridad de la información partiendo del modelo PDCA (planear, hacer, chequear y actuar) sistema que da origen a un control interno informático.

Tabla 7 Diseño de control interno informático

Pasos	Procedimiento	Detalle
Paso 1	Establecimiento de requerimientos generales	• Responsabilidad de la gerencia • Compromiso de la gerencia • Conocer el contexto empresarial tanto interno como externo de la entidad • Establecer política de control interno informático • Establecer objetivos • Establecer roles y responsabilidades para control interno informático • Comunicar importancia del objetivo de seguridad y cumplir la política • Proporcionar recursos para desarrollar, implementar, monitorear, revisar, mantener y mejorar el control interno informático • Decidir el criterio para la aceptación del riesgo y niveles de riesgo aceptado • Asegurar que se realicen las auditorías internas de control interno informático • Realizar revisiones generales del control interno informático

Paso 2	Establecer y manejar el control interno informático	• Definir alcance y limites • Definir una política • Definir el enfoque de evaluación de riesgos • Identificar los riesgos • Analizar y evaluar los riesgos • Identificar y evaluar el tratamiento del riesgo • Definir el tratamiento de los riesgos • Obtener la autorización de la gerencia para implementar y operar el control interno informático • Prepara un enunciado de aplicabilidad
Paso 3	Implementar y operar	• Definir un plan de tratamiento de riesgos • Implementar el plan de tratamiento de riesgos • Implementar los controles • Definir un sistema de métricas • Implementar programas de formación y capacitación en relación a la seguridad de la información • Gestionar las operaciones de control interno informático • Gestionar los recursos necesarios para el mantenimiento y seguridad de la información • Implementar los procedimientos y controles para la detección y repuesta de incidentes
Paso 4	Monitorear y revisar	• Ejecutar procedimientos de monitoreo y revisión • Realizar revisiones regulares de la efectividad del control interno • Medir la efectividad de los controles • Revisar la evaluación de los riesgos en los intervalos planeados • Realizar auditorías internas a intervalos planeados • Realizar una revisión gerencial del control interno • Actualizar los planes de seguridad en función de los

		nuevos hallazgos encontrados en el monitoreo y revisión • Registrar acciones y eventos que pueden haber impactado sobre la efectividad y rendimiento del control interno informático
Paso 5	Mantener y mejorar	• Implementar las mejoras identificadas • Realizar las acciones preventivas y correctivas • Comunicar las acciones y mejoras a todas las partes interesadas • Asegurar que las mejoras al control interno logren su objetivos previstos

Elaboración propia

CAPÍTULO II METODOLOGÍA DE INVESTIGACIÓN Y DIAGNÓSTICO

2.1 Tipo de estudio

La investigación se basó en un estudio de tipo hipotético-deductivo.

2.2 Unidad de análisis

Las unidades de análisis fueron las empresas distribuidoras de telefonía en El Salvador, (Gerencia o Gobierno corporativo) y los contadores autorizados inscritos en el Consejo de Vigilancia de la Profesión de la Contaduría Pública y Auditoría.

2.3 Universo y muestra

Universo

Con las unidades de análisis descritas anteriormente se identificaron los siguientes universos:

El primero está constituido por el listado de las personas naturales autorizadas para ejercer la contaduría pública y auditoría; según listado publicado por el CVPCPA con fecha 31 de diciembre de 2014

El siguiente lo conforman, las entidades distribuidoras de las telefónicas en el país según el directorio de empresas 2014, proporcionado por la Dirección General de Estadísticas y Censos.

Muestra

El número de contadores públicos a tomar en cuenta para encuestar, ha sido determinado utilizando la fórmula estadística para poblaciones finitas.

La fórmula es la siguiente:

$$n=\frac{N.P.Q.Z^2}{(N-1)e^2+P.Q.Z^2}$$

Terminología

n= tamaño de la muestra.

N= Población.

Z= Coeficiente de confianza.

e= Margen de error.

P= Probabilidad de éxitos de que la problemática exista.

Q= Probabilidad de fracaso.

Entonces:

n=? e= 0.05

N= 4184P = 0.96

Z= 1.96Q = 0.04

Sustituyendo se obtienen los siguientes resultados:

$$n = \frac{4184(0.96)(0.04)(1.96)^2}{(4184-1)_{(0.05)^2} + (0.96)(0.04)(1.96)^2} =$$

$$n = \frac{617.51}{10.60}$$

$$n = 58.25$$

$$n = 58$$

Para el cálculo de las entidades distribuidoras de telefonía, ha sido también utilizada la fórmula estadística para poblaciones finitas.

La fórmula es la siguiente:

$$n = \frac{N.P.Q.Z^2}{(N-1)e^2 + P.Q.Z^2}$$

Terminología

n= tamaño de la muestra.

N= Población.

Z= Coeficiente de confianza.

e= Margen de error.

P= Probabilidad de éxitos de que la problemática exista.

Q= Probabilidad de fracaso.

Entonces:

n=? e = 0.05

N= 58 P= 0.96

Z = 1.96 Q= 0.04

Sustituyendo se obtienen los siguientes resultados:

$$n = \frac{53(0.96)(0.04)(1.96)^2}{(53-1)_{(0.05)^2} + (0.96)(0.04)(1.96)^2} =$$

$$n = \frac{7.8184}{0.2775}$$

$$n = 28.17$$

$$n = 28$$

Para ambos casos se tomó como probabilidad de éxito el 0.96 y como probabilidad de fracaso el 0.04 debido a las estimaciones probabilísticas donde se detalla que la probabilidad de éxito sea alta no obviando la probabilidad inherente del error que como grupo de investigación se puede tolerar y que no incidiera en el estudio a realizar.

2.4 Instrumentos y técnicas a utilizar en la investigación

Encuestas

La herramienta que se utilizó para la recolección de la información fue el cuestionario, con preguntas cerradas. Se presentó en dos formatos dirigidos, uno a los contadores públicos autorizados y el segundo dirigidos a las distribuidoras de la telefonía en El Salvador. A través de la cual se recopilo la información de campo; que han sido realizadas a las unidades determinadas en la muestra.

2.5 Procesamiento de la información

Para procesar la información obtenida a través de las técnicas o instrumentos de investigación se utilizó Microsoft Excel.

2.6Análisis e interpretación de los datos

Considerando que se utilizó la herramienta de Microsoft Excel, la consolidación de respuestas de cada una de las interrogantes presentadas en el cuestionario, se presentan en términos absolutos y relativos, estableciendo la información tabulada y el análisis de los datos o resultados obtenidos a través del cuestionario. (Anexo 1)

2.7 Diagnóstico de la investigación

Se presentó el análisis de la información obtenida y recopilada, que corresponde a los datos obtenidos por los contadores públicos y las distribuidoras de las empresas de telefonía en El Salvador.

Por lo que se determinó los principales puntos que implica la temática

- Conocer en qué medida puede ayudar un diseño de control interno basado en riesgos de TI implementando lineamientos del marco de gestión de COBIT 5.
- La necesidad de implementar un control interno basadas en los estándares, lineamientos, y conjuntos de mejores prácticas, dirigidas a las tecnologías de información.
- El papel del contador público en el conocimiento y aplicación de resguardos y requerimientos de controles en los sistemas informáticos.
- Gestión del desempeño y riesgos en las tecnologías de información y comunicación.

Diagnóstico para el área de los contadores públicos.

Una vez analizados los resultados de las encuesta se determinó que no todos los contadores públicos poseen una formación en tecnologías de información; tal como lo establece la pregunta uno; los que sí, la poseen, la mitad ofertan los servicios de diseño sistema de control interno informático y estos en su mayoría trabaja con sistemas tradicionales. El grado de formación que han obtenido ha sido a través de capacitaciones siendo el área más importante desarrollada la de protección de los activos de TI; tema impartido bajo la metodología ISACA en el enfoque COBIT versión 5 que es el preámbulo para trabajo de auditorías de sistemas dado que este permite el desarrollo de políticas para el control de las tecnologías de toda la organización.

La seguridad de la información ha sido una temática poco vista por parte de los profesionales de contaduría pública; dado que cuando estos diseñan un sistema de control interno lo realizan en la mayoría de los casos bajo el enfoque o método Coso ERM este marco no es el adecuado para crear controles enfocados especialmente a determinada áreas como lo es las tecnologías de información y comunicación; si bien es cierto dicho marco, establece que la tecnología de la información y comunicación es un factor a considerar; pero es COBIT en su versión 5 el marco integrado de información que comprende estándares y lineamientos específicos bajo el enfoque basado en riesgos, así como ITIL y aspecto de la ISO 27002 los que denotan mayor incidencia en cuanto a los sistemas de seguridad de gestión de la información

Pese a conocer en algunos casos el marco COBIT, los profesionales de la contaduría pública no se consideran con la competencia profesional suficiente; tal como lo establece la pregunta cuatro respecto al

aplicar para un trabajo relacionado con las tecnologías de información, esto se debe precisamente a la ausencia de planes universitarios que provean suficiente material educativo, para que el alumno se forme en dicha área. Abonando a lo anterior los profesionales una vez graduados cubren sus horas de educación continuada en las áreas de mayor demanda como lo son contabilidad, auditoria y tributación; dado lo anterior resulta difícil encontrar capacitaciones para el área de tecnología de información dado a que, la que aplica para dicha área, nada más va dirigida al comercio electrónico, considerando además las que se encuentran no aplican para horas de educación continuada tales como CTIC de la UDB, FEPADE, INSAFORP, entre otras, , no obstante hoy en día el área de tecnologías de información y comunicación es una herramienta importante en la cual gira el mundo de los negocios y que es útil para todas las actividades que se realizan entre la que comúnmente se pueden mencionar el procesamiento de datos y los sistemas informático; es por lo anterior la importancia que el profesionales opte por especializarse u obtener conocimiento en el área de tecnologías de información; Es en ese sentido una de las limitantes que tienen los profesionales de ofertar en el campo laboral sus servicios y es importante resaltar que pese a no poseer la formación adecuada respecto de tecnologías de información existen profesionales que se desenvuelven en dicha área siendo pocos los que tienen la competencia y habilidad suficiente para desollar e implementar controles necesarios que garanticen una adecuada protección y salvaguarda de la información; y por tal razón y es en este sentido que es necesario un desarrollo actualizado de la temática, ya que en la mayoría de los casos son personas que tienen un nivel de especialización quienes desarrollan los controles para dicha área, es por ello que resultaría útil para el profesional respecto a la actualización y desarrollo del área de control interno informático además que otros de los limitantes son los costos de formación ya que son altos y esto es uno de los factores principales por lo que los profesionales no cubran su formación de dicha área, como está establecido en la pregunta dieciséis.

La importancia que el profesional de contaduría pública tenga participación en los diseños de control interno independientemente de los tipos de controles que existan, es una parte integral de sus conocimientos para afrontar cualquier desafío en un mundo de constante cambio y actualización, lo que hace que crezca las expectativas de crecimiento profesional por lo que la responsabilidad de los contadores públicos va mas allá de llevar contabilidad; considerando que el contador público no ofrece solo lo general si no también trabajos específicos en la cual este tema de diseños de control interno forma parte de los servicios en lo que la norma sobre servicios relacionados establece; en ese sentido para el diseño de un control interno informático se debe preguntar ¿Cómo?, ¿Por qué?, y ¿de qué? Proteger la

información, para ello el profesional de contaduría pública debe estar actualizado con las diferentes normas técnicas referentes a dicha área.

Es por lo anterior que el presente propuesta de diseño de control interno informático orientará al profesional, no solo a nivel de normativa y aspectos legales para la generación de controles, sino también para la implementación de procedimientos y otros factores a considerar, además a que el profesional de contaduría pública establezca todos los requerimientos sobre el cumplimiento de la legalidad de la entidad, protección adecuada de los objetivos del negocio, procedimientos para las gestiones administrativas y una correcta planificación e implantación de controles para la seguridad de la información en cumplimiento principalmente de la normativa COBIT 5 y el estándar de la ISO 27002.

Diagnóstico para el área de las intermediarias de las distribuidoras de los servicios de telefonía en El Salvador

Una vez analizados los resultados de las encuestas se determinó que: Existe un alto porcentaje, puntualmente un 40% que implementa un modelo de control interno informático; de igual manera se cuenta con una unidad de auditoría interna siendo esta conjuntamente con la auditoría externa y las telefónicas mediante auditorías y supervisión quienes evalúan y ejecutan procedimientos respecto de la validez y efectividad de las políticas y procedimientos dentro del sistema de control interno informático, tal como se mencionó en la pregunta cuatro, en la mayoría de los casos viene siendo auditoría externa quien evalúa los procedimiento de control a pesar de ello el grado de alcance es distinto, dado que esta va enfocada hacia la razonabilidad de las cifras en los estados financieros.

No obstante que estas entidades cuenten con algunos controles y procedimientos estos son bastante deficientes en relación a la seguridad de la información tal como lo establecen las preguntas diez y once dado al desconocimiento de algunos riesgos a los cuales están expuestos y por ende conlleva a la debilidad de los controles que implementan.

Los pilares de la información se destacan en la confidencialidad, Integridad, y disponibilidad, bajo este enfoque es que el control interno informático se debe implementar. partiendo de de estas tres características, se analiza la confidencialidad para estas entidades, dado que la manera en como estas compañías protegen la información de accesos no autorizados generalmente lo hacen mediante la

autorizado del personal en la mayoría de los casos y listas de control de acceso en otros, siendo pocos los que implementan el cifrado, técnicas de firmas digitales que a su vez cuentan con técnicas de encriptación y redes perimetrales de seguridad, que son tan importantes como la ISO 27002 y COBIT5 lo establecen, es por ello que la confidencialidad ha sido vulnerada dado que ha existido robo de información producto de la extracción de datos no autorizados entre otros. Violaciones a tales controles dan como resultado un uso indebido de la información, venta de bases de datos (como en los casos de DICOM e INFORNET), hacking externo entre otros. Dado que la ISO 27002 a través de la aceptación del riesgo para identificar amenazas, además de conocer las vulnerabilidades y la probabilidad de que estos ocurran, establece cuatro posibles factores como lo es aceptar el riesgo, evitarlo, reducirlo o transferirlo a un tercero a través de la gestión del mismo, estableciendo controles, políticas y procedimientos en su guía de implantación.

Existen pocos controles que pueden ser eficaces en estas compañías, los resultados han determinado que existen fallas importantes respecto a la utilización de la información. A pesar que estas entidades manejan grandes volúmenes de bases de datos, entre los que destacan información relacionada como el nombre de la persona, número de DUI, dirección, e información importante, dado que los servicios de mayor demanda son los de telefonía prepago, pos-pago e internet, siendo estos los que principalmente deben cumplir con las características y derechos que establece la ISO 27002 y la Constitución de la República respectivamente, la primera respecto a las integridad, disponibilidad y confidencialidad de la información, y la segunda con referencia al Artículo 2 que establece la existencia de un derecho a la intimidad y protección de datos.

Considerando la recién aprobada ley de firmas electrónicas, estas compañías dentro de su diseño de control interno informático deberán tomar en cuenta conjuntamente con los aspectos regulatorios de la ISO 27002 y COBIT 5 lo cual se deberá llevar a cabo mediante la actualización.

De acuerdo a lo anterior el hecho que pocas entidades utilicen las técnicas de encriptación y firma digital, aumenta la posibilidad de fuga de información, esto es evidente a pesar que la participación dentro de la compañía en cuanto a los controles está formado por un equipo multidisciplinario como lo establece la pregunta tres, entre ellos ingenieros en sistema y los técnicos en redes, en relación a esto las entidades optan mayormente por contratar personal con experiencia en el área así como formar su capital humano mediante capacitaciones con el fin de brindar conocimiento a la vanguardia de las tecnologías., sin embargo más del 71 % de las entidades han tenido conocimiento de extracción o perdida de información,

que si existiera una política o un control de cifrado y protección de la misma disminuyese el riesgo que esa información se fugara, siendo este la mayor amenaza a la seguridad de la información que estas entidades han sufrido según los resultados obtenidos

En cuanto a la integridad de la información básicamente el control más implementado es la modificación a la base de datos solo al personal autorizado, así como también llevan una autorización de usuarios a nivel de transacciones que se guardan en registros, algunas de estas entidades siendo menos del 40 % utilizan seguridad a nivel de sistemas operativos, es decir existe un alto porcentaje que sus sistemas operativos no están protegidos, ya que se mantienen con las configuraciones de fabrica, aumentando el riesgo de vulnerabilidad y amenazas relacionadas a ellos, es evidente que la integridad de la información que se mantienen por estas entidades están expuestos dado que los controles como lo son la criptografía y seguridad lógica es implementada en un bajo porcentaje, siendo estos controles tan importante para la salvaguarda de tal característica.

Analizando la última característica que es la disponibilidad de la información el control más utilizado por estas entidades en la copias de respaldo de la información contenida en las bases de datos y la autenticación de usuarios; para el caso de backups existen ciertas vulnerabilidades como lo son copias de forma secreta, la custodia y para el caso del trasporte de datos cuando se realiza sin cifra;, es por ello que es necesario la combinación de controles para la protección de los datos; lo que respecta al control de prevención de ataques de denegación de servicios siendo este un control de los más importantes que estas entidades deben implementar, sin embargo solo lo hace menos del 30 % de ellas, siendo evidente que la disponibilidad de la información tiene un alto grado de riesgo.

Un sistema de control interno basado en riesgo de tecnología de información principalmente se basa en la evaluación de un contexto interno y externo de la entidad, definición de los posibles riesgos, evaluación e identificación de los riesgo, establecimiento de políticas, controles y monitoreo constante con el fin de comunicar a los niveles adecuados dentro de la organización los resultados de los sistemas de gestión de riesgos, es por ello que este diseño de control interno está orientado a aumentar el logro de los objetivos, el fomento de una gestión proactiva, a ser consistente en la necesidad de identificar y administrar los riesgos dentro de la entidad, al cumplimiento de los aspectos legales, normativos y reglamentarios mejorando la confianza de las partes interesadas, estableciendo una fuente confiable que garanticen la toma de decisiones y planificaciones a fin de determinar controles más efectivos, sin

embargo En todas las compañías evaluadas no fue posible garantizar que el control interno se base en lo anterior.

La ISO establece el primer paso para diseñar un sistema de gestión de riesgo el cual da a lugar a un sistema de control interno el cual es el compromiso con la gerencia, asimismo el diseño de políticas, la aprobación de ellas y otros encaminados al proceso de integridad, confidencialidad y disponibilidad de la información lo cual las compañías a la fecha no lo tienen, abonado a que estas empresa son consideradas pequeñas y que no poseen los recursos necesarios para poder implementarlos, por lo tanto estas entidades en un 60% están en la disponibilidad de aplicar un modelo como este; a pesar que el resto afirma no necesitarlo es tan evidente las deficiencias de control interno, por lo que también pueden ser de utilidad, sobre todo porque los controles internos van cambiando de acuerdo a la vanguardia de la tecnología

CAPÌTULO IIIDISEÑO DE CONTROL INTERNO BASADO EN RIESGOS DE TECNOLOGÍA DE INFORMACIÓN

3.1 Planteamiento del caso

3.1.1 Generalidades

Se presenta un modelo de control interno informático para una empresa que se dedique a la distribución de los servicios de telefonía bajo el enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la gestión de la información adoptando el modelo del proceso PDCA detallado a continuación:

- **Planear**
  Los aspectos de alta gestión dentro de este dominio van enfocados a las estrategias del negocio, el uso óptimo de los recursos, si la empresa atiende y cumple los objetivos y la gestión y respuesta a los riesgos de TI.
- **Hacer**
  En este dominio se enfoca en implementación de nuevos proyectos, si funcionaran de la manera correcta es decir la eficiencia y eficacia de los nuevos sistemas.
- **Chequear**
  Se enfoca en la optimización de costes, personal capacitado, los requerimientos y prioridades del negocio, además de la verificación de que los sistemas cumplen con las características de confidencialidad, integridad y disponibilidad.
- **Actuar**
  La medición de los desempeños y detección de problemas, la eficacia de los controles y el cumplimento de las disposiciones regulatorias.

Se plantea este modelo con el fin de cumplir con las características establecidas en la ISO 27002, las cuales son integridad, confidencialidad y disponibilidad de la información.

Este define una guía que podrá ser adaptado a los requerimientos específicos de cada entidad según su estructura, jerarquía y disposición, dado que los controles deben diseñarse a la medida de las necesidades de la entidad.

Además que este servirá de modelo para otras entidades que deseen implementarlo, partiendo de los riesgos de tecnología existentes en cada entidad en particular, tomando de referencia el marco integrado de COBIT 5 que reúne los estándares de la ISO en particular la ISO 27002, así como la referencia que establece ITIL.

3.2 Explicaciones generales, estructura y forma del diseño de control interno informático.

La empresa distribuidora 4G, S.A DE C.V fue constituida el 28 de noviembre de 2011 necesita se le diseñe un modelo de control interno basado en riesgos de tecnología; para lo cual proporciona los siguientes elementos:

- tipos de activos
- aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos
- información, datos y servicios
- dimensiones de valoración de los activos
- criterios de valoración de los activos
- amenazas más comunes sobre los sistemas de información
- Contexto externo e interno de la entidad
- Regulaciones legales

Para el diseño del caso práctico en la tabla Nº 7 Diseño de control interno informático, se detallan los pasos a seguir una vez realizado el conocimiento previo de la entidad, la comprensión de sus procesos y el análisis del entorno.

Como siguiente paso el estándar ISO 27002 establece los criterios o requerimientos generales los cuales las entidades deben cumplir ya sea mediante registros, procedimientos, y controles todos los anteriores documentados como se establece en los apartados comprendidos del 4 al 8, detallados a continuación.

Requisitos de la Norma	1 Procedimiento / procedimiento documentado	2 Definir /Documentar / acción /	3 Medición / medible / Revisar	4 Método o metodología	5 Registro	6 Controles para: / Controlar	7 Planificar / planificación	Comentarios Generales
4.1 Requerimientos Generales	Establecer, implementar, operar, monitorear, mantener y mejorar	Actividades comerciales generales		PDCA				
4.2 Establecer y manejar el SGSI								

Requisitos de la Norma	1 Procedimiento / procedimiento documentado	2 Definir /Documentar / acción /	3 Medición / medible / Revisar	4 Método o metodología	5 Registro	6 Controles para: / Controlar	7 Planificar / planificación	Comentarios Generales
4.2.1 Establecer el control interno		Alcance y límites del SGSI Política del SGSI Enunciado de aplicabilidad	Enfoque de la evaluación del riesgo Impacto comercial de por una falla. La probabilidad realista de suceder una falla	Como evaluar el riesgo		Vulnerabilidades y amenazas		
4.2.2 Implementar y operar		Tratamiento de riesgos Sistema de métricas	Efectividad de los controles			Detección y respuesta a los incidentes de seguridad		

Requisitos de la Norma	1 Procedimiento / procedimiento documentado	2 Definir /Documentar / acción /	3 Medición / medible / Revisar	4 Método o metodología	5 Registro	6 Controles para: / Controlar	7 Planificar / planificación	Comentarios Generales
4.2.3 Monitorear y revisar	Monitorización y revisión		Efectividad de los controles		Las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del control interno			
4.2.4 Mantener y mejorar	Acciones preventivas y correctivas	Resultado de las acciones a las partes interesadas			Acciones y eventos a las partes interesadas			
4.3 Requerimientos de documentación								

Requisitos de la Norma	1 Procedimiento / procedimiento documentado	2 Definir /Documentar / acción /	3 Medición / medible / Revisar	4 Método o metodología	5 Registro	6 Controles para: / Controlar	7 Planificar / planificación	Comentarios Generales
4.3.1 General		Enunciados de las políticas. Alcance Procedimientos y controles Enunciado de aplicabilidad			Decisiones gerenciales, Evaluación de riesgo	Planeación, operación, y procesos de seguridad de la información		
4.3.2 Control de documentos					Reprobación de la documentación		Protección y control los procedimientos documentados	

Requisitos de la Norma	1 Procedimiento / procedimiento documentado	2 Definir /Documentar / acción /	3 Medición / medible / Revisar	4 Método o metodología	5 Registro	6 Controles para: / Controlar	7 Planificar / planificación	Comentarios Generales
4.3.3 Control de registros	Establecer y mantener registros de las evidencias	Implementación de los controles.			Registro de evidencias Desempeño del proceso de control interno y de la ocurrencias de los incidentes de seguridad de la información	Legibles, identificables y recuperables		

Respecto del cumplimiento del estándar de la ISO 27001 se establecen las declaratorias del debe orientado a cumplir los lineamientos para el aseguramiento de los sistemas de información. Es decir el diseño de un control interno conlleva al cumplimiento de importantes aspectos para la eficacia de las operaciones de la organización, diseñando controles para el aseguramiento de los activos de información y de las partes interesadas, es por ello que se detalla los siguientes apartados que dentro de la organización y sus áreas deben establecerse.

Apartado	Declarativa(s) del debe.
5. RESPONSABILIDAD DE LA DIRECCION.	
5.1 Compromiso de la dirección	PROPORCIONAR EVIDENCIA DEL COMPROMISO a) Establecer política de control interno b) Establecer objetivos c) Establecer roles y responsabilidades para control interno d) Comunicar importancia del objetivo de seguridad y cumplir la política e) Proporcionar recursos para desarrollar, implementar, monitorear, revisar, mantener y mejorar el sistema f) Decidir el criterio para la aceptación del riesgo y niveles de riesgo aceptado g) Asegurar que se realicen las auditorías internas de interno h) Realizar revisiones generales del control interno
5.2 Gestión de recursos	Determinar y proporcionar los recursos necesarios a) Establecer, implementar, operar, monitorear, revisar, mantener y mejorar un control interno b) Asegurar que los procedimientos de seguridad de la información respalden los procedimientos comerciales

	c) Identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales d) Mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados e) Llevar a cabo revisiones cuando sea necesario y reaccionar apropiadamente ante los resultados de estas revisiones f) Donde se quiera mejorar la seguridad de control interno Asegurar que todo el personal a quien asignó responsabilidades definidas en control interno sea competente para realizar las tareas requeridas para: a) Determinar capacidades necesarias para el personal que realice el trabajo que afecta el control interno b) Proporcionar capacitación o realizar otras acciones (emplear personal competente) para satisfacer estas necesidades c) Evaluar actividades de las acciones tomadas d) Mantener registros de educación, capacitación, capacidades, experiencia y calificaciones Asegurar que todo el personal relevante esté consciente de la relevancia e importancia de sus actividades de seguridad de información y como debe contribuir al logro de los objetivos del control interno
6. AUDITORÍAS INTERNAS AL CONTROL INTERNO	Realizar auditorías internas del control interno a intervalos planeados a) Cumplir con requerimientos de la ISO 27000 b) Cumplir con requerimiento de seguridad de SI identificados c) Implementar y mantener de manera efectiva y conforme Planear un programa de auditoría Definir claramente el criterio, alcance, frecuencia y métodos de auditorías

	Asegurar la objetividad e imparcialidad en el proceso de auditoría Asegurar que se den sin demoras las acciones para eliminar las no conformidades detectadas y sus causas. Definir un procedimiento documentado para establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y operación efectiva de un control interno
7. REVISIÒN DEL CONTROL INTERNO POR LA DIRECCIÓN	
7.1 General	Revisar el control interno en la organización a intervalos planeados Incluir oportunidades de evaluación para la mejora y necesidad de cambios en el control interno Documentar claramente los resultados de las revisiones y mantener registros
7.2 Insumo de la revisión	En insumos de revisión incluir: • Resultados de auditorías • Retroalimentación de las partes interesadas • Técnicas, productos o procedimientos a usar • Estatus de acciones preventivas y correctivas • Vulnerabilidades o amenazas no tratadas • Resultados de mediciones de efectividad • Acciones de seguimiento • Cualquier cambio que afecta el control interno • Recomendaciones para mejoramiento
7.3 Resultado de la revisión	RESULTADOS DE REVISIÓN • Incluir mejoramiento de actividad de control interno • actualización de la evaluación del riesgo • modificación de procedimientos y controles que afectan la seguridad de información

	• necesidades de recursos • mejoramiento de cómo se mide la efectividad de los controles
8 MEJORAMIENTO DEL CONTROL INTERNO	
8.1 Mejoramiento continuo	Mejorar continuamente la efectividad del control interno por políticas de seguridad de información
8.2 Acción correctiva	Realizar acciones para eliminar causas de no conformidades a) identificar no conformidades b) determinar las causas de no conformidades c) evaluar la necesidad de acciones para no repetirlas d) determinar e implementar la acción correctiva e) registrar los resultados de la acción tomada f) revisar la acción correctiva
8.3 Acción preventiva	Determinar la acción para eliminar la causa de la no conformidad potencial a) identificar las no conformidades potenciales b) evaluar la necesidad para acción para evitar ocurrencia c) determinar e implementar la acción preventiva d) registrar los resultados de acción tomada e) revisar la acción preventiva tomada Identificar riesgos cambiados en gestión y requerimientos de acción preventiva Determinar con base a resultados de la evaluación del riesgo, las acciones preventivas

Relacionado al conocimiento de conformidad de los dominios de control por parte de la entidad y el conocimiento previo de la entidad se establecen de acuerdo a los lineamientos del estándar ISO 27001 un listado de preguntas que las organizaciones deben de responder para determinar el riesgo asociado a los que están expuestos, es por ello que se establece a continuación el siguiente cuestionario para determinar los niveles de conformidad dentro de la entidad.

N°	Pregunta	Escala de Likert				
		1	2	3	4	5
	RESPONSABILIDAD DE LA DIRECCION.	Muy en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Muy de acuerdo
1	¿La entidad ha establecido adecuadamente las políticas para el control interno?				x	
2	¿Se ha verificado que los objetivos para el control interno están alineados con el área de tecnología de información?			X		
3	¿Se delegaron roles y responsabilidades adecuadamente para el control interno?			X		
4	¿Se verificó el cumplimiento de las políticas y la importancia de comunicación con respecto a la seguridad en el control interno?			X		
5	¿Se proporcionó los recursos necesarios para el desarrollo, implementación, monitoreo, y mantenimiento del control interno?			X		
6	¿Se definieron los criterios del riesgo y los niveles de riesgo		X			

	aceptado?					
7	¿Se han realizado auditorías internas sobre control interno?				x	
8	¿Se han realizado revisiones generales de control interno?				x	
9	¿Se verificó que los procedimientos de seguridad de la información se respaldan en base a procedimientos comerciales?				x	
10	¿Se proporcionaron los recursos necesarios para mantener una seguridad apropiada en la aplicación de controles?			X		
11	¿Se han efectuado revisiones cuando es necesario y si responden de manera adecuada antes los resultados?			X		
12	¿Se ha dado cumplimiento de acuerdo a los requerimientos necesarios en cuanto a las capacidades del personal que realiza trabajo de control interno?			X		
13	¿Se han brindado capacitaciones de acuerdo a los servicios de la entidad y otras acciones toman en cuanto a la formación del personal?				x	
14	¿Se ha recopilado información en cuanto a la educación, capacitación, experiencia y capacidades del personal en el			X		

	área de control interno?					
	AUDITORÍAS INTERNAS					
15	¿La entidad ha cumplido con los requerimientos establecidos en el marco técnico y legal?			X		
16	¿La entidad ha cumplido con los requerimientos de seguridad de SI identificados?			X		
17	La entidad ha implementado y ha realizado de manera efectiva lo siguiente: • un programa de auditoría • Definir claramente el criterio, alcance, frecuencia y métodos de auditorías. • Asegurar la objetividad e imparcialidad en el proceso de auditoría • Asegurar que se den sin demoras las acciones para eliminar las no conformidades detectadas y sus causas. • Define un procedimiento documentado para establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y operación efectiva				x	
	REVISIÒN DEL CONTROL INTERNO POR LA DIRECCIÒN					
18	¿Se ha revisado el control				x	

	interno en la organización a intervalos planeados?					
19	¿Se ha incluido oportunidades de evaluación para la mejora y necesidad de cambios en el control interno informático?			X		
20	¿Se ha documentado claramente los resultados de las revisiones y se mantiene los registros adecuadamente?				x	
21	¿ Se ha incluido en el insumos de revisión gerencial lo siguiente: • Resultados de auditorías • Retroalimentación de las partes interesadas • Técnicas, productos o procedimientos a usar • Estatus de acciones preventivas y correctivas • Vulnerabilidades o amenazas no tratadas • Resultados de mediciones de efectividad • Acciones de seguimiento • Cualquier cambio que afecta al control interno • Recomendaciones para mejoramiento			X		
22	Se ha incluido en el resultados de la revisión los siguiente aspectos: • Incluir mejoramiento de actividad del control interno			X		

	• actualización de la evaluación del riesgo • modificación de procedimientos y controles que afectan la seguridad de información • necesidades de recursos • mejoramiento de cómo se mide la efectividad de los controles					
	MEJORAMIENTO DEL CONTROL INTERNO INFORMÁTICO					
23	En el mejoramiento continuo: ¿La entidad ha mejorado consecutivamente la efectividad del control interno informático por políticas de seguridad de información?			X		
24	Para las acciones correctivas: Se han realizado acciones para eliminar causas de no conformidades sobre: g) identificación de no conformidades h) determinar las causas de no conformidades i) evaluar la necesidad de acciones para no repetirlas j) determinar e implementar la acción correctiva k) registrar los resultados de la acción tomada l) revisar la acción correctiva			x		
25	Para la acción preventiva Se han realizado acciones para			X		

	eliminar causas de no conformidades potenciales sobre: • identificación de las no conformidades potenciales • evaluación de la necesidad para acción para evitar ocurrencia • determinación e implementación de la acción preventiva • registro de los resultados de acciones tomada • revisar la acción preventiva tomada					
26	¿Se han identificado los riesgos cambiados en gestión y requerimientos de acción preventiva			XX	X	
27	¿Se ha determinado con base a resultados de la evaluación del riesgo, las acciones preventivas?			X		
			2	54	32	

De acuerdo a los niveles de conformidad de la aceptación del riesgo por parte de la entidad, se determina que esta poseen en relación a las interrogantes realizadas respecto a los dominios de control y el conocimiento que se tiene de estos, que un alto porcentaje de la entidad, se encuentra en nivel indeciso, en particular en los controles de segregación de funciones, cumplimientos de políticas, niveles de comunicación, con los recursos necesarios para las fases de control interno, para garantizar la seguridad en la aplicación de controles, los niveles de formación en el capital humano entre otros.

Con lo anterior se determina las áreas más expuestas determinando así la orientación que deberá desarrollarse en el control interno informático.

Como siguiente punto se establece el listado de los objetivos de control y las actividades a desarrollar en cada uno de los controles ya sea una asignación o documento que se debe implementar dentro de un plan de tratamiento de riesgos que identifique los recursos, las responsabilidades y prioridades en los sistemas de información, dando como resultados la implementación de controles como lo establece el apartado 4.2.1 de la ISO 27001, la cual determina como establecer tales controles, es por ello que a continuación se presentan los objetivos de control adaptado a las necesidades de las organizaciones.

Control	Control	Actividades para desarrollar
A.5.1.1	La Dirección debe aprobar un documento de política de seguridad de la información, publicarlo y comunicarlo a todos los empleados y entidades externas afectadas.	• Elaborar una política. • Realizar un documento. • Desarrollar un plan de capacitación.
A.5.1.2	Revisión de la política de seguridad de la información	• Analizar el entorno de forma periódica para determinar si existen cambios. • Realizar un acta de revisión para aprobación de cambios • Documentar el registro de versiones • Actualizar los apartados de las políticas que han sufrido cambios • Comunicar a las partes interesadas
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	• Asistir a reuniones con las partes interesadas • Elaborar de actas de reuniones
A.6.1.2	Coordinación de la seguridad de la información	• Establecer roles y responsabilidades relacionados a la seguridad de información • Comunicar al personal las responsabilidades
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	• Actualizar/ el perfil del descriptor de puestos para personal de seguridad de información • Capacitar y evaluar al personal dedicado a seguridad de información
A.6.1.4	Proceso de autorización para los medios de procesamiento de información	• Documentar procedimiento de autorización

A.6.1.5	Acuerdos de confidencialidad	• Identificar y revisar requerimientos de confidencialidad
A.6.1.7	Contactos con grupos de interés especial	Mantener contacto con los grupos de interés
A.6.1.8	Revisión independiente de la seguridad de la información	• Revisar a intervalos planeados o cuando ocurran cambios significativos el enfoque de la organización para el manejo del control interno informático y su implementación.
A.6.2.1	Identificación de riesgos relacionados con entidades externas	• Identificar riesgos de la información y los medios de procesamiento • Implementar controles antes de otorgar accesos
A.6.2.2	Tratamiento de la seguridad cuando trabaja con clientes	• Gestionar los requerimientos de seguridad antes de otorgar accesos a la información
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	• Documentar los acuerdos de acceso, procesamiento, comunicación o manejo por parte de terceros • Determinar los requerimientos de seguridad para agregar nuevos productos o servicios
A.7.1.1	Inventarios de activos	• Elaborar y mantener un inventario de los activos
A.7.1.2	Propiedad u uso de los activos	• Determinar la parte de la entidad a que pertenecen los activos • Documentar las políticas de uso para el procesamiento de la información y los activos asociados para este fin
A.7.1.3	Lineamientos de clasificación, etiquetado y manejo de la información	• Clasificar la información de acuerdo al valor, requerimientos legales y confidencialidad • Implementar procedimientos para el etiquetado y manejo de la información
A.8.1.1	Antes del empleo	• Definir y documentar roles y responsabilidades del personal

	Roles y responsabilidades Selección Término y condiciones de empleo	• Realizar chequeos de verificación de antecedentes de los empleados de acuerdo a leyes, regulaciones y etiquetas relevantes • Definir documento que establezca compromisos términos y condiciones de las responsabilidades de los empleados que deberán firmar y aceptar
A.8.1.2	Durante el empleo Gestión de responsabilidades Capacitación y educación en seguridad de la información Proceso disciplinario	• Establecer un requerimiento que los empleados cumplen con los procedimientos y políticas de la entidad. • Establecer capacitaciones, actualizaciones de políticas, procedimientos relevantes para las funciones laborales. • Implementar un proceso disciplinario.
A.8.1.3	Responsabilidades de terminación Devolución de activos Eliminación de derechos de accesos	• Definir responsabilidades respecto a la terminación o cambio de empleo. • Documentar la devolución de activos en la terminación del empleo. • Eliminar los derechos de acceso a la información
A.9.1.1	Medidas de seguridad física y acceso físico	• Implementar controles de seguridad para el acceso del personal autorizado. • Diseñar y aplicar la protección física ante un fenómeno natural o provocado.
A.9.2.1	Ubicación y protección del equipo	• Proteger los equipos contra riesgos, amenazas y peligros ambientales. • Implementar un sistema de mantenimiento para los equipos. • Implementar un sistema de protección.
A.9.2.2	Políticas y procedimientos para personal contratado y mantenimiento de la infraestructura	• Definir los procesos, organizaciones y relaciones de TI. • Gestionar el ambiento físico
A.9.2.3	Protección de la tecnología de	• Garantizar la seguridad de los

	información	sistemas
A.9.2.4	Gestión de instalaciones físicas	● Gestionar el ambiente físico
A.10.1.1	Procedimientos de operaciones documentados	● Documentar los procedimientos de operación y estar a disposición del usuario.
A.10.1.2	Gestión de cambio	● Proteger y controlar los cambios en los medios y sistemas de procesamiento
A.10.1.3	Segregación de deberes	● Documentar las segregaciones, así como los deberes, y niveles de responsabilidad.
A.10.2.1	Entrega del servicio	● Implementar controles para determinar que terceros cumplan lo incluido en el contrato.
A.10.2.2	Monitoreo y revisión de los servicios de terceros	● Diseñar controles para el monitoreo y revisión de los servicios, reportes y registros.
A.10.3.1	Gestión de capacidad	● Gestionar controles para monitorear los recursos del sistema y su desempeño
A.10.3.2	Aceptación de sistemas	● Establecer criterios para la aceptación de un nuevo sistema, actualizaciones o versiones nuevas.
A.10.4.1	Controles sobre software maliciosos	● Implementar controles para la detección, prevención y recuperación para protegerse de códigos maliciosos.
A.10.4.2	Controles contra códigos móviles	● Definir políticas de seguridad para evitar que códigos móviles se ejecuten.
A.10.5.1	Back-up o respaldo de la información	● Realizar copias de respaldo de la información comercial y software.
A.10.6.1	Controles de red	● Implementar controles para el adecuado manejo de las redes y evitar amenazas y mantener la seguridad de los sistemas
A.10.7.1	Gestión de los medio removibles	● Realizar procedimientos para la gestión de medios removibles. ● Establecer controles para el manejo y almacenaje de la información
A.10.7.2	Seguridad de la documentación del	● Proteger la documentación del

	sistema.	acceso autorizado.
A.10.8.1	Procedimientos y políticas de información y software	• Establecer políticas, procedimiento y controles para proteger el intercambio de información.
A.10.8.2	Acuerdos de intercambio	• Establecer acuerdos para: • El intercambio de información dentro de la entidad. • Acceso no autorizado para los medios que contiene la información • Mensajes electrónicos.
A.10.9.1	Comercio electrónico	• Identificar los riesgos a fin de proteger la información que se trasmite a través de redes públicas.
A.10.9.2	Información disponible públicamente	• Implementar controles para mantener la integridad de la información.
A.10.10.1	Registro de auditoria	• Documentar los registros de las auditoria realizadas
A.10.10.2	Uso del sistema de monitoreo	• Establecer procedimientos para el monitoreo del uso de medios de procesamiento
A.10.10.3	Protección del administrador y operador	• Documentar los registro y actividades del administrador y operador del sistema • Documentar los registros de fallas • Implementar controles de sincronización con una fuente de tiempo
A.11.1.1	Políticas de control de acceso	• Documentar las políticas de control de acceso en base a los requerimientos de seguridad.
A.11.2.1	Gestión de privilegios	• Implementar restricciones en el uso de los privilegios.
A.11.2.2	Gestión de claves de usuario	• Establecer la asignación de claves a través de un proceso de gestión formal.
A.11.3.1	Uso de claves	• Diseñar buenas prácticas de seguridad en el uso de claves
A.11.3.2	Políticas de pantalla y escritorio limpio	• Establecer política de escritorio limpio para los documentos y medios de almacenaje.
A.11.4.1	Política sobre los servicios de uso de	• Diseñar políticas sobre accesos solo

	red	personal autorizado
A.11.4.2	Autenticación de usuario para conexiones externas	• Implementar métodos de autenticación para el control de acceso.
A.11.4.3	Protección del puerto de diagnóstico remoto	• Establecer controles para el acceso físico y lógico
A.11.4.4	Control de conexiones de red	• Restringir la capacidad de conexión de los usuarios de redes compartidas.
A.11.5.1	Procedimiento en la terminal	• Documentar los registros sobre el acceso a los servicios operativos
A.11.5.2	Identificación y autenticación del usuario	• Establecer controles para la identificación para su uso personal y exclusivo.
A.11.5.3	Sistema de gestión de claves	• Diseñar claves que deben ser interactivas y seguras.
A.11.5.4	Limitación de tiempo de conexión	• Establecer restricciones sobre los tiempos de conexión para seguridad de las aplicaciones
A.11.6.1	Restricción al acceso a la información	• Diseñar restricciones al acceso de los usuarios y personal de soporte al sistema de información
A.11.7.1	Computación móvil y comunicaciones	
A.12.1.1	Análisis y especificaciones de los requerimientos de seguridad	• Documentar los requerimientos de los sistemas nuevos o las mejoras de los ya existentes
A.12.2.1	Procesamiento correcto de las aplicaciones	• Realizar chequeos de verificación de las aplicaciones y que la información esté libre de errores de procesamiento o actos deliberados
A.12.3.1	Controles criptográficos	• Diseñar y establecer políticas sobre el uso de controles criptográficos • Establecer controles de gestión de claves para dar soporte a las técnicas criptográficas
A.12.4.1	Control de software operacional	• Implementar controles para: • Instalación de software de sistema. • Selección y protección sobre la data de prueba • Restricción al acceso al código fuente
A.12.5.1	Procedimientos del control de cambio	• Diseñar controles para la

		implementación de cambios del sistema
A.12.5.2	Filtración de información	● Elaborar controles para evitar filtraciones de la información
A.12.6.1	Control de vulnerabilidades técnicas	● Gestionar la protección de las vulnerabilidades técnicas para reducir riesgos en los sistemas de información
A.13.1.1	Reporte de eventos en la seguridad de la información	● Implementar un reporte de eventos de seguridad de la información
A13.1.2	Reporte de debilidades en la seguridad	● Implementar para que los empleados, y otros afines a la entidad reporten debilidades o sospechas de incidentes de seguridad
A.13.2.1	Responsabilidades y procedimientos	● Establecer las responsabilidades y procedimientos gerenciales ante incidentes de seguridad
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	● Determinar mecanismos que permitan cuantifiquen y monitoreen los incidentes en la seguridad de la información
A.14.1.1	Seguridad de la información en el proceso de gestión de continuidad comercial	● Desarrollar un proceso gerencial para la continuidad del negocio
A.14.1.2	Implementar planes de continuidad	● Implementar planes para mantener o restaurar las operaciones ante interrupciones o fallas en los procesos críticos
A.14.1.3	Prueba, mantenimiento y re-evaluación de planes de continuidad	● Desarrollar planes de continuidad regularmente
A.15.1.1	Identificación de legislación aplicable	● Definir y documentar los requerimientos estatutarios, reguladores y contractuales
A.15.1.2	Derecho de protección intelectual	● Implementar procedimientos para el cumplimiento sobre el uso del material de software patentado
A.15.1.3	Protección de los registros organizacionales	● Establecer una protección de los registros de incidentes
A.15.1.4	Protección de data y privacidad de la información personal	● Asegurar la protección y privacidad de la información
A.15.1.5	Regulación de controles criptográficos	● Implementar el uso de controles

A.15.1.6	Cumplimientos con las políticas y estándares de seguridad	● Establecer por parte de la gerencia el cumplimiento de los estándares de seguridad ● Revisar periódicamente el cumplimiento de dichos estándares
A.15.1.7	Controles de auditoría de sistemas de información	● Planear requerimientos y actividades de auditoría relevantes a la información
A.15.1.8	Protección de las herramientas de auditoría	● Establecer un mecanismo de protección del acceso a las herramientas de auditoría

DISEÑO DE CONTROL INTERNO BASADO EN RIESGOS DE TECNOLOGÌA DE INFORMACIÒN

3.3 Diseño de control interno basado en riesgo de tecnología de la información.

3.3.1 Desarrollo del caso

ÍNDICE

Paso A76
Establecimiento de requerimientos generales 76
A.1.Conocimiento de la entidad. 76
A.2Breve reseña histórica y resumen de sus actividades. 76
A.3Mercado y Competencia 77
A.4Cuadro resumen de la información de la entidad.77
A.5 Misión y visión de la entidad 78
A.6 Organigrama 78
A.7 Determinación de los activos. 79
Paso B Establecer y manejar el control interno 80
B.1Política en términos de la características del negocio, activos y otro factores a considerar 80
B.2Criterios de medición de riegos 80
B.3Identificar los riesgos 81
B.4Analizar y evaluar el riesgo 83
B.5Opciones de tratamiento del riesgo 88
B.6Objetivos de control y controles para el tratamiento del riesgo 91
B.7 Documentación 104
B.8 Autorizacion de la gerencia para implementar y operar el control interno informatico 106
B.9 Enunciado de aplicabilidad 107
Paso C Implementar y operar 107

C.1 Plan de Tratamiento del riesgo 107
C.2 Implementación del plan de tratamiento del riesgo 107
C.3 Implementación de controles seleccionados 107
C.4 Programas de capacitación y conocimiento 107
C.5 Manejar las operaciones de control interno informático 107
C.6 Manejar los recursos del control interno informático 107
Paso D Monitorear y revisar 108

Paso A

Establecimiento de requerimientos generales

Para sustentar el paso Aen el procedimiento de establecer los requerimientos; se establecen en el Anexo Nº 4 las actas de Junta Directiva referente a:

- Responsabilidad de la gerencia
- Compromiso de la gerencia
- Conocer el contexto empresarial tanto interno como externo de la entidad
- Establecer política de control interno informático
- Establecer objetivos
- Establecer roles y responsabilidades para control interno informático
- Comunicar importancia del objetivo de seguridad y cumplir la política
- Proporcionar recursos para desarrollar, implementar, monitorear, revisar, mantener y mejorar el control interno informático
- Decidir el criterio para la aceptación del riesgo y niveles de riesgo aceptado
- Asegurar que se realicen las auditorías internas de control interno informático

A.1 Conocimiento de la entidad.

A.1.1 Breve reseña histórica y resumen de sus actividades.

4G, S.A DE C.V abrió sus puertas en San Salvador a finales de noviembre de 2011 cuenta con 25 empleados, y entre los servicios que prestan están la distribución de servicios de telefonía de tipo prepago, pos pago, e internet.

Su misión es proveer a los clientes los servicios de calidad asegurando la confianza, eficiencia y ética. Orientada a la satisfacción de las necesidades logrando un compromiso constante hacia la innovación transparencia y el deseo de constante de mejorar mediante el servicio de calidad.

Se determina la comprensión clara de los aspectos fundamentales de la información que maneja la entidad y los servicios que presta a fin de tener un conocimiento del contexto interno y externo de la empresa.

A.1.2 Mercado y Competencia

El enfoque actual de 4G, S.A de C.V se encuentra en los sectores de telecomunicaciones.

Los principales distribuidores de 4G, S.A de C.V son los siguientes:

- CTE Telecom Personal S.A de C.V
- Telemòvil S.A de C.V
- Digicel S.A de C.V
- Telefónicas Móviles de El Salvador S.A de C.V.

A.1.3 Cuadro resumen de la información de la entidad.

Nombre de la entidad	4G, S.A DE C.V
Naturaleza	Anónima de Capital Variable
Nacionalidad	Salvadoreña
NIT	0604-281111-104-3
NRC	153006-4
Fecha de inicio de operaciones	Noviembre, 2011
Dirección	73 Av. norte entre Avenida Olímpica pasaje Carbonell
Teléfono	2243-1694
Giro de la entidad	Distribución de servicios de telefonía
Plazo	Indefinido

A.1.4 Misión y visión de la entidad

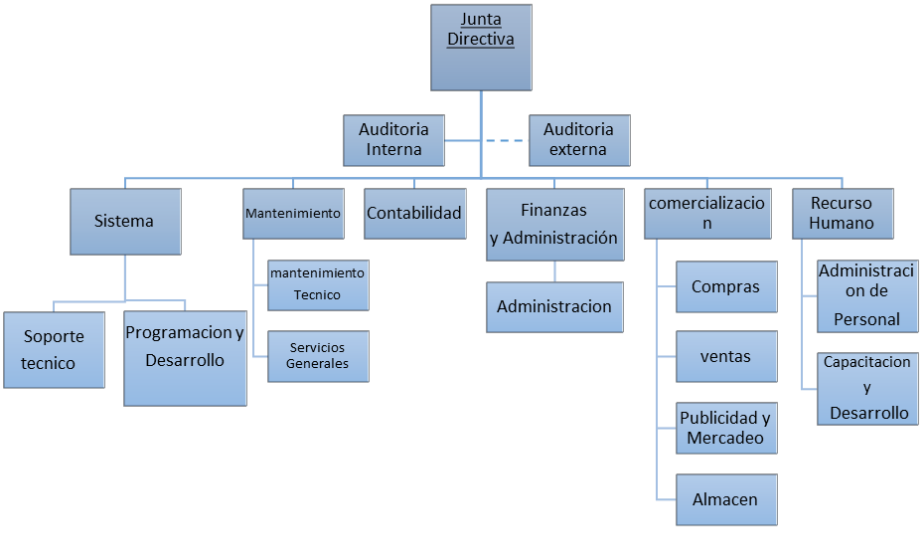
MISIÒN:

Somos una empresa dedicada a proporcionar los más alto niveles de calidad y constante innovación a la necesidad de telecomunicaciones con el fin de lograr satisfacción total de los clientes generando el mayor bienestar, desarrollo personal y profesional de nuestros trabajadores.

VISIÒN:

Situarnos como altos líderes en el mercado de telecomunicaciones a través de nuestros productos, servicios, calidad e innovación. Destacándose por la eficiencia, eficacia, dinamismo, rentabilidad, calidad competencia de talento humano garantizando la satisfacción de sus clientes.

A.1.5 Organigrama



A.1.6 Determinación de los activos.

Los activos esenciales rigen los requisitos de seguridad para todos los componentes del sistema; dependiendo de la clasificación del activo, las amenazas y las salvaguardas son diferentes. La valoración de los activos se puede determinar desde la perspectiva de proteger, pues es decir entre más valioso es un activo mayor nivel de protección requiere. Además de considerar que según la ISO 27001 establece que activo es cualquier cosa que tenga valor para la entidad.

La compañía 4G proporciona la lista de activos esenciales

Criterio de valoración del riesgo: Disponibilidad

Activo	Evaluación del riego		
	Bajo	Medio	Alto
Router			X
Switch			X
Redes			X
Periféricos		X	
Instalaciones		X	
Cableado		X	
Conectores	X		
Kit de herramientas	X		
Terminales			X
Software			X
Sistema operativo			X
Base de datos			X
Mobiliario	X		
Instalaciones técnicas	X		
Patch panel		X	
Rack		X	
Antenas		X	
Tester			
Caja decodificadora	X		
Servidores	X		

Paso B Establecer y manejar el control interno informático

B.1 Política en términos de las características del negocio, activos y otros factores a considerar

Para desarrollar el paso B: Establecer y manejar el control interno informático se establece el documento de la política de la seguridad de la información que se muestra en el Anexo Nº 5

B.2 Criterios de medición de riegos

La magnitud de riesgo se determina de acuerdo a la siguiente fórmula:

Magnitud= probabilidad x impacto

Mapa de calor

En este se establece la medición del riesgo de acuerdo a su probabilidad e impacto lo cual se detalla a continuación:

Probabilidad: La frecuencia que puede presentar el riesgo

Alta: Es muy factible que se presente el riesgo
Medio: Es factible que se presente el riesgo
Baja: Es poco factible que se presente el riesgo

Impacto: Forma en que el riesgo podría afectar los resultados del proceso

Alta: Afecta en alto porcentaje la disponibilidad del servicio
Media: Afecta en un porcentaje medio la disponibilidad del servicio
Baja: Afecta en un porcentaje bajo la disponibilidad del servicio

Probabilidad	Alta	B	A	A
	Media	B	B	A
	Baja	C	B	B
		Bajo	Medio	Alto
		Impacto		

Figura 4: Matriz de priorización

B.3 Identificar los riesgos

Se definen los potenciales riesgos a los cuales se podría ver afectado el servicio de Red, bases de datos, software, y sistemas operativos de la entidad 4G.

RED		
Tipo de riesgo	**Riesgo**	**Descripción**
Interno	• Falla en el UPS	Falla en el equipo electrónico que se mantiene de respaldo
	• Falla en equipos de ventilación	Propicia una temperatura no adecuada para los equipos
	• Desconexión física	Producida por un cable mal conectado, en mal estado o un corte intencionado o no del cable
	• Corte de servicio en servidores externos e internos	Ocasiona que el servicio no esté disponible, así como el servicio web y DNS
	• Falla sobre núcleos de comunicaciones	Desperfecto eléctrico o un problema en el núcleo de comunicaciones
	• Saturación en el núcleo de comunicaciones	Problemas en el procesamiento de la información y en la memoria.
	• Saturación de carga en el enlace	El servicio tiende a colapsar producto de una sobre carga
Externo	• Corte de energía	Falla en el sistema eléctrico y por ende falla en el funcionamiento del equipo
	• Inundaciones, terremotos , Incendios, interrupción del servicio de internet, entre otros	Daños al equipo y desconexión de la Red
Bases de datos		
Tipo de riesgo	**Riesgo**	**Descripción**
Interno	• Back ups desactualizados	Problemas respecto a la disponibilidad de la información
	• Accesos no restringidos	Pueden llevar a un uso indebido de la información
	• Sin medidas de seguridad	Generación de vulnerabilidad de los datos conservados en la entidad
	• Procesamiento incorrecto de datos	Propicia una alteración respecto a la integridad del procesamiento

		de los datos
	• Infecciones con virus, troyanos u otro malware	Fallas en el uso de la base de datos, robos o ralentización de la información
	• Procedimientos para el tratamiento de la información no valida	La información está ejecutándose con procedimientos no estipulados por la entidad
Externo	• Ataques externos	Ataques dirigidos al robo de la información contenida en las bases de datos
	• Personal insatisfecho	Personal inconforme con las medidas de suspensión de labores en la entidad
Software y sistemas operativos		
Tipo de riesgo	**Riesgo**	**Descripción**
Interno	• Falla en el control de las licencias	La entidad tiende a no controlar el uso de licencias
	• Caídas y cuelgues del sistema	Tiende a colapsar el sistema operativo producto de una saturación y ausencia de mantenimiento hacia el equipo, en ocasiones por pruebas realizadas a los sistemas
Externo	• Ataques externos	Ataques dirigidos al sistema operativo, infecciones de malware, virus y otros
Terminales		
Tipo de riesgo	**Riesgo**	**Descripción**
Interno	• Ataques internos	Fallas en el procesamiento de datos por falta de capacitaciones o conocimientos de los procedimientos del resguardo de la información
	• Infecciones de virus, troyanos, gusanos u otro tipo de malware	Altera el funcionamiento normal de una computadora sin el permiso o consentimiento del usuario, pueden ocasionar robos de información
	• Fallas en los conectores eléctricos	Daños a los equipos
	• Medios extraíbles	Fallas en el control de conexión de medios extraíbles
	• Mantenimiento	Desperfectos en el hardware, y ralentización en el sistema de las maquinas

Externo	• Hacker, Cracker	Riesgo externo al que todas las entidades están expuestas

B.4 Analizar y evaluar el riesgo

Análisis del riesgo

Una vez identificado los riesgos potenciales o a los que la entidad está expuesta se determina la probabilidad, impacto y magnitud tal como se establece a continuación:

Riesgo	Control existente	Probabilidad	Impacto	Magnitud
Falla en el UPS	-	Bajo	Medio	B
Falla en equipos de ventilación	Mantenimiento periódico	Baja	Bajo	C
Desconexión física	Control de acceso del personal	Baja	Alto	B
Corte de servicio en servidores externos e internos	Respaldo	Baja	Alto	B
Falla sobre núcleos de comunicaciones		Media	Alto	A
Saturación en el núcleo de comunicaciones		Media	Alto	A
Saturación de carga en el enlace		Media	Alto	A
Corte de energía	Mantenimiento de UPS	Bajo	Medio	B

Inundaciones, terremotos , Incendios, interrupción del servicio de internet, entre otros	Extinguidores, rutas de evacuación y mantenimiento de equipos en un altura considerable para casos de inundaciones	Baja	Alto	B
Back ups desactualizados	Copias en medios extraíbles	Media	Alto	A
Accesos no restringidos	bitácora de acceso a la información	Media	Alto	A
Deficiencias en las medidas de seguridad para el tratamiento de la información		Media	Alto	A
Procesamiento incorrecto de datos		Baja	Medio	B
Infecciones con virus, troyanos u otro malware	Antivirus	Media	Alto	A
Procedimientos para el tratamiento de la información no valida		Media	Alto	A
Ataques externos		Media	Medio	B
Personal insatisfecho		Baja	Medio	B
Falla en el control de las licencias	Registro de las adquisiciones de licencias.	Baja	Bajo	C

Caídas y cuelgues del sistema		Media	Alto	A
Ataques internos		Baja	Medio	B
Fallas en los conectores eléctricos	Mantenimiento de UPS	Baja	Medio	B
Medios extraíbles	La entidad propicia los medios extraíbles para el traspaso de las bases de datos	Baja	Medio	B
Mantenimiento	Cada año se realiza una revisión de las instalaciones y del equipo	Baja	Bajo	C
Hacker, Cracker		Media	Medio	B
Incumplimiento		Media	Medio	B

Evaluación de los riesgos

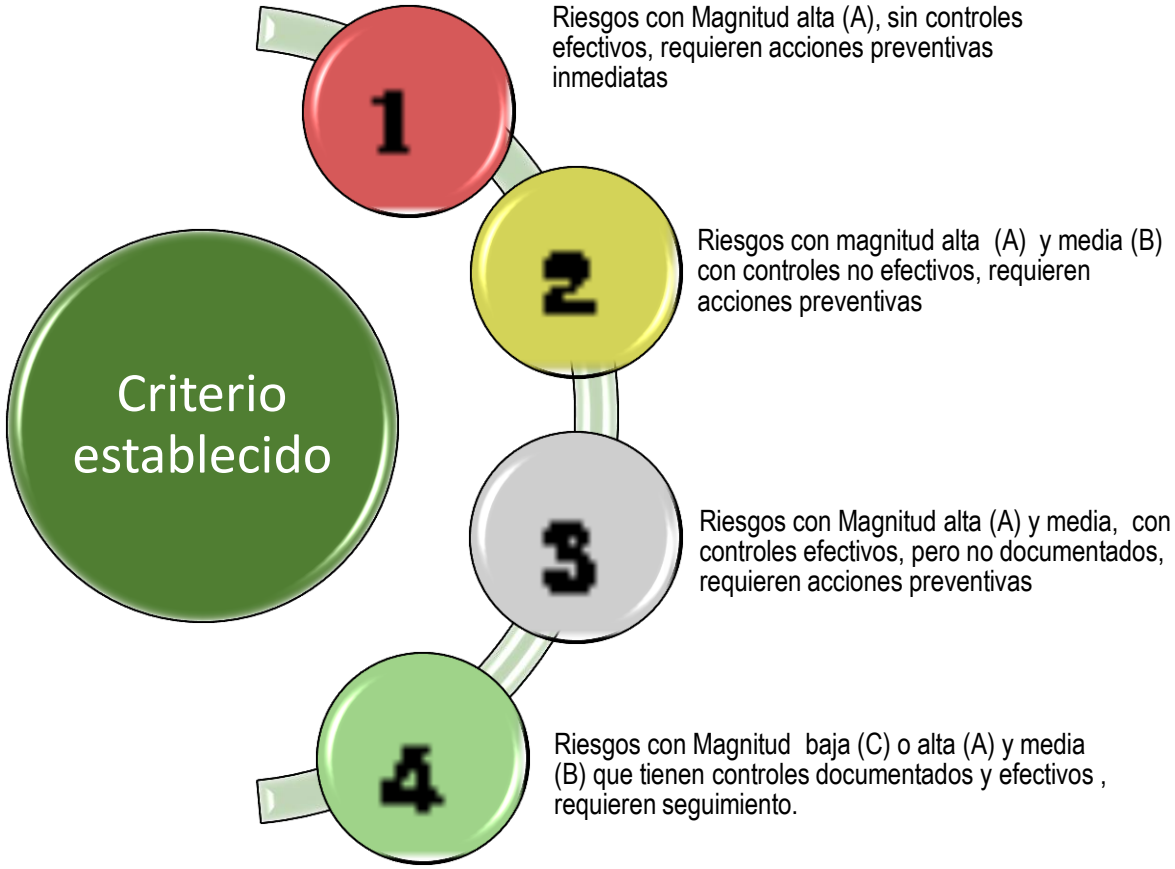


Figura 5: Criterio de evaluación el riesgo

Evaluación de los riesgos

Una vez definidos los criterios de la evaluación del riesgo se procede a realizar la respectiva evaluación que se detalla a continuación:

Riesgo	Criterio	Tratar el riesgo
Falla en el UPS	3	SI
Falla en equipos de ventilación	4	NO
Desconexión física	4	NO
Corte de servicio en servidores externos e internos	3	SI
Falla sobre núcleos de comunicaciones	1	SI
Saturación en el núcleo de comunicaciones	1	SI
Saturación de carga en el enlace	2	SI
Corte de energía	4	NO
Inundaciones, terremotos , Incendios, interrupción del servicio de internet, entre otros	2	SI
Back ups desactualizados	2	SI
Accesos no restringidos	2	SI
Deficiencias en las medidas de seguridad para el tratamiento de la información	1	SI
Procesamiento incorrecto de datos	1	SI
Infecciones con virus, troyanos u otro malware		
Procedimientos para el tratamiento de la información no valida	1	SI

Ataques externos	1	SI
Personal insatisfecho	2	SI
Falla en el control de las licencias	3	SI
Caídas y cuelgues del sistema	2	SI
Ataques internos	1	SI
Fallas en los conectores eléctricos	4	NO
Medios extraíbles	1	SI
Mantenimiento	4	NO
Hacker, Cracker	2	SI
Incumplimiento	2	SI

B.5 Opciones de tratamiento del riesgo

Tratamiento de los riesgos

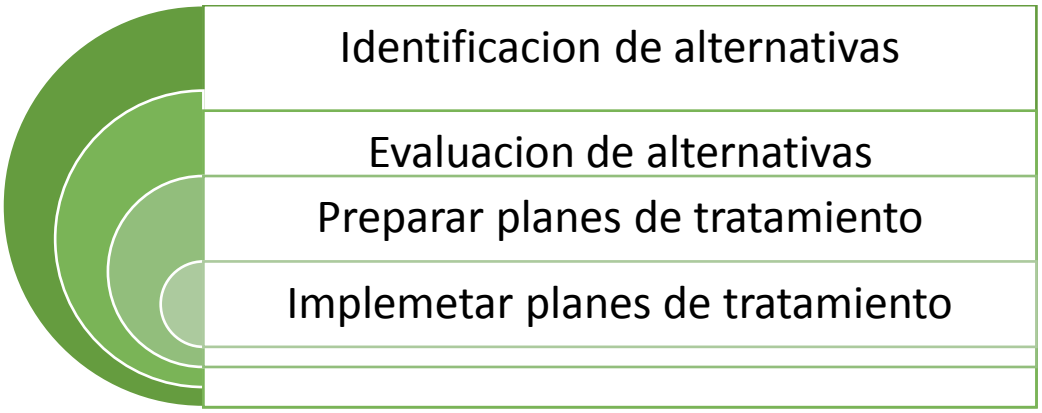


Figura 6 Opciones de tratamiento

Identificación de las alternativas

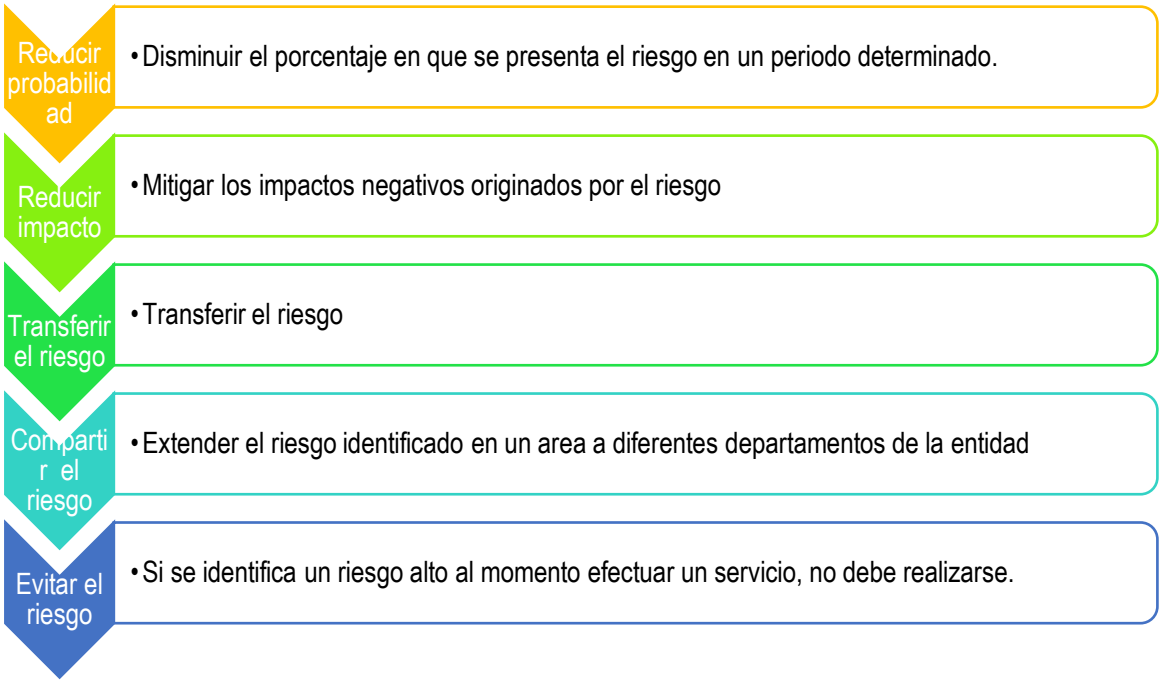


Figura7Alternativas para mitigar el riesgo

Evaluación de alternativas

Para determinar la evaluación de las alternativas se toma en cuenta las opciones de tratamiento establecidas anteriormente.

N°	Riesgo	Alternativa de manejo	Área responsable
1	Falla en el UPS	Reducir el impacto	Mantenimiento
2	Falla en equipos de ventilación		
3	Desconexión física		
4	Corte de servicio en servidores externos e internos	Reducir impacto	Mantenimiento

5	Falla sobre núcleos de comunicaciones	Reducir impacto	Mantenimiento
6	Saturación en el núcleo de comunicaciones	Reducir probabilidad	Mantenimiento
7	Saturación de carga en el enlace	Reducir probabilidad	Mantenimiento
8	Corte de energía		
9	Inundaciones, terremotos , Incendios, interrupción del servicio de internet, entre otros	Transferir el riesgo	
10	Back ups desactualizados	Reducir probabilidad	Gerencia administrativa
11	Accesos no restringidos	Reducir impacto	Gerencia administrativa
12	Deficiencias en las medidas de seguridad para el tratamiento de la información	Reducir el impacto	Gerencia administrativa y personal a cargo del departamento
13	Procesamiento incorrecto de datos	Reducir probabilidad	Personal a cargo del departamento
14	Infecciones con virus, troyanos u otro malware	Reducir impacto	Mantenimiento
15	Procedimientos para el tratamiento de la información no valida	Reducir probabilidad	Personal a cargo del departamento
16	Ataques externos	Reducir impacto	
17	Personal insatisfecho	Reducir impacto	

18	Falla en el control de las licencias	Reducir probabilidad	Mantenimiento
19	Caídas y cuelgues del sistema	Reducir impacto	Mantenimiento
20	Ataques internos	Reducir impacto	Mantenimiento y gerencia
21	Fallas en los conectores eléctricos		
22	Medios extraíbles	Reducir impacto	Mantenimiento
23	Mantenimiento		
24	Hacker, Cracker	Reducir impacto	
25	Incumplimiento: de carácter legal y técnico	Reducir impacto	Gerencia administrativa

B.6 Objetivos de control y controles para el tratamiento del riesgo

Una vez identificado el riesgo de la entidad, el impacto, magnitud y probabilidad y determinado las opciones de tratamiento del riesgo se determina un plan de tratamiento detallado a continuación a través de los controles para cada dominio:

1. Política de seguridad		
Alcance: Determinar con exactitud la dirección de la política alineados a los objetivos del negocio.		
Objetivo: • **Proporcionar a la gerencia la dirección para el resguardo de la información de acuerdo a las leyes y regulaciones aplicables**		
Controles		
1.1Política de seguridad de la información		
	Objetivo de control	Controles
1.1.1	Documento de la política de la seguridad de la información	• Establecer el compromiso de la gerencia • Definición de seguridad de información, objetivos

		y alcances • Establecer el marco referencial • Describir una breve explicación de las políticas, principios y estándares. • Definir las responsabilidades para la gestión de la seguridad de la información
1.1.2	Revisión de la política de seguridad de la información	• Verificar que la información deba ser realizada en tiempos determinados.

2. Organización de la seguridad de la información		
Alcance: La gerencia debe establecer un marco referencial para el control e implementación de la seguridad de la información		
Objetivo: Operar la seguridad de la información en el contexto interno de la entidad		
Controles		
2.1 Organización interna		
	Objetivo de control	Controles
2.1.1	Compromiso de la gerencia con la seguridad de la información	• Identificar que los objetivos de seguridad cumplan con los requerimientos organizacionales • Diseñar y aprobar la política de seguridad de la información • Proporcionar los recursos necesarios para la seguridad la organización.
2.1.2	Coordinación de la seguridad de la información	• Verificar que la seguridad de la información involucre la colaboración de los gerentes, usuarios y administradores. • Aprobar las metodologías y procesos para la seguridad de la información • Promover la educación, capacitación y conocimiento de la seguridad de la información.

		• Verificar y evaluar los reportes del monitoreo y los incidentes de seguridad.
2.1.3	Asignación de las responsabilidades de la seguridad de la información	• Definir claramente las responsabilidades de la información • Documentar los detalles de las responsabilidades, así como también documentar los niveles de autorización. • Identificar y revisar que los requerimientos de confidencialidad determinan las necesidades de la entidad para la protección de la información.
2.1.4	Contacto de las autoridades	• Mantener la comunicación con las autoridades relevantes ya sea internas o externas.

3. Gestión de activos		
Alcance: La entidad identificara sus activos y la asignación de la responsabilidad para la determinación y mantenimiento de los controles aplicables.		
Objetivo: • **Lograr y mantener una apropiada protección de los activos de 4G S.A de C.V**		
Controles		
3.1	**Responsabilidad por los activos**	
	Objetivo de control	Controles
3.1.1	Inventario de los activos	Identificar todos los activos, elaborar y mantener inventario de todos los activos significativo.
3.1.2	Propiedad de los activos	La información y los activos relacionados con los medios de procesamiento de información debieran estar designados previamente por la entidad.
3.2	Clasificación de la información	
3.2.1	Lineamientos de clasificación	Clasificar la información de acuerdo a su valor, requerimientos legales y sensibilidad para la entidad.

3.2.2	Etiquetado y manejo de la información:	Desarrollar e implementar procedimientos de manejo seguros, almacenaje, transmisión, clasificación y destrucción en términos de clasificación de la entidad.

4. Seguridad de recursos humanos		
Alcance: recursos humanos debe seguir parámetros al momento de la selección de los empleados, contratistas y terceros.		
Objetivo: • **Establecer procesos para asegurar que los empleados, contratistas y terceros conozcan las responsabilidades para los cuales son contratados y reducir el riesgo del mal uso de los recursos.**		
Controles		
4.1	**Antes del empleo**	
	Objetivo de control	Controles
4.1.1	Roles y responsabilidades Selección. Término y condiciones de empleo.	• Definir y documentar roles y responsabilidades del personal • Realizar chequeos de verificación de antecedentes de los empleados de acuerdo a leyes, regulaciones y etiquetas relevantes • Definir documento que establezca compromisos términos y condiciones de las responsabilidades de los empleados que deberán firmar y aceptar
4.2	Durante el empleo	
4.2.1	Gestión de responsabilidades Capacitación y educación en seguridad de la información Proceso disciplinario	• Establecer un requerimiento que los empleados cumplen con los procedimientos y políticas de la entidad. • Establecer capacitaciones, actualizaciones de políticas, procedimientos relevantes para las funciones laborales. • Implementar un proceso disciplinario.

4.2.2	Terminación o cambio de empleo	• Definir responsabilidades respecto a la terminación o cambio de empleo. • Documentar la devolución de activos en la terminación del empleo. • Eliminar los derechos de acceso a la información y los medios de procesamiento de información.

5. Seguridad física y del entorno		
Alcance: Los medios de procesamiento de información deben estar ubicados en lugares seguros definidos y deberá estar protegido de accesos no autorizados.		
Objetivo: Proteger de la pérdida, daño y robo de los activos de la entidad, así como también del acceso no autorizado a la información y locales de la entidad.		
Controles		
5.1	**Seguridad física y control de acceso físico**	
	Objetivo de control	Controles
5.1.1	Medidas de seguridad física y acceso físico	• Utilizar perímetros de seguridad como lo son tarjetas o una persona encargada de proteger el área que contiene la información, para el acceso físico proteger mediante controles de ingreso apropiados.
5.1.2	Ubicación y protección del equipo	• Ubicar y proteger el equipo para disminuir el riesgo de amenazas y peligros ambientales y de personas no autorizadas, así como también el registro de fallas sospechosas o reales.
5.1.3	Políticas y procedimientos para personal contratado y mantenimiento de la infraestructura	• Definir los procesos para la incorporación de nuevos elementos a la entidad. • Definir los procesos a seguir para el mantenimiento de la infraestructura.
5.1.4	Protección de las tecnologías de	• Se debe llevar un control del software

	información	instalado, copias de respaldo al momento de actualizaciones o cambios de software.

6. Gestión de las comunicaciones y operaciones		
Alcance: La entidad debe determinar responsabilidades a todos los niveles apropiados y si es necesario establecer la segregación de funciones para determinar los procedimientos para la gestión y operación del procesamiento de los datos		
Objetivo: Resguardar en forma segura y correcta de los medios de procesamiento de la información		
Controles		
6.1	**Procedimientos y responsabilidades operacionales**	
	Objetivo de control	Controles
6.1.1	Procedimientos de operaciones documentados:.	Documentar, mantener y proporcionar a los usuarios que lo necesiten los procedimientos de operación
6.1.2	Gestión de cambio:	Controlar los cambios en medios y sistemas de procesamiento de la información
6.1.3	Segregación de deberes:	Las áreas de responsabilidad y los deberes deben estar segregados para reducir accesos no autorizados, modificaciones o utilizar los activos sin detección y autorización.
6.2	Gestión de la entrega del servicio de terceros	
6.2.1	Entrega del servicio:	Asegurar que los controles referentes a la entrega de servicios de terceros se implementen, operen y cumplan respecto a la seguridad, definiciones establecidas y niveles de entrega de los servicios
6.2.2	Monitoreo y revisión de los servicios de terceros:	Monitorear, revisar regularmente y realizar auditorías regularmente respecto de los

		servicios, reportes y registros provistos por terceros.
6.3	Planeación y aceptación del sistema	
6.3.1	Gestión de capacidad:.	Para asegurar el desempeño del sistema se debe Monitorear y detallar el uso de los recursos así como realizar proyecciones de los requerimientos de capacidad futura de los sistemas
6.3.2	Aceptación de sistemas:	Establecer el criterio de aceptación de los sistemas de información nuevos, actualizaciones y desarrollar pruebas durante el desarrollo y antes de la aceptación.
6.4	Protección contra el código malicioso y móvil	
6.4.1	Controles sobre software maliciosos:.	Implementar procedimientos para propiciar conocimiento adecuado al usuario establecer un sistema de control de detección, prevención y recuperación para proteger contra códigos maliciosos y otros
6.4.2	Controles contra códigos móviles:	Cuando se autorice el uso de códigos móviles se deben asegurar que dicho código opere de acuerdo con la política de seguridad definida, evitando ejecutar códigos móviles no autorizados.
6.5	Respaldo o Back-up	
6.5.1	Back-up:	Realizar copias de respaldo de la información y software y probar regularmente en un período establecido en la política de copias de respaldo.
6.6	Gestión de seguridad de la Red	

6.6.1	Seguridad en Red:	Establecer un adecuado manejo para la protección de la información en las redes y mantener así la seguridad de los sistemas y aplicaciones. Así mismo se deben Identificar las características de seguridad, los niveles de servicio y requerimientos de gestión
6.7	Gestión de medios	
6.7.1	Gestión de los medio removibles:	Determinar los procedimientos para la correcta gestión de los medios removibles de acuerdo así serán re-usados o si serán eliminados.
6.7.2	Seguridad de la documentación del sistema:.	Establecer una protección de la documentación del sistema con accesos no autorizados
6.8	Intercambio de información	
6.8.1	Procedimientos y políticas de información y software:	Establecer una política, procedimientos y controles
6.8.2	Acuerdos de intercambio:	Para el acuerdo del intercambio se deben considerar el manejo de las responsabilidades, procedimientos para notificar, procedimientos para asegurar el rastreo, acuerdos de depósitos, estándares, responsabilidades y obligaciones en incidentes de seguridad, uso del sistema de etiquetado, propiedad y responsabilidad de la protección de data derechos de autor, licencias de software y cualquier otro que se requiera para la protección en el despacho y recepción de la información,

6.8.3	Mensajes electrónicos:	Establecer una protección de la información involucrada en el mensaje electrónico respecto a los accesos no autorizados, la correcta dirección y transporte del mensaje la confiabilidad y disponibilidad y los niveles de autenticación.
6.9	Servicios de comercio electrónico	
6.9.1	Comercio electrónico:	La información a que la se hace referencia en el comercio electrónico debe protegerse de la actividad fraudulenta, disputas de contratos, divulgación no autorizada y modificación
6.9.2	Información disponible públicamente:	Proteger la integridad de la información puesta a disposición del público en general, con respecto a la modificación no autorizada
6.10	Monitoreo	
6.10.1	Registro de auditoría:	Establecer y mantener registros de auditorías en relación con las actividades, eventos e incidentes de la seguridad de la información y monitorear el control de acceso
6.10.2	Uso del sistema de monitoreo:	Establecer procedimientos para el monitoreo del usos de medios de procesamiento así como de revisar los resultados de las actividades de monitoreo.
6.10.3	Protección del registro de información:	Proteger los medios de registro y la información del registros con el fin de evitar la alteración y el acceso no

		autorizado
6.1.0.4	Registros del administrador y operador:	Registrar las actividades del administrador y operador del sistema
6.10.5	Registro de fallas:	Registrar y analizar las fallas, establecer las acciones necesarias.

7. Control de acceso		
Alcance: Controlar a los niveles de entidad y terceros relacionados los niveles de acceso. Medios de procesamiento en relación a los requerimientos comerciales reglas de control tomando en cuenta las políticas para la divulgación y autorización de la información.		
Objetivo: Controlar en la entidad el acceso a la información		
Controles		
7.1	**Requerimiento del negocio para el control de acceso**	
	Objetivo de control	Controles
7.1.1	Política de control de acceso	Establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad del acceso
7.2	Gestión de acceso del usuario	
7.2.1	Gestión de privilegios	Realizar un procedimiento para el registro y remoción del registro del usuario para otorgar y revocar el acceso a los sistemas de información; así como la restricción y control de privilegios.
7.2.2	Gestión de claves de usuario	Asignar claves que se deben controlar en un sistema de gestión formal para establecer a nivel de usuario, así como la identificación del usuario antes de otorgarle claves
7.3	Responsabilidades del usuario	
7.3.1	Uso de claves	Requerir a los usuarios las buenas prácticas de seguridad para mantener la confidencialidad de las claves y la complejidad que deben llevar dichas claves.

7.3.2	Políticas de pantalla y escritorio limpio	Adoptar una política de escritorio limpio para papeles y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
7.4	Control de acceso a la red	
7.4.1	Política sobre los servicios de uso de red	Los usuarios únicamente deben tener acceso a los servicios de red estrictamente para los que están autorizados.
7.4.2	Autenticación de usuario para conexiones externas	Determinar los métodos de autenticación para el control de accesos de usuarios remotos.
7.4.3	Protección del puerto de diagnóstico remoto	Controlar el acceso físico y lógico a los puestos de diagnóstico y configuración.
7.4.4	Control de conexiones de red	Para redes compartidas se debe restringir la capacidad de los usuarios para conectarse a la red con relación con la política de control de acceso.
7.5	Control de acceso al sistema operativo	
7.5.1	Procedimiento en la terminal	Establecer un procedimiento de registro seguro para el acceso de los sistemas operativos
7.5.2	Identificación y autenticación del usuario	Establecer un ID de usuario y escoger una técnica de autenticación para validar la identidad del usuario
7.5.3	Sistema de gestión de claves	Establecer que los sistemas de gestión de claves sean interactivas asegurar que sean las mejores.
7.5.4	Limitación de tiempo de conexión	Utilizar restricciones relacionados a los tiempos de conexión, con el fin de establecer adicionalmente seguridad para las aplicaciones de alto riesgo
7.6	Control de acceso a la aplicación y a la información	
7.6.1	Restricción al acceso a la información	Limitar en relación con la política de control de acceso, a los usuarios y al personal de soporte a la información y funciones del sistema
7.7	Computación y tele-trabajo móvil	
7.7.1	Computación móvil y comunicaciones	Establecer e implementar una política las medidas de

		seguridad apropiadas con el fin de proteger de los riesgos que implica el uso de los medios de computación y comunicación móvil
8. Adquisición, desarrollo y mantenimiento de los sistemas de información		
Alcance: El diseño e implementación de los sistemas de información son decisivos para la seguridad, por lo que la identificación y acuerdo de los requerimientos de seguridad.		
Objetivo: • **Garantizar que la seguridad sea la principal características de los sistemas de información.** • **Prevenir el mal uso de la información de las aplicaciones de la entidad.** • **Proteger la confidencialidad, integridad y disponibilidad por medio de técnicas criptográficas.**		
Controles		
8.1	**Requerimientos de seguridad de los sistemas de información**	
	Objetivo de control	Controles
8.1.1	Análisis y especificaciones de los sistemas:	• Especificar los requerimientos de los controles de seguridad. • Determinar el valor de los activos de información y el daño que este causaría como resultado de una falla o falta de seguridad.
8.1.2	Procesamiento correcto de las aplicaciones	• Verificar el input data para las aplicaciones para asegurar que los registros efectuados sean correctos. • Revisión periódica de los campos para confirmar su validez. • Verificar la validación que la aplicación y detectar cualquier acto deliberado de corrupción.
8.2	Controles criptográficos	
8.2.1	Políticas sobre el uso de controles criptográficos	• Desarrollar y por consiguiente implementar una política sobre técnicas de criptográficas para el resguardo de la información. • Establecer una gestión de claves para dar

		soporte a las técnicas criptográficas • Protección de las técnicas de encriptado contra modificación, pérdida y divulgación no autorizada.
8.3	Seguridad del archivo del sistema	
8.3.1	Controles de software operacional	• Establecer procedimientos para el control de la instalación de software en los sistemas de la entidad. • Las actualizaciones del software debe realizarse por los administradores encargados. • Evitar el uso de las bases de datos para propósitos de prueba, que contenga información personal o información confidencial
8.4	Seguridad de los procesos de seguridad de cambio	
8.4.1	Procedimientos de control de cambio	• Controlar la implementación de los cambios del sistema mediante procedimientos. • Documentar los procesos formales del control de cambio. • Revisar y probar las aplicaciones para comprobar la integridad y que no se haya visto afectada por los cambios del sistema.
8..4.2	Filtración de información	• Evitar las oportunidades para la filtración de la información • Monitorear la utilización de recursos en los sistemas • Monitorear las actividades efectuadas por los empleados. • Inspeccionar los medios en busca de información escondida.
8.5	Gestión de vulnerabilidades técnicas	
8.5.1	Control de la vulnerabilidades	• Obtener información sobre las vulnerabilidades

	técnicas	técnicas de los sistemas de información • Definir roles y responsabilidades para la gestión de las vulnerabilidades y evaluación del riesgo de las vulnerabilidades

9. Gestión de incidentes y mejoras en la seguridad de la información.		
Alcance: Establecer procedimientos en cuanto a eventos fortuito y debilidades de la seguridad de la información		
Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información con relación a los sistema de información sean comunicado de manera oportuna a través de acciones correctivas con el fin de minimizar el impacto y garantizando la seguridad de los activos de la entidad.		
Controles		
9.1	Reporte de eventos y debilidades de la seguridad de la información.	
	Objetivo de control	Controles
9.1.1	Reporte de eventos de seguridad de información:	Establecer reportes de manera oportuna sobre entornos que pongan en riesgo la seguridad de la información, por medio de la comunicación a través de la gerencia.
9.1.2	Reporte de debilidades en la seguridad:	Desarrollar requerimientos encaminados a que los usuarios, empleados y encargados del departamento de sistema y seguridad de la información tomen nota y generen reportes sobre cualquier debilidad o anomalía que ponga en riesgo la seguridad de la información.
9.2	Gestión de incidentes y mejoras en la seguridad de la información.	
9.2.1	Responsabilidades y procedimientos:	Establecimiento de responsabilidades y procedimientos en cuanto a respuestas rápida, efectiva por parte de la gerencia ante los incidentes de la seguridad de la información.
9.2.2	Educarse a través de los incidentes de seguridad de la información:	Establecer mecanismo para permitir medir y monitorear los tipos, volúmenes, y costo de los

		incidentes de información.
9.2.3	Recolección de evidencia:	Implementar controles sobre recolección de evidencia por medio de acciones de seguimiento contra un empleado u organización en cumplimiento con las leyes civiles establecidas en el país.

10. Gestión de continuidad del negocio.		
Alcance: Implementar procesos de gestión sobre continuidad del negocio para disminuir el riesgo sobre la entidad y factores que afecten los activos de la información.		
Objetivo: Desarrollar controles para identificar y minimizar riesgos que afecten la continuidad del negocio.		
Controles		
10.1	Aspectos de seguridad de la información con respecto a la continuidad del negocio	
	Objetivo de control	Controles
10.1.1	Proceso de gestión de continuidad del negocio incluyendo la seguridad de la información:	Implementar, desarrollar y mantener proceso de continuidad del negocio por medio de la gerencia para el tratamiento de la seguridad de la información indispensable para la continuidad de la entidad.
10.1.2	Evaluación del riesgo sobre la continuidad de la entidad:	Identificar sucesos que provoquen interrupciones en las actividades comerciales de la entidad así como evaluación del riesgo ante la probabilidad de dichos sucesos.
10.1.3	Desarrollar e implementar planes de continuidad de la entidad:	Desarrollar e implementar planes para mantener, restaurar las operaciones en caso de interrupción y asegurando la disponibilidad de la información en forma oportuna cumpliendo con las escalas de tiempo sin que afecte los procesos.
10.1.4	Marco referencial de planeación de continuidad de la entidad:	Implementar un solo marco referencial enfocado a la continuidad del negocio como en los requerimientos de seguridad de la información.
10.1.5	Prueba, mantenimiento, re-evaluación	Ejecutar procedimientos para evaluar la continuidad

	de planes de continuidad de la entidad:	del negocio de manera que sean probados, actualizados y efectivos antes los eventos.
11. Cumplimiento.		
Alcance: implementar un diseño de control interno para uso, operación y gestión de los sistemas de información sujetos a los requerimientos de seguridad estatuarios, reguladores y contractuales		
Objetivo: Evitar incumplimientos a los requerimientos legales e incumplimiento de las políticas y estándares de seguridad aplicables a las tecnologías de información.		
Controles		
11.1	**Cumplimiento de los requerimientos legales**	
	Objetivo de control	Controles
11.1.1	Identificación de la legislación aplicable:	Documentar y actualizar los requerimientos estatutarios, reguladores y contractuales. Orientado a la gerencia para la satisfacción de los requerimientos del sistema de información.
11.1.2	Derecho de propiedad intelectual:	Implementar procedimientos para el cumplimiento de los requerimientos legislativos, reguladores y contractuales con relación al derecho de propiedad intelectual y uso de patente.
11.1.3	Protección de registros organizacionales:	Protección de registros importante de pérdida, destrucción, falsificación en concordancia con los requerimientos estatutarios, reguladores y contractuales.
11.1.4	Protección de la data y privacidad de la información personal:	Desarrollar e implementar política de protección y privacidad de la data en conformidad con la legislación y cláusulas contractuales relevantes.
11.1.5	Prevención del mal uso de los procesamiento de información:	Desarrollar procedimientos de monitoreo en los medios de procesamiento de información para propósitos de verificar el mal uso de los mismo por parte de los empleados de la entidad.

11.1.6	Regulación de controles criptográficos:	Implementar controles encaminados a las funciones criptográficas en cumplimiento con las leyes y Regulaciones nacionales.
11.2	Cumplimiento de las políticas y estándares de seguridad	
11.2.1	Cumplimiento con las políticas y estándares de seguridad:	La gerencia será la encargada que se lleven a cabo el cumplimiento de políticas, estándares y procedimiento de seguridad
11.2.2	Chequeo del cumplimiento técnico:	La verificación de los sistemas de información deberán de chequearse regularmente de acuerdo a los estándares de implementación
11.3	Consideraciones de auditoría de los sistemas de información.	
11.3.1	Controles de auditoría de los sistemas de información:	Desarrollo de controles para las actividades, encaminadas a los requerimientos de auditoría y para la salvaguarda de los sistemas de información.
11.3.2	Protección de las herramientas de auditoría de los sistemas de información.	Desarrollo de controles para el acceso de herramientas de auditoría de los sistemas de información con el fin de minimizar el mal uso o transgresión posible.

B.7 Documentación

El documento del manual de control interno basado en riesgos de tecnologías de información se encuentra establecido en el anexo N° VIII.

B.8 Autorización de la gerencia para implementar y operar el control interno informático

Autorización de la gerencia para implementar y operar el control interno informático.

Entidad: 4G, S.A de C.V
Responsable: Gerencia administrativa
Asunto: Autorización del control interno informático

Autorización para implementar y operar el control interno informático
Objetivo: • Documentar los acuerdos de la gerencia administrativa relacionado a la implementación y operacionalización del control interno informático.
Compromiso de la gerencia en apoyar la seguridad de la información.
Asegurar que los objetivos de la seguridad de la información estén alineados con los elementos de la entidad y sus procesos.
Aprobación de la política de la seguridad de la información
Compromiso gerencial ante nuevas políticas, procedimientos y controles para la seguridad de la información.
Compromiso ante un plan de capacitaciones y concientización del recurso humano en cuanto a la seguridad de la información.
Implementación de los controles y la coordinación para el cumplimiento de estos en toda la entidad y ante terceros cuando sea necesario.

F: _____
Firma de la gerencia

F:_____ F: _____ F: _____
Firma de los sustentantes

San Salvador ____ de_____ de 2015

B.9 Enunciado de aplicabilidad

Se establece el enunciado de aplicabilidad y se detalla en el Anexo N° 6

Paso C Implementar y operar.

C.1 Plan de tratamiento del riesgo

El plan de tratamiento de riesgos se detalla en el Anexo N° 7

C.2 Implementación del plan de tratamiento del riesgo

Una vez se definió el plan de tratamiento del riesgo en el Anexo N° 7 se procede a la implementación por parte de la entidad tomando en cuenta todas las consideraciones necesarias

C.3 Implementación de controles seleccionados

Estos se encuentran definidos en el paso 2 y es en esta etapa que se implementan dichos controles

C.4 Programas de capacitación y conocimiento

Definidos en el Apéndice A del manual diseño de control interno informático.

C.5 Manejar las operaciones del control interno informático

En referencia al plan de tratamiento del riesgo, la implementación de programas de capacitación y conocimiento, los recursos y procedimientos.

C.6 Manejar los recursos del control interno informático

Se debe tomar en cuenta la gestión de los recursos y propiciar que estos sean útiles para el establecimiento, implementación y operación del control interno informático; así como del monitoreo y revisión del mismo

Paso D Monitorear y revisar

La entidad a través de la administración y los comités de seguridad de la información son los garantes de que se cumplan los procedimientos descritos respecto al monitoreo y a revisar el control interno informático para lo cual deberán desarrollar los procedimientos descritos en la tabla 7

CAPÍTULO IV CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Al analizar cada uno de los resultados obtenidos en el instrumento de investigación se concluye lo siguiente:

- Las empresas distribuidoras de los servicios de telefonía no cuentan con un modelo de control interno informático en su mayoría, manteniendo controles básicos por lo que su sistema de información se vuelve vulnerable ante pérdida o extracción de información.

- La verificación de un sistema de control interno informático está a cargo de la auditoría interna, sin embargo es la auditoría externa la que realiza la verificación de los controles de la entidad.

- Al no contar con un diseño de control interno las entidades están expuestas a las pérdidas de las características de confidencialidad, integridad y disponibilidad de la información.

- Un alto porcentaje de profesionales en contaduría pública desconoce la temática de la gestión de las Tecnologías de Información.

- Los profesionales de la contaduría pública cubren su formación de educación continuada requerida por el Consejo, principalmente en las áreas de contabilidad, auditoria y tributación.

- La mayoría de los profesionales de la contaduría pública por factores como altos costos de formación profesional, capacitaciones no acreditadas para horas de educación continuada, desconocimiento de la temática, son factores por los cuales no se forman en el área de Tecnologías de Información.

- Los profesionales con conocimientos de la temática que diseñan u ofertan un modelo de control interno informático, utilizan como marco de referencia para tal caso, el marco Coso ERM, que si bien es cierto es una herramienta que contribuye con algunos controles no es el indicado para la gestión de la seguridad de la información

4.2 Recomendaciones

- Que las distribuidoras implementen un diseño de control interno para mantener la información protegida y segura.

- Capacitar a los profesionales de la contaduría pública a la vanguardia de los avances tecnológicos respecto de la salvaguarda e integridad de los sistemas de información.

- Que un diseño de control interno informático sea elaborado bajo el marco integrado de COBIT en su versión 5 a fin de establecer un sistema que cumpla con lineamientos y estándares necesarios para establecer un Sistema de Gestión de la Seguridad de la Información adecuado.

- Que la presente propuesta se tome en consideración a fin de ser una herramienta útil para las entidades distribuidoras de los servicios de telefonía en El Salvador respecto a la salvaguarda e integridad de los sistemas de información.

- A los centros de formación superior implementar en sus asignaturas la temática y aplicación de las tecnologías de información, y que estas se encuentren a la vanguardia de las actualizaciones referentes al dicha área.

- A las asociaciones, corporaciones, gremios y grupos afines a la carrera de la contaduría pública, implementar en los seminarios, congresos, capacitaciones entre otros, las temáticas orientadas a las tecnologías de información y comunicación.

- A los profesionales que han participado en el diseño de controles internos informáticos regirse por el marco de COBIT 5 a fin de establecer controles fuertes tanto a nivel preventivo como correctivo minimizando los factores de riesgos, a los que las entidades están expuesta diariamente.

BIBLIOGRAFÌA

Alvarez, S. &. (2011). El habeas data como instrumento juridico de la proteccion al individuo contra el uso ilegal o indebido de sus datos personales en buros de credito e instituciones financieras, San Salvador.

Comite Internacional de Estandarización. (2005). 27000, ISO Sistema de gestion de la seguridad de la informacion.

Comite Internacional de Estandarización. (2005). 27001, ISO Tecnologias de la informacion- Tecnologias de seguridad - Sistemas de gestion de la seguridad de la informacion - requerimientos.

Comite Internacional de Estandarización. (2005). 27002, ISO Tecnologias de informacion, tecnincas de seguridad- Codigo para la practica de la gestion de la seguridad de la informacion.

Comite Internacional de Estandarización. (2009). 31000, ISO Gestion de riesgos- principios y guias.

Huercano, S. R. (2007). Manual ITIL V3. Obtenido de http://www.itlibrary.org/

ISACA. (2012). Cobit 5.

Mejia Guardado, S. (2008). Diseño de un modelo de control interno administrativo para la Facultad de Ciencias Economicas de la Universidad de El Salvador .

Organismo Salvadoreño de Normalización OSN. (s.f.). OSN. Obtenido de www.osn.gob.sv

Perini, A. y. (s.f.). (Habeas Data. Derecho a la Intimidad, pág. 21.

redseguridad.com. (s.f.). Revista especializada en seguridad. Obtenido de www.redseguridad.com

Vasquez Jerez, J. (s.f.). Historia de las telecomunicaciones. Tetecomunicaciones.

ANEXOS

ANEXO N° I

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

CUESTIONARIO

DIRIGIDO A: Los contadores públicos autorizados por el Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoría.

OBJETIVO: Obtener información relevante de como los profesionales de la contaduría pública y auditoría responden a los riesgos de tecnologías de información (TI), en empresas que manejan información de terceros

PROPÓSITO: La presente guía de preguntas ha sido elaborada por estudiantes de la carrera de licenciatura de contaduría pública, con el propósito de sustentar el trabajo de investigación relativo a controles la identificación y evaluación de riesgos de tecnologías de información

INDICACIONES: Marque con una "X" la(s) respuesta(s) que usted considere más conveniente o complementar según el caso.

1. ¿Posee conocimiento sobre gestión de tecnologías de información y comunicación? Si su respuesta es no, pase a la pregunta 5.

   SI ☐ NO ☐

2. ¿En dónde obtuvo conocimientos sobre control interno para tecnologías de información y comunicación? (puede seleccionar más de una opción)

   a. Congresos ☐
   b. Seminarios ☐

c. Libros ☐

d. Plan continúo de educación ☐

e. Documentos informativos ☐

f. Programas de formación y de prácticas ☐

.¿Cuáles de las siguientes temáticas han sido abordadas en la formación sobre tecnologías de información que ha recibido? puede marcar más de una opción.

a. Protección de activos de TI ☐

b. Ciclo de vida de los sistemas ☐

c. Infraestructura de TI ☐

d. Gobierno de TI ☐

e. Entrada, soporte y servicio (DSS) ☐

f. ISO 27002 ☐

g. COBIT ☐

h. Ninguna de las anteriores ☐

3. ¿Considera queposee la competencia profesional adecuada sobre control interno relacionado a tecnología de información y comunicación, que sea suficiente para prestar un servicio de calidad en el campo laboral?

SI ☐ NO ☐

4. Dentro del marco de educación continuada seleccione del siguiente listado en qué áreas ha cubierto las horas de actividad educativa que requiere el Consejo.

a. Normas internacionales de contabilidad ☐

b. Normas internacionales de auditoría ☐

c. Tributación ☐

d. Leyes penales ☐

e. Leyes mercantiles ☐
f. Áreas especializadas (bancos, seguro, entre otros) ☐
g. Código de ética profesional ☐
h. Otras materias relacionadas a la profesión ☐

5. ¿Ha participado en el diseño de un control interno informático? Si su respuesta es no pase a la pregunta 9.

Si ☐ No ☐

6. ¿Para qué tipo de empresas ha diseñado control interno informático? (puede seleccionar más de una opción).

a. Firmas de auditoría ☐
b. Empresas comerciales ☐
c. Empresas de servicio ☐
d. Empresas industriales ☐
e. Empresas agrícolas ☐
f. Empresas públicas ☐
g. Organismos internacionales ☐
h. ONG`s ☐

7. ¿Qué marcos de referencia utiliza para diseñar controles internos basados en tecnología de información?

a. COBIT 5 ☐
b. Estándares ISO ☐
c. COSO ERM ☐
d. ITIL ☐
e. Enfoque MAGERIT ☐

8. ¿En la firma de auditoría que labora ofrece dentro de su catálogo o portafolio el servicio de diseño de controles internos?

   Si ☐ No ☐

Si su respuesta es sí, marque del siguiente listado los tipos de controles internos que ofrece.

   a. Control interno administrativo ☐
   b. Control interno contable ☐
   c. Control interno informático ☐

9. ¿Cuáles de los siguientes aspectos considera importante que deben ir en relación al cumplimiento de los objetivos de un control interno informático?

   a. Cumplimiento de la legalidad de la entidad ☐
   b. Protección adecuada de los objetivos del negocio ☐
   c. Procedimientos adecuados para gestiones administrativas ☐
   d. Planificación e implantación de controles de seguridad para la información ☐

10. ¿Cuáles de las siguientes categorías considera usted son imprescindibles de considerar para el diseño de un sistema de control interno?

   a. Principios, políticas y marcos de gestión aplicables al negocio ☐
   b. Procesos implementados en la entidad ☐
   c. Estructuras organizacionales y sus funciones principales ☐
   d. Evaluación de riesgos asociados a la entidad ☐
   e. Respuestas a los riesgos detectados ☐
   f. Procedimientos a seguir ☐
   g. Monitoreo y revisión de las gestiones del riesgo ☐

11. Del siguiente listado seleccione cuales riesgos pueden ser asociados con las tecnologías de informaciónqueconsideraríapara el diseño de un control interno informático

a. Riesgos estratégicos ☐
b. Riesgos ambientales ☐
c. Riesgos de mercado ☐
d. Riesgos de crédito ☐
e. Riesgos operacionales ☐
f. Riesgos de cumplimiento ☐

12. ¿Qué se debe incluir en un sistema de gestión de la seguridad de la información? Puede seleccionar más de una opción.

    a. Manual de la seguridad ☐
    b. Procedimientos ☐
    c. Instrucciones ☐
    d. Checklists ☐
    e. Formularios ☐
    f. Registros ☐

13. De las siguientes opciones determine según su criterio ¿Cuál sería el motivo deque algunos profesionales de la contaduría pública y auditoría no cubren su formación en el área de tecnologías de información?

    a. Altos costos de formación profesional ☐
    b. No lo considera importante la temática ☐
    c. Desconocimiento sobre el tema ☐
    d. Falta de aplicación dentro de la profesión. ☐

ANEXO N° II

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

CUESTIONARIO

DIRIGIDO A: Las distribuidoras de telefonía en El Salvador

OBJETIVO: Obtener información relevante de cómo las empresas distribuidoras manejan controles de TI, y las respuestas a los riesgos identificados en las tecnologías de información (TI).

PROPÓSITO: La presente guía de preguntas ha sido elaborada por estudiantes de la carrera de licenciatura de contaduría pública, con el propósito de sustentar el trabajo de investigación relativo a controles la identificación y evaluación de riesgos de tecnologías de información

INDICACIONES: Marque con una "X" la(s) respuesta(s) que usted considere más conveniente o complementar según el caso.

1. ¿Cuenta la entidad con el área de auditoría interna?

   a) Si ☐ b) No ☐

2. Del siguiente listado, seleccione el o los tipos de controles que implementa la entidad.

a) Control interno administrativo ☐
b) Control interno financiero ☐
c) Control interno contable ☐
d) Control interno informático ☐
e) Ninguno ☐

3. En caso de contar con control interno informático ¿Qué tipo de especialistas se requieren para el control interno de las TI? Si no cuenta con control interno informático pase a la siguiente pregunta.

   a. Técnicos en informática ☐
   b. Ingenieros en sistemas ☐
   c. Ingenieros en telecomunicaciones ☐
   d. Técnicos en redes ☐
   e. Electricistas ☐
   f. Técnicos en sistemas de computación ☐

4. ¿Quién realiza el trabajo de verificación del sistema de control interno que implementa la entidad? (puede seleccionar más de una opción)

   a. Auditorías especiales ☐
   b. Auditoría interna ☐
   c. Auditoría externa ☐
   d. Auditoría en sistemas ☐
   e. Personal administrativo ☐
   f. Gerencia o el gobierno administrativo ☐
   g. La telefónica mediante auditorías y supervisión ☐
   h. Socios o accionistas de la entidad ☐

5. ¿Cómo se realiza la formación del capital humano para el área de tecnologías de información dentro de la entidad? (Puede seleccionar más de una opción)

   a. Capacitaciones ☐
   b. Experiencia en el área ☐
   c. Seminarios de especialización ☐

6. Para preservar la confidencialidad de la información. ¿Qué controles implementa la entidad? (Puede seleccionar más de una opción)

   a. Autorización solo a personal autorizado ☐
   b. Codificación de la información ☐
   c. Certificados digitales ☐
   d. Redes perimetrales de seguridad ☐
   e. Listas de control de acceso ☐
   f. Técnicas de cifrado ☐
   g. Administrador de base datos ☐

7. Para salvaguardar la integridad de la información. ¿Qué controles implementa la entidad? (Puede seleccionar más de una opción)

   a. Modificación solo mediante personal autorizados ☐
   b. Criptografía ☐
   c. Registro de actividades y eventos ☐
   d. Autorización de usuarios a nivel de transacción ☐
   e. Seguridad lógica ☐
   f. Seguridad a nivel de sistema operativo ☐

8. Para mantener la disponibilidad de la información. ¿Qué controles implementa la entidad? Puede seleccionar más de una opción)

   a. Copias de respaldo de la información contenida en la base de datos ☐
   b. Autenticación de usuarios ☐
   c. Prevención de ataques de denegación de servicios ☐

9. ¿Cuáles son los servicios que mayor demanda tienen dentro de la entidad? Puede seleccionar mas de una opción)

   a. Contratos de fidelización ☐
   b. Telefonía prepago ☐
   c. Telefonía pos-pago ☐
   d. Renovación de contratos ☐
   e. Internet ☐
   f. Video vigilancia ☐
   g. Servicio de cable ☐
   h. TV satelital ☐

10. ¿La entidad ha tenido conocimiento de incidentes de extracción o pérdida de información?

    Si ☐ No ☐

11. ¿Cuál ha sido la respuesta por parte de la entidad hacia los incidentes de extracción o pérdida de datos? (Puede seleccionar más de una opción)

    a. Establece y mantiene una vista de riesgo común ☐
    b. Integra un sistema de control interno basado en riesgos ☐
    c. Toma decisiones consistentes de los riesgos del negocio ☐
    d. Realiza una correcta comunicación del riesgo ☐
    e. No ha tenido incidentes ☐

12. ¿Qué tipo de medidas se implementan para asegurar la protección de los datos de los usuarios y/o clientes? (Puede seleccionar más de una opción)

    a. Mediante controles ☐
    b. Contratos con la empresa ☐
    c. Contratos de confidencialidad ☐
    d. Políticas ☐

e. Encripción de información ☐

13. Del siguiente listado seleccione las amenazas para la seguridad de la información que usted considere más comunes dentro de la entidad. (Puede seleccionar más de una opción)

a. Fuga de datos (por descuidos o violación) ☐
b. Errores no intencionales de los empleados ☐
c. Los incidentes relacionados con los dispositivos personales de los empleados ☐
d. Cloud computing ☐
e. Ataques cibernéticos ☐
f. Hacking externo ☐
g. Personal insatisfecho ☐

14. ¿Qué medidas de seguridad se implementa al momento de compartir información relacionada a datos del cliente? (Puede seleccionar más de una opción)

a. Cifrado ☐
b. Firmas digitales ☐
c. Encriptación ☐
d. Ninguna ☐

¿Por qué razón considera que las entidades no implementan un control interno?

a. La empresa es considerada pequeña ☐
b. Altos costos ☐
c. No poseen los recursos necesarios para implementarlo ☐
d. No es necesario ☐

15. ¿Estaría interesado la administración en utilizar un modelo de control internos de tecnología de información para la protección, resguardo y aseguramiento de la información?

Si ☐ No ☐

ANEXO N° III

TABULACIÓN Y ANÁLISIS DE LA INFORMACIÓN RECOPILADA

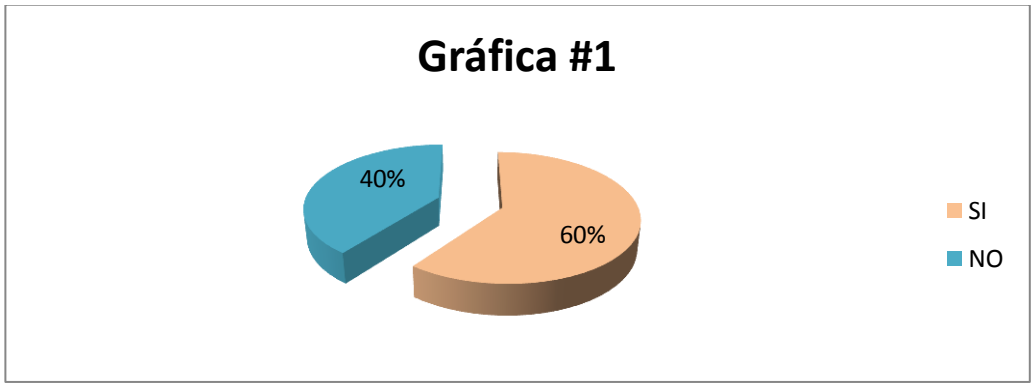
Tabulación y análisis de la información recopilada a los profesionales de la contaduría pública.

Análisis e interpretación de datos

1. ¿Posee conocimiento sobre gestión de tecnologías de información y comunicación?

Objetivo: Conocer el nivel de conocimientos que el contador público cuenta para poner en práctica controles para el manejo y aseguramiento de la información que maneja.

	FRECUENCIA	
RESPUESTA	ABSOLUTA	RELATIVA
SI	35	60.34%
NO	23	39.66%
TOTAL	58	100.00%

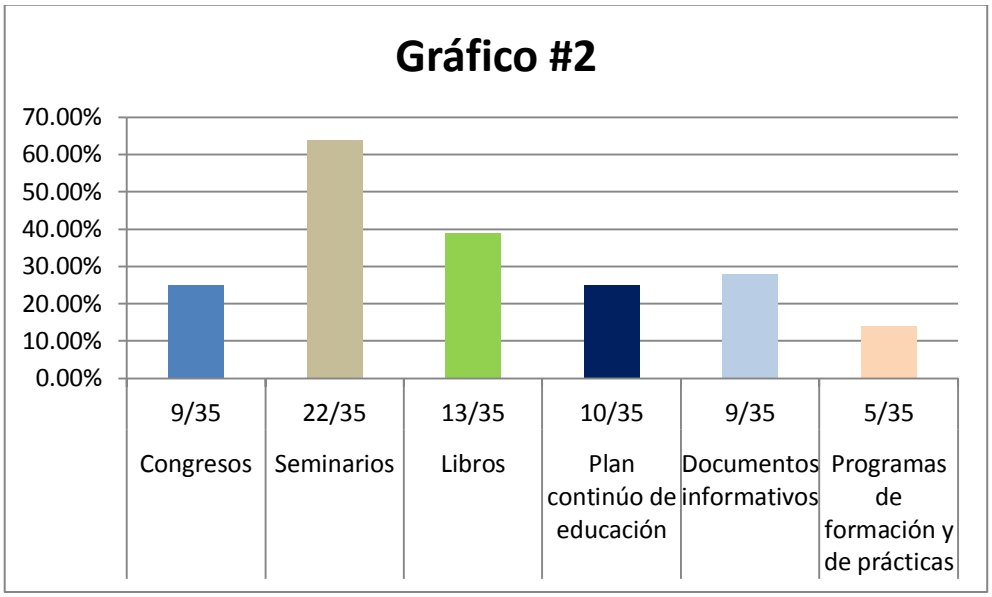


Análisis:Del total de encuestado; el 6O% afirma tener conocimientos sobre la gestión de tecnología de información y comunicación para poner en práctica controles que le sea útil para el manejo y aseguramiento de la información.

2. ¿En dónde obtuvo conocimientos sobre control interno para tecnologías de información y comunicación?

Objetivo: Conocer cuáles son los medios en el cual el contador público ha adquirido conocimientos relacionados a tecnologías de información.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Congresos	9/35	25.00%
B	Seminarios	22/35	63.89%
C	Libros	13/35	38.89%
D	Plan continúo de educación	10/35	25.00%
E	Documentos informativos	9/35	27.78%
F	Programas de formación y de prácticas	5/35	13.89%

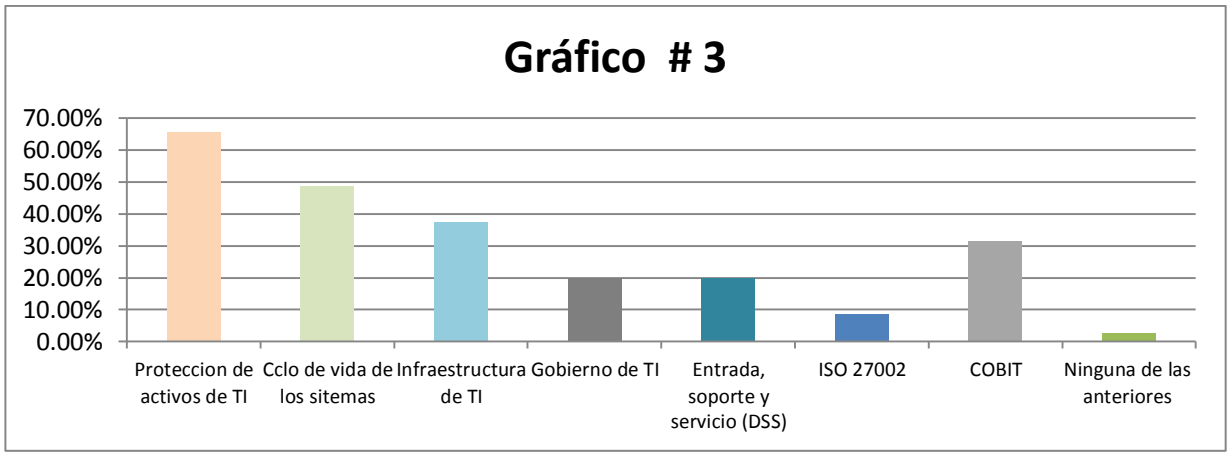


Análisis: Un total del 23 de los 35 encuestados en comunión con la pregunta 1, afirma tener conocimientos sobre la gestión de tecnología de información y comunicación a través de seminarios, ya que los congresos, libros y la educación continua, no aborda con mucha frecuencia los temas relacionados a tecnologías de información.

3. ¿Cuáles de las siguientes temáticas han sido abordadas en la formación sobre tecnologías de información que ha recibido?

Objetivo: Conocer los temas que se implementan y el conocimiento que el contador público adquiere.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Protección de activos de TI	23/35	65.71%
B	Ciclo de vida de los sistemas	17/35	48.57%
C	Infraestructura de TI	13/35	37.14%
D	Gobierno de TI	7/35	20.00%
E	Entrada, soporte y servicio (DSS)	7/35	20.00%
F	ISO 27002	3/35	8.57%
G	COBIT	11/35	31.43%
H	Ninguna de las anteriores	1/35	2.86%

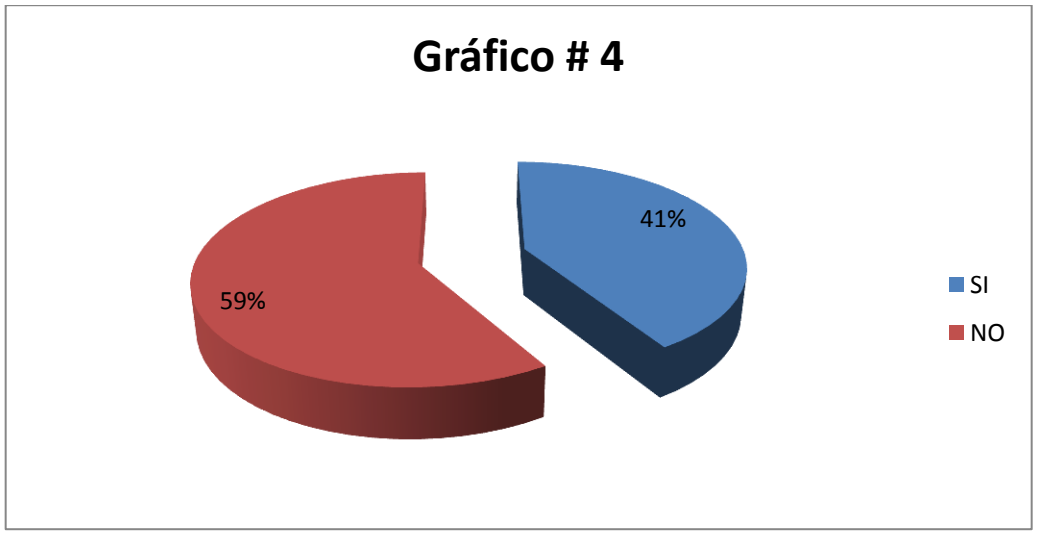


Análisis: Un total de 23 contadores públicos que representa el 58% de la muestra afirma que dentro de su formación en el área de tecnología de la información la temática con mayor énfasis abordada ha sido en la protección de activo de TI, por lo que es un tema de mucha importancia ya que se sabrá cómo mantener una adecuada gestión de protección de los activos.

4. ¿Considera que posee la competencia profesional adecuada sobre control interno relacionado a tecnología de información y comunicación y que esta es suficiente para prestar un servicio de calidad en el campo laboral?

Objetivo: Determinar si el contador público considera que posee los conocimientos obtenidos son suficientes para poder ser aplicados en el campo laboral.

	FRECUENCIA	
RESPUESTA	ABSOLUTA	RELATIVA
SI	14	41.18%
NO	20	58.82%
TOTAL	34	100.00%

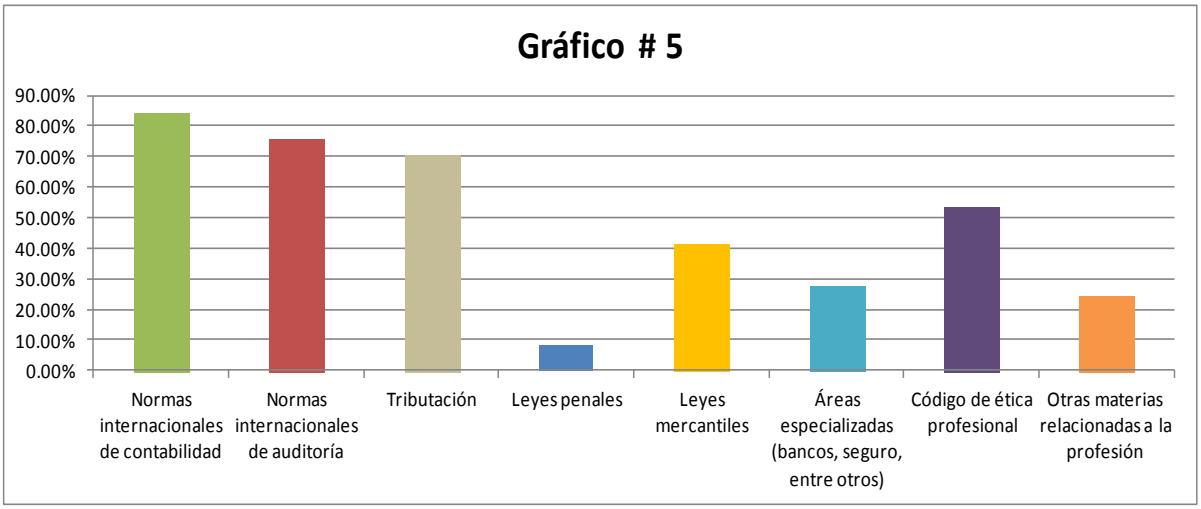


Análisis: Del 100% de los encuestados el 59% afirma no poseer la competencia profesional suficiente para prestar un servicio de calidad en relación al control interno de tecnología de información y comunicación; en relación con la pregunta 1 a pesar de poseer conocimiento sobre dicha área, no se tiene la formación adecuada para desempeñar un servicio de calidad dentro de dicho campo laboral, debido a las limitantes que existen en el proceso de formación profesional.

5. Dentro del marco de educación continuada seleccione del siguiente listado en qué áreas ha cubierto las horas de actividad educativa que requiere el Consejo.

Objetivo: Indagar sobre los conocimientos de tecnologías de información que se imparten como educación continuada.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Normas internacionales de contabilidad	49/58	84.48%
B	Normas internacionales de auditoría	44/58	75.86%
C	Tributación	41/58	70.69%
D	Leyes penales	5/58	8.62%
E	Leyes mercantiles	24/58	41.38%
F	Áreas especializadas (bancos, seguro, entre otros)	16/58	27.59%
G	Código de ética profesional	31/58	53.45%
H	Otras materias relacionadas a la profesión	14/58	24.14%

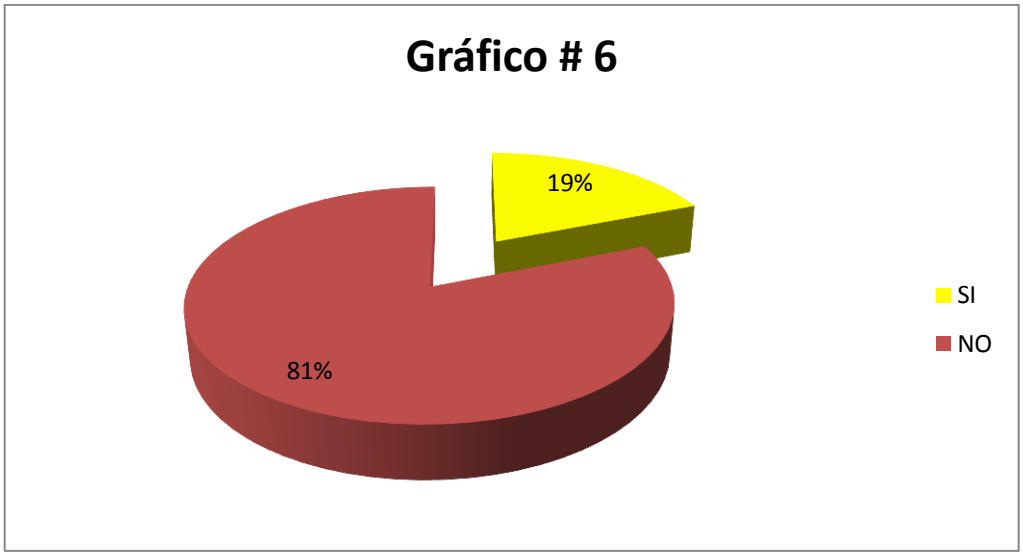


Análisis: Las normas internacionales de contabilidad, auditoria y tributación con el 84%, 76% y 71% respectivamente son las áreas que los contadores cubren dentro del marco de educación continuada requerido por el consejo;de tal manera que los profesionales de contaduría pública se especializan más en el área financiera y fiscal y las áreas especializadas solo tienen una participación cerca de la tercera parte.

6. ¿Ha participado en el diseño de un control interno informático?

Objetivo: Conocer en qué medida el contador público ha participado en controles internos para el área de tecnologías de información en empresas con sistemas informáticos.

	FRECUENCIA	
RESPUESTA	ABSOLUTA	RELATIVA
SI	11	18.97%
NO	47	81.03%
TOTAL	58	100.00%

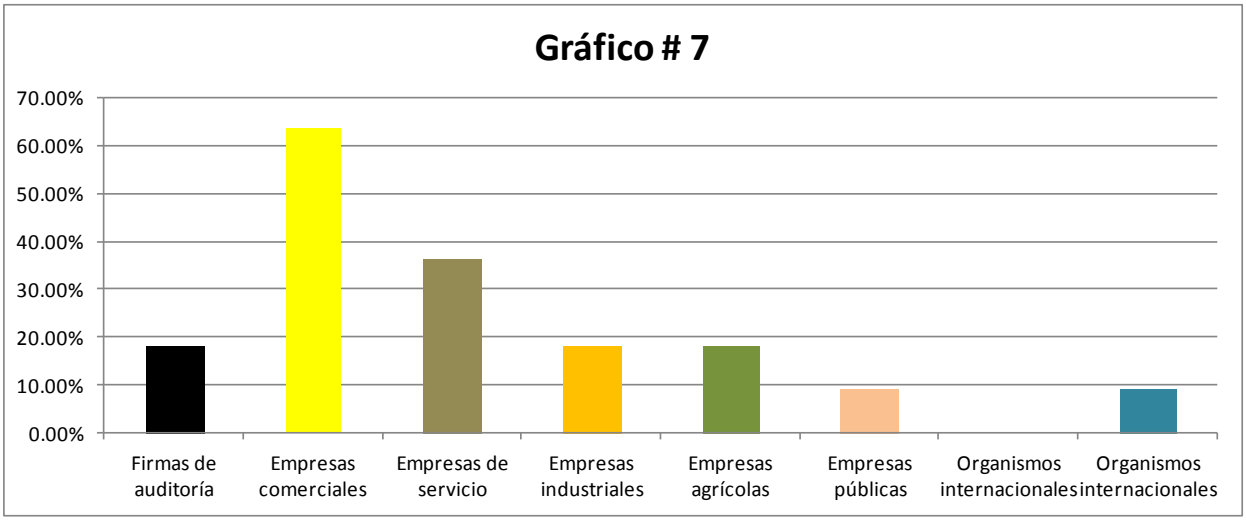


Análisis: Del total de encuestado; el 81% afirma no haber participado en el diseño de un control interno informático, lo cual es congruente de acuerdo a los resultados de la pregunta #1 en la que no todos poseen conocimientos de tecnologías de información y los que han tenido participación en el área según los resultados de la pregunta #3 destacan pocos temas abordados dentro de su formación.

7. ¿Para qué tipo de empresas ha diseñado control interno informático?

Objetivo: Conocer para que tipos de empresas el contador público ha desarrollado controles internos.

		FRECUENCIA	
	REPUESTA	ABSOLUTA	RELATIVA
A	Firmas de auditoría	2/11	18.18%
B	Empresas comerciales	7/11	63.64%
C	Empresas de servicio	4/11	36.36%
D	Empresas industriales	2/11	18.18%
E	Empresas agrícolas	2/11	18.18%
F	Empresas públicas	1/11	9.09%
G	Organismos internacionales	0/11	0.00%
H	Organismos internacionales	1/11	9.09%

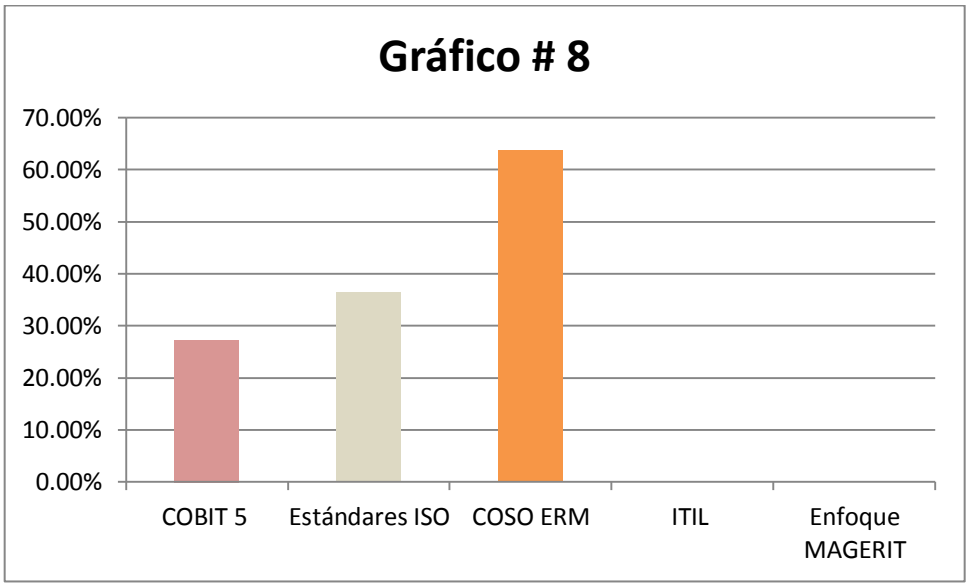


Análisis: Del 19% de contadores públicos que han participado en el diseño de un control interno informático, el 64% lo ha elaborado para empresas comerciales en ese sentido; el 64% ha tomado de referencia el marco COSO ERM en relación con la pregunta 8.

8. ¿Qué marcos de referencia utiliza para diseñar controles internos basados en tecnología de información?

Objetivo: Conocer el marco de referencia utilizado para el diseño e implementación de un control interno informático.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	COBIT 5	3/11	27.27%
B	Estándares ISO	4/11	36.36%
C	COSO ERM	7/11	63.64%
D	ITIL	0/11	0.00%
E	Enfoque MAGERIT	0/11	0.00%

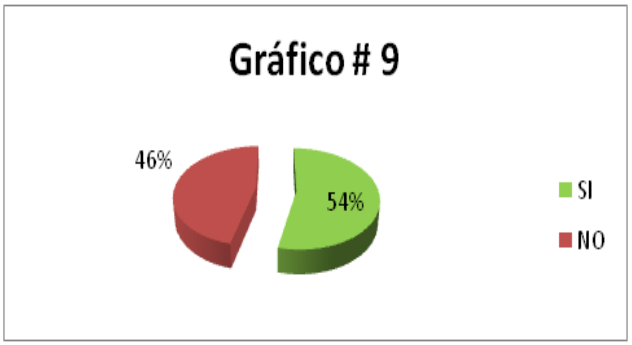


Análisis: del total de encuestados que manifestaron haber participado en el diseño de control interno informático han tomado de referencia el marco COSO ERM, en ese sentido para el diseño de dicho control interno no se utiliza un marco especializado en controles de tecnologías de información como lo es COBIT, ITIL y estándares ISO.

9. ¿En la firma de auditoría que labora ofrece dentro de su catálogo o portafolio el servicio de diseño de controles internos?

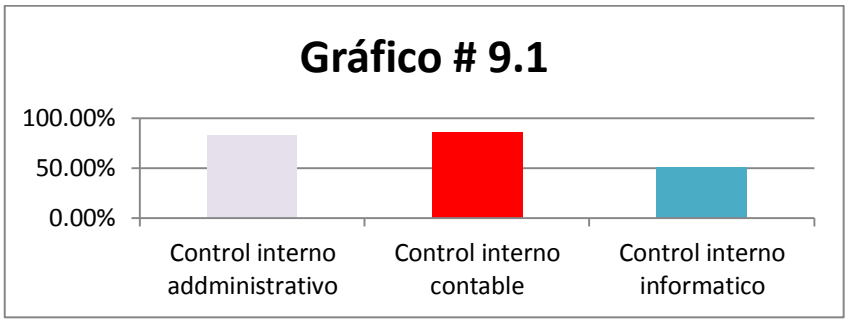
Objetivo: Conocer sí las firmas de auditoría diseñan controles y la participación del contador público en el diseño de los mismos.

	FRECUENCIA	
CATEGORIA	ABSOLUTA	RELATIVA
SI	29	53.70%
NO	25	46.30%
TOTAL	54	100.00%



Marque del siguiente listado los tipos de controles internos que ofrece.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Control interno administrativo	24/29	82.76%
B	Control interno contable	25/29	86.21%
C	Control interno informático	15/29	51.72%

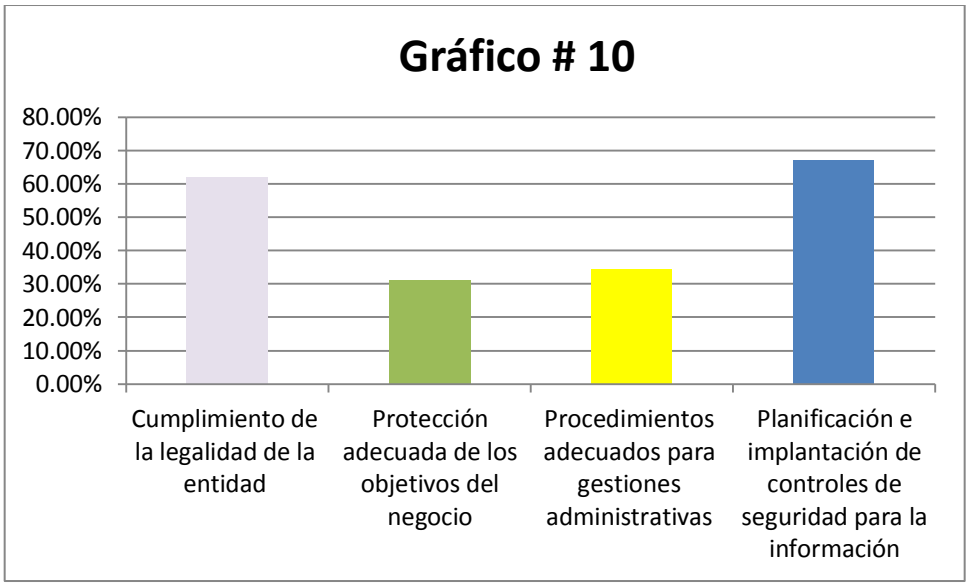


Análisis: El 53% de los encuestados afirman que la firma donde laboran ofrecen el servicio de diseño de control interno; en este sentido, el diseño cuya mayor demanda obtiene la entidad con el 86% es el diseño de control interno contable, es por ello que no todos los que ofertan el servicio de control interno en el área de tecnologías de información han tenido la oportunidad de diseñar un control interno informático; tal cual lo muestran los resultados de la pregunta # 6.

10. ¿Cuáles de los siguientes aspectos considera importante en relación al cumplimiento de los objetivos de un control interno?

Objetivo: Indagar los aspectos más importantes para el cumplimiento de los objetivos de control interno plasmados por los profesionales de la contaduría pública.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Cumplimiento de la legalidad de la entidad	36/58	62.07%
B	Protección adecuada de los objetivos del negocio	18/58	31.03%
C	Procedimientos adecuados para gestiones administrativas	20/58	34.48%
D	Planificación e implantación de controles de seguridad para la información	39/58	67.24%

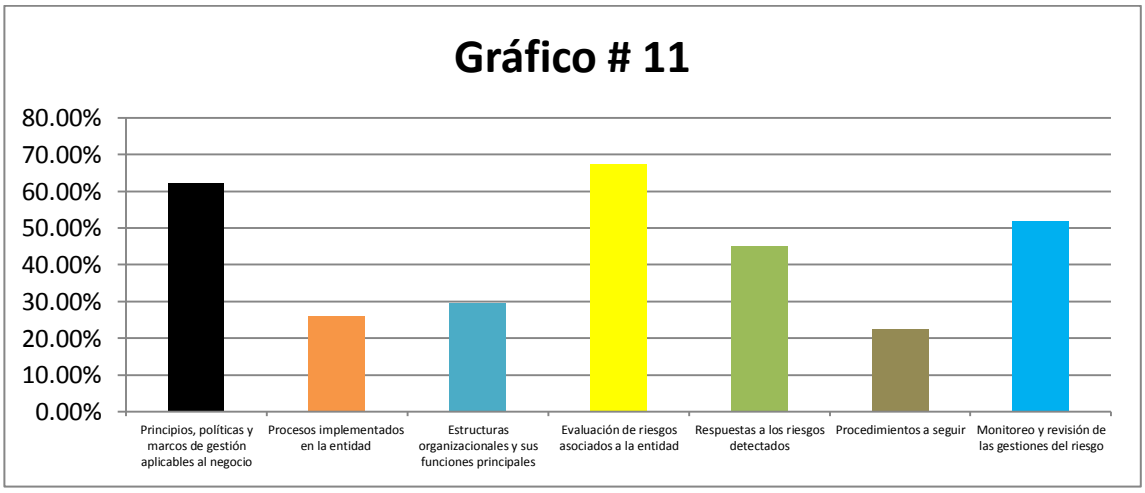


Análisis: El 67% de los encuestados manifiesta que la planificación e implementación de controles de seguridad para la información es el aspecto más importante en relación al cumplimiento de un control interno informático que se debería tomar en consideración para el diseño como tal.

11. ¿Cuáles de las siguientes categorías considera usted son imprescindibles de considerar para el diseño de un sistema de control interno?

Objetivo: Determinar las categorías necesarias que se deben comprender en el diseño de un control interno informático.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Principios, políticas y marcos de gestión aplicables al negocio	36/58	62.07%
B	Procesos implementados en la entidad	15/58	25.86%
C	Estructuras organizacionales y sus funciones principales	17/58	29.31%
D	Evaluación de riesgos asociados a la entidad	39/58	67.24%
E	Respuestas a los riesgos detectados	26/58	44.83%
F	Procedimientos a seguir	13/58	22.41%
G	Monitoreo y revisión de las gestiones del riesgo	30/58	51.72%

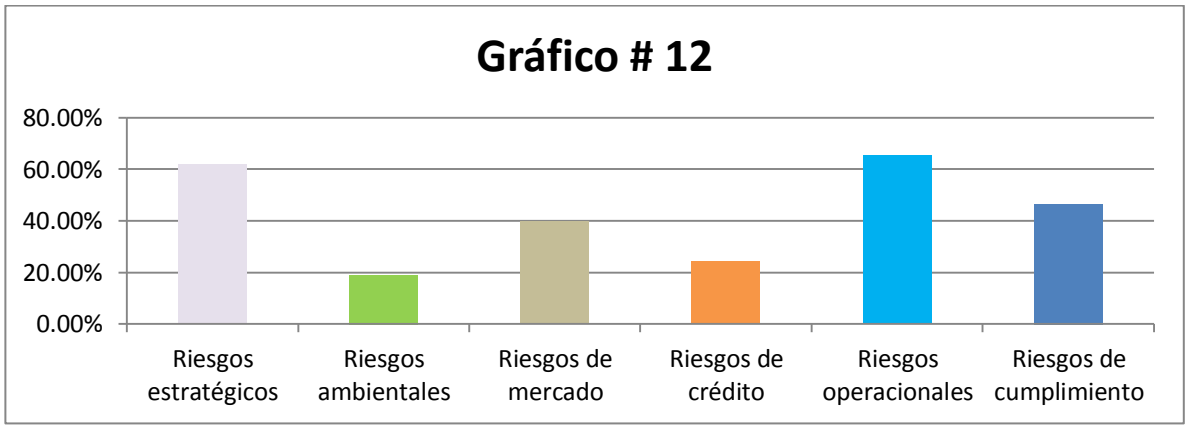


Análisis: La evaluación de riesgos asociados a la entidad y los principios, políticas y marcos de gestión aplicable al negocio; con el 67% y 62% respectivamente para los encuestados es considerada de vital importancia para el diseño de un sistema de control interno, es así que la evaluación de riesgos busca identificar y eliminar riesgos presentes en el entorno; tal cual COBIT y la ISO 27002 validan lo anterior.

12. Del siguiente listado seleccione cuales de los riesgos pueden ser asociados con las tecnologías de información consideraría para el diseño de un control interno informático

Objetivo: Determinar cuáles son los riesgos más frecuentes asociados a las tecnologías de información que han sido considerados dentro del diseño de un control interno informático.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Riesgos estratégicos	36/58	62.07%
B	Riesgos ambientales	11/58	18.97%
C	Riesgos de mercado	23/58	39.66%
D	Riesgos de crédito	14/58	24.14%
E	Riesgos operacionales	38/58	65.52%
F	Riesgos de cumplimiento	27/58	46.55%



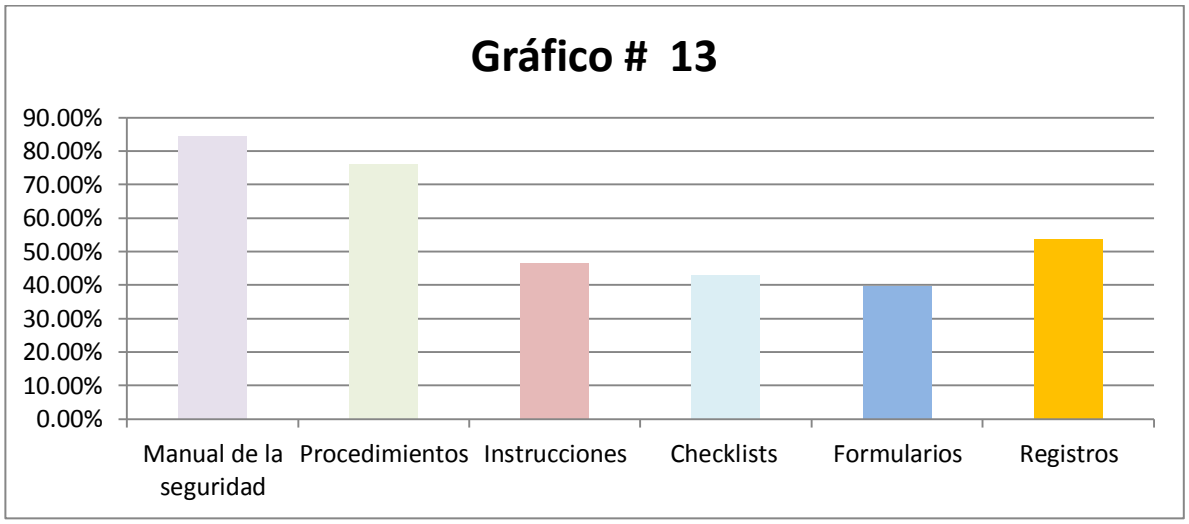
Análisis: Los encuestados opinaron que los riesgos operacionales y los riesgos estratégicos; con el 65% y 62% respectivamente son los riesgos mayormente asociado con la tecnología de información, en ese sentido el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, y los sistemas internos o externos son los mayores riesgos a los que se debe dar respuestas mediante controles relacionados a las tecnologías de información.

.

13. ¿Qué se debe incluir en un sistema de gestión de la seguridad de la información? Puede seleccionar más de una opción.

Objetivo: Determinar los factores fundamentales para la gestión de la calidad de los sistemas de información.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Manual de la seguridad	49/58	84.48%
B	Procedimientos	44/58	75.86%
C	Instrucciones	27/58	46.55%
D	Checklists	25/58	43.10%
E	Formularios	23/58	39.66%
F	Registros	31/58	53.45%

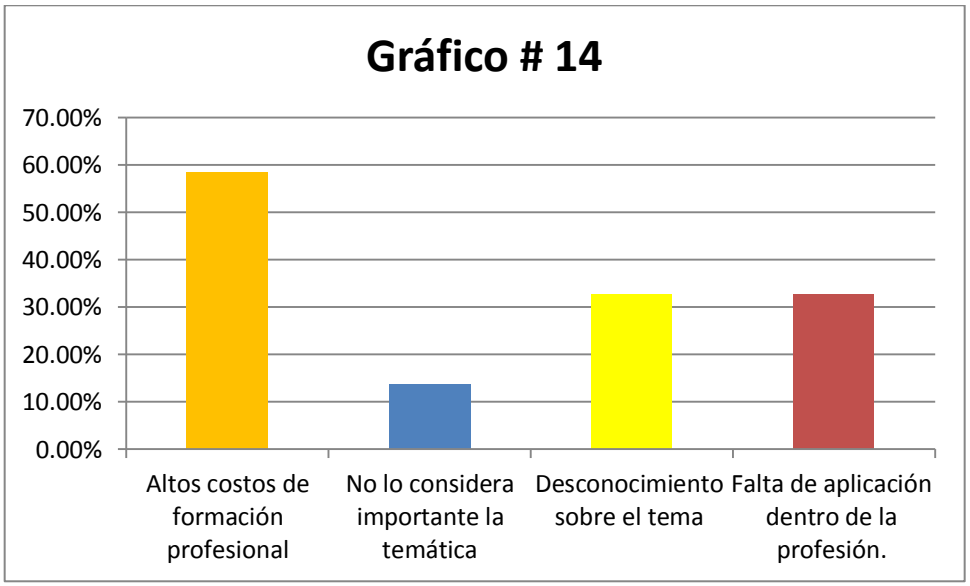


Análisis: Los encuestados opinaron que el manual de seguridad es el elemento que se debe incluir en un sistema de gestión de la seguridad de la información, además de los procedimientos y registros, es por ello que el adecuado cumplimiento es un punto clave para el logro de los objetivos y finalidad.

14. De las siguientes opciones determine según su criterio ¿Cuál sería el motivo de que algunos profesionales de la contaduría pública y auditoría no cubren su formación en el área de tecnologías de información?

Objetivo: Indagar cuáles son las razones por las que el contador público no ha obtenido conocimientos sobre tecnologías de información.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Altos costos de formación profesional	34/58	58.62%
B	No lo considera importante la temática	8/58	13.79%
C	Desconocimiento sobre el tema	19/58	32.76%
D	Falta de aplicación dentro de la profesión.	19/58	32.76%



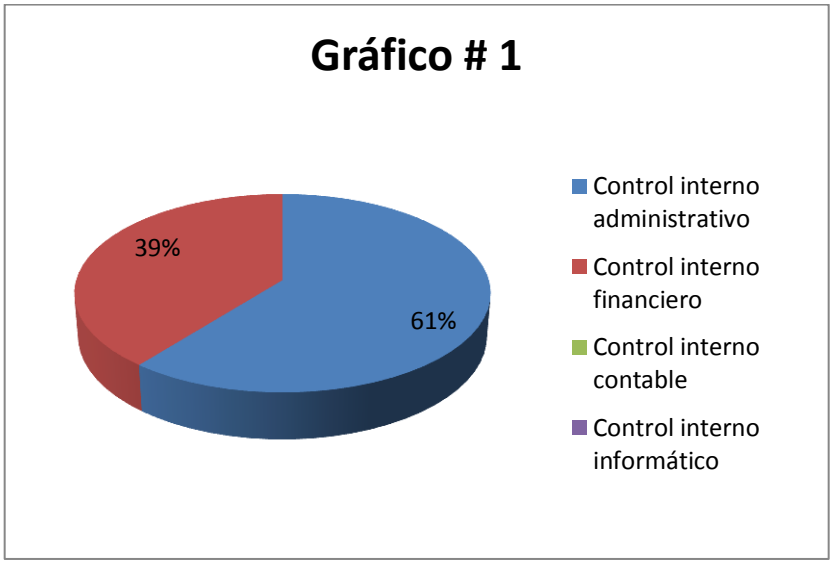
Análisis: Un total de 58 contadores públicos que representa el 59% de la muestra determinan que los altos costos de formación profesional son el motivo por el cual no cubren su formación en el área de tecnología de información; razón por la cual en la pregunta #9 solamente 15 entidades ofertan el servicio de control interno informático. Por otro lado el desconocimiento del tema así como la falta de aplicación dentro de la profesión son también factores que influyen dentro de su formación.

Tabulación y análisis de la información recopilada a las empresas distribuidoras de telefonía en El Salvador.

1. ¿Cuenta la entidad con el área de auditoría interna?

Objetivo: Establecer la importancia del área de la auditoría interna dentro de una entidad.

	FRECUENCIA	
RESPUESTA	ABSOLUTA	RELATIVA
SI	17	60.71%
NO	11	39.29%
TOTAL	28	100.00%



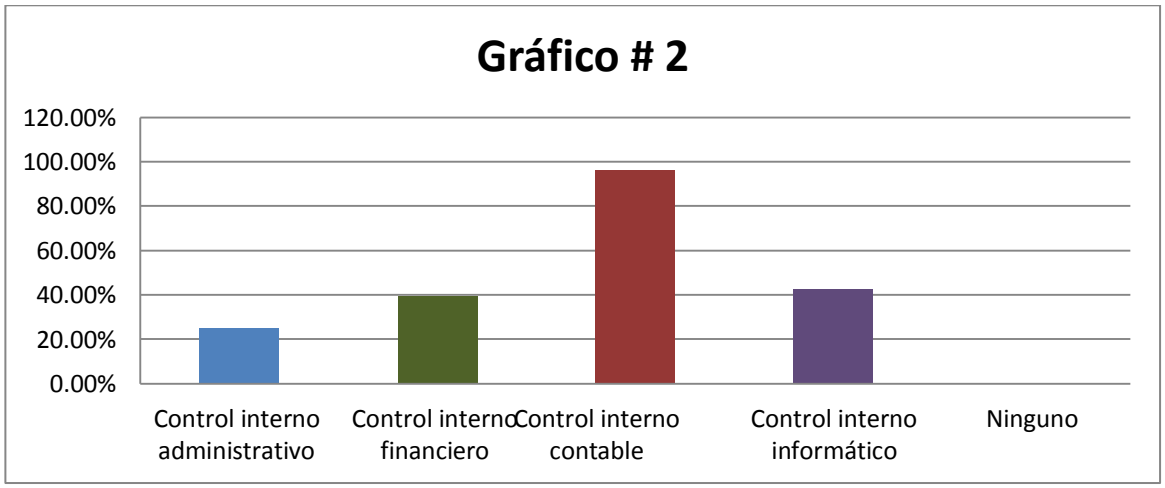
Análisis: Del 100% de los encuestados el 61% afirma contar con un área de auditoría interna; en este sentido se determina la importancia del área dentro de la estructura organizativa de las entidades, además de ser auditoría interna quien evalúa el control interno informático.

.

2. Del siguiente listado, seleccione el o los tipos de controles que implementa la entidad.

Objetivo: Conocer en qué áreas la entidad ha implementado controles internos

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Control interno administrativo	7/28	25.00%
B	Control interno financiero	11/28	39.29%
C	Control interno contable	27/28	96.43%
D	Control interno informático	12/28	42.86%
E	Ninguno	0/28	0.00%

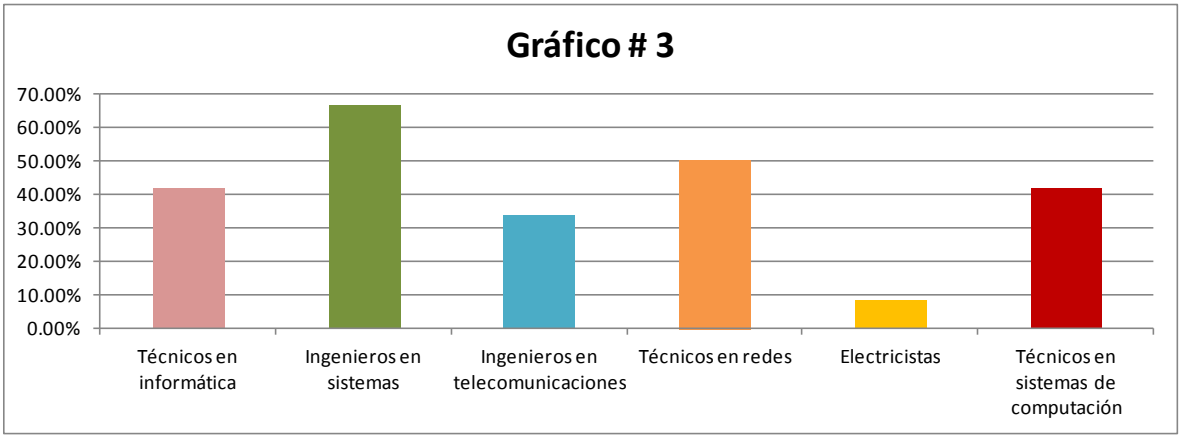


Análisis: El control interno contable es el tipo de control que las entidades implementan con mayor frecuencia con el 96%, sin embargo más de la mitad de las entidades encuestadas no poseen un control interno informático adaptado a sus necesidades y su enfoque principalmente se basa en la parte contable por lo que los controles están más orientados a este.

3. En caso de contar con control interno informático ¿Qué tipo de especialistas se requieren para el control interno de las TI? Si no cuenta con control interno informático pase a la siguiente pregunta.

Objetivo: Determinar el perfil del responsable del área de tecnología de información.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Técnicos en informática	5/12	41.67%
B	Ingenieros en sistemas	8/12	66.67%
C	Ingenieros en telecomunicaciones	4/12	33.33%
D	Técnicos en redes	6/12	50.00%
E	Electricistas	1/12	8.33%
F	Técnicos en sistemas de computación	5/12	41.67%

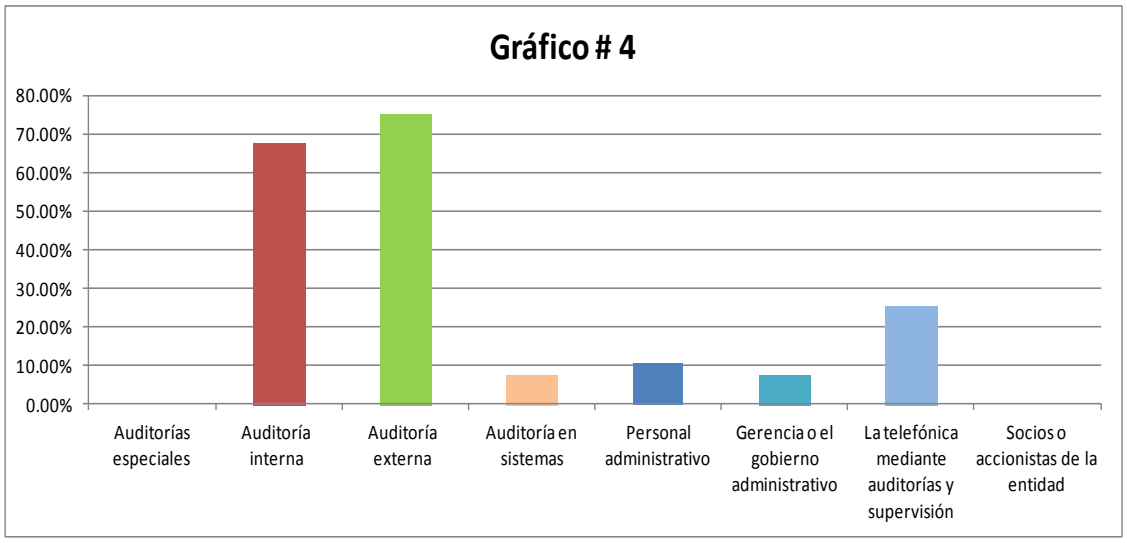


Análisis: Del total de las 12 entidades que representan el 43% que manifestaron poseer un control interno informático en relación con la pregunta #2, estas afirman utilizar un equipo multidisciplinario por el tipo de trabajo realizado.

4. ¿Quién realiza el trabajo de verificación del sistema de control interno que implementa la entidad?

Objetivo: Conocer en qué medida las entidades supervisan la protección de las tecnologías de información y el perfil de la persona que lo realiza.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Auditorías especiales	0/28	0.00%
B	Auditoría interna	19/28	67.86%
C	Auditoría externa	21/28	75.00%
D	Auditoría en sistemas	2/28	7.14%
E	Personal administrativo	3/28	10.71%
F	Gerencia o el gobierno administrativo	2/28	7.14%
G	La telefónica mediante auditorías y supervisión	7/28	25.00%
H	Socios o accionistas de la entidad	0/28	0.00%



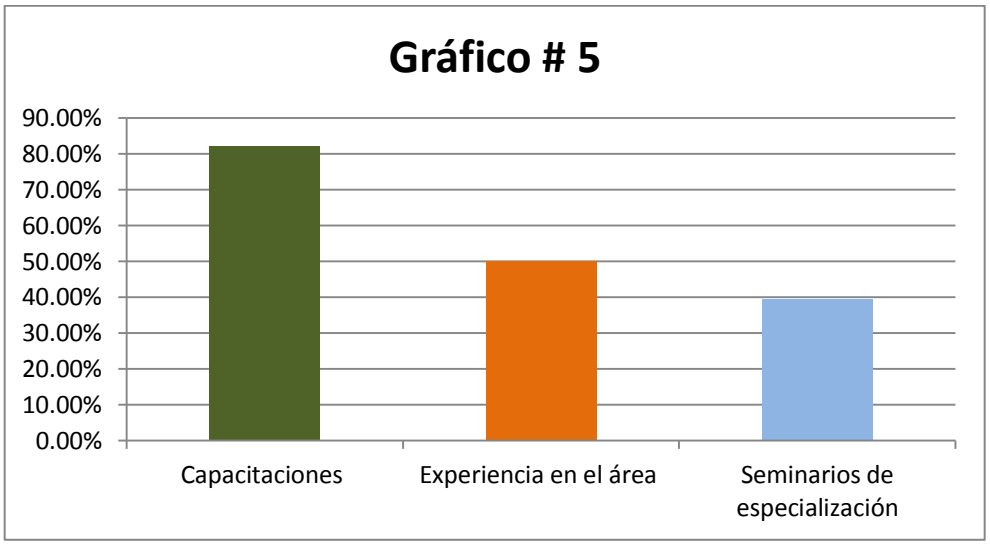
Análisis: Del 100% de los encuestados el 75% afirman que la verificación de los controles internos que implementan, están a cargo de la auditoría externa. Determinando que la

supervisión y protección de las tecnologías de información también la desarrolla la auditoría externa.

5. ¿Cómo se realiza la formación del capital humano para el área de tecnologías de información dentro de la entidad?

Objetivo: Identificar los requerimientos de las empresas al contratar personal.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Capacitaciones	23/28	82.14%
B	Experiencia en el área	14/28	50.00%
C	Seminarios de especialización	11/28	39.29%

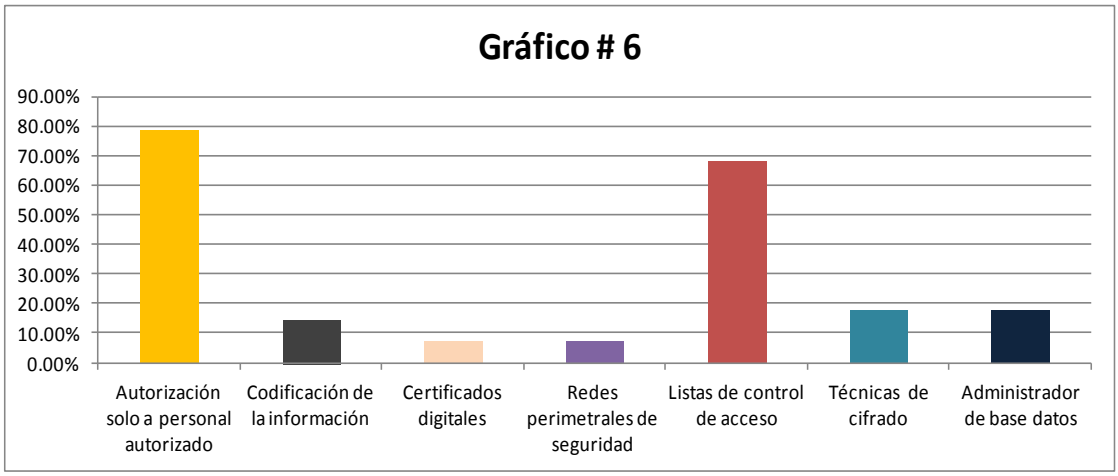


Análisis: Un total de 23 entidades que representan el 82% de la muestra determinan que las capacitaciones son las herramientas que implementan para desarrollar la parte del capital humano relacionado al área de informática. Es en este sentido que el Instituto Salvadoreño de Formación Profesional juega un papel importante dentro de la formación que pudiere recibir la parte del capital humano de las entidades.

6. Para preservar la confidencialidad de la información. ¿Qué controles implementa la entidad?

Objetivo: Verificar la eficiencia de los controles para la seguridad de la información en cuanto a la confidencialidad de la información.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Autorización solo a personal autorizado	22/28	78.57%
B	Codificación de la información	4/28	14.29%
C	Certificados digitales	2/28	7.14%
D	Redes perimetrales de seguridad	2/28	7.14%
E	Listas de control de acceso	19/28	67.86%
F	Técnicas de cifrado	5/28	17.86%
G	Administrador de base datos	5/28	17.86%

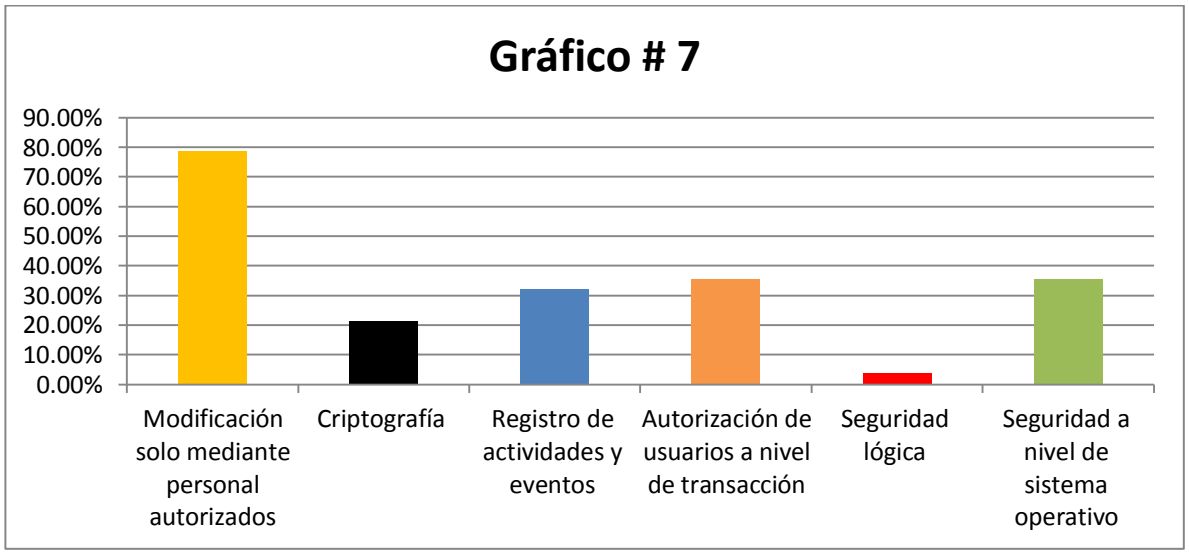


Análisis: Un total de 22 entidades que representan el 79% de la muestra, poseen como control interno, orientados a la preservación de la confidencialidad de la información, la autorización solo al personal autorizado; por lo tanto existen deficiencias en cuanto a los procesos de validación que utilizan para salvaguardar la integridad de la información.

7. Para salvaguardar la integridad de la información. ¿Qué controles implementa la entidad?

Objetivo: Verificar la eficiencia de los controles para la seguridad de la información en cuanto a la integridad de la información.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Modificación solo mediante personal autorizados	22/28	78.57%
B	Criptografía	6/28	21.43%
C	Registro de actividades y eventos	9/28	32.14%
D	Autorización de usuarios a nivel de transacción	10/28	35.71%
E	Seguridad lógica	1/28	3.57%
F	Seguridad a nivel de sistema operativo	10/28	35.71%

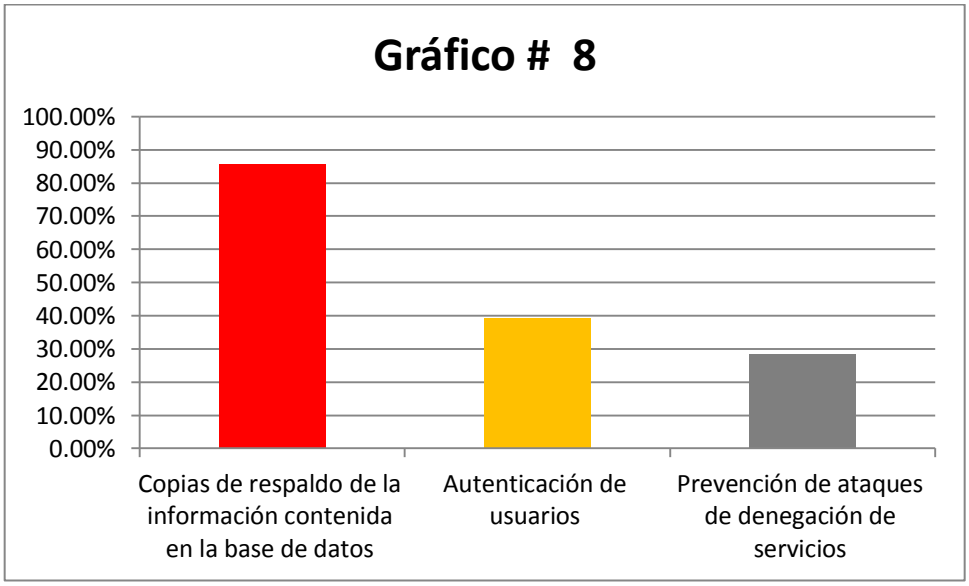


Análisis: Del 100% de los encuestados solamente el 25% afirman utilizar técnicas como el encriptado y medidas de seguridad lógica para salvaguardar la integridad de la información.Por lo que es evidente que los controles que utilizan son débiles.

8. Para mantener la disponibilidad de la información. ¿Qué controles implementa la entidad?

Objetivo: Verificar la eficiencia de los controles para la seguridad de la información en cuanto a la disponibilidad de la información.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Copias de respaldo de la información contenida en la base de datos	24/28	85.71%
B	Autenticación de usuarios	11/28	39.29%
C	Prevención de ataques de denegación de servicios	8/28	28.57%

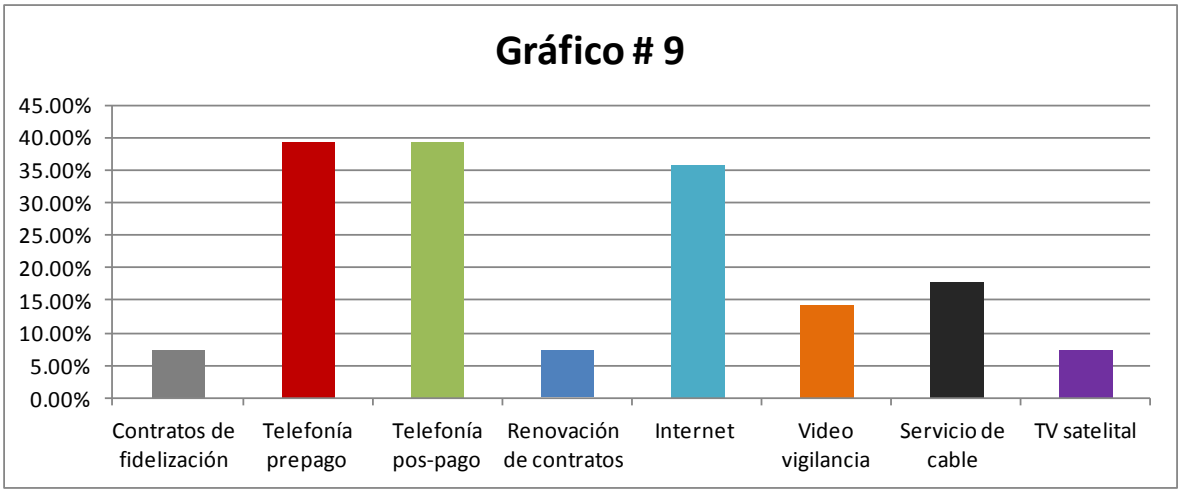


Análisis: Se indago sobre los controles implementados para mantener la disponibilidad de la información; en ese sentido en cuanto a la disponibilidad de la información el aspecto más importante es la prevención de ataques de denegación de servicios dado que el objetivo de este ataque es dejar inaccesibles un determinado recurso o uso de la información en un momento dado. A pesar de lo anterior solamente 8 de los encuestados afirman tener ese control.

9. ¿Cuáles son los servicios que mayor demanda tienen dentro de la entidad?

Objetivo: Conocer los servicios que la empresa ofrece para determinar la información que la entidad maneja.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Contratos de fidelización	2/28	7.14%
B	Telefonía prepago	11/28	39.29%
C	Telefonía pos-pago	11/28	39.29%
D	Renovación de contratos	2/28	7.14%
E	Internet	10/28	35.71%
F	Video vigilancia	4/28	14.29%
G	Servicio de cable	5/28	17.86%
H	TV satelital	2/28	7.14%

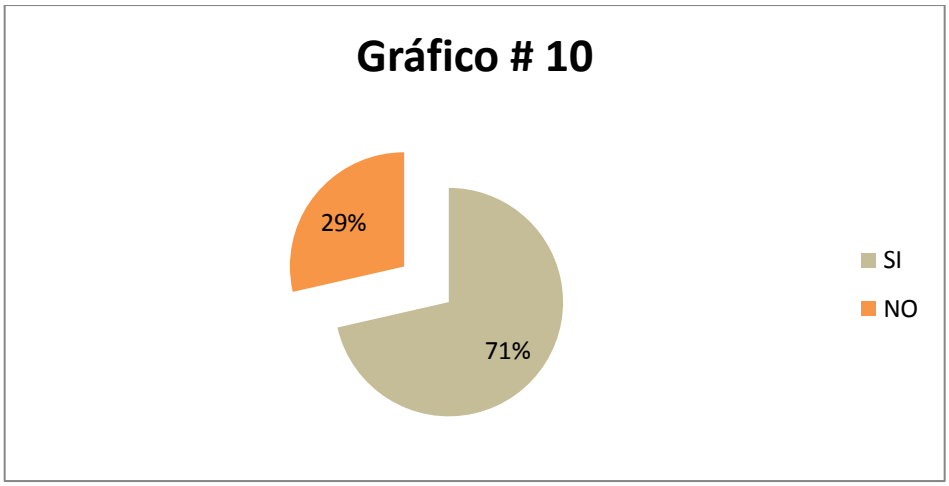


Análisis: Se indago sobre los servicios que poseen mayor demanda en el mercado de las Telefónicas; del 100% de los encuestados el 39% afirman que dichos servicios son la telefonía pre pago y post pago seguidamente de los servicios de internet; los cuales tienen como característica principal la protección de datos; lo que por su parte la ISO 27002 establece como seguridad a cubrir correspondiente a la integridad, confidencialidad y disponibilidad de la información.

10. ¿La entidad ha tenido conocimiento de incidentes de extracción o pérdida de información?

Objetivo: Determinar si en algún momento la entidad ha sufrido incidentes en el cual los datos han sido vulnerados.

	FRECUENCIA	
RESPUESTA	ABSOLUTA	RELATIVA
SI	20	71.43%
NO	8	28.57%
TOTAL	28	100.00%

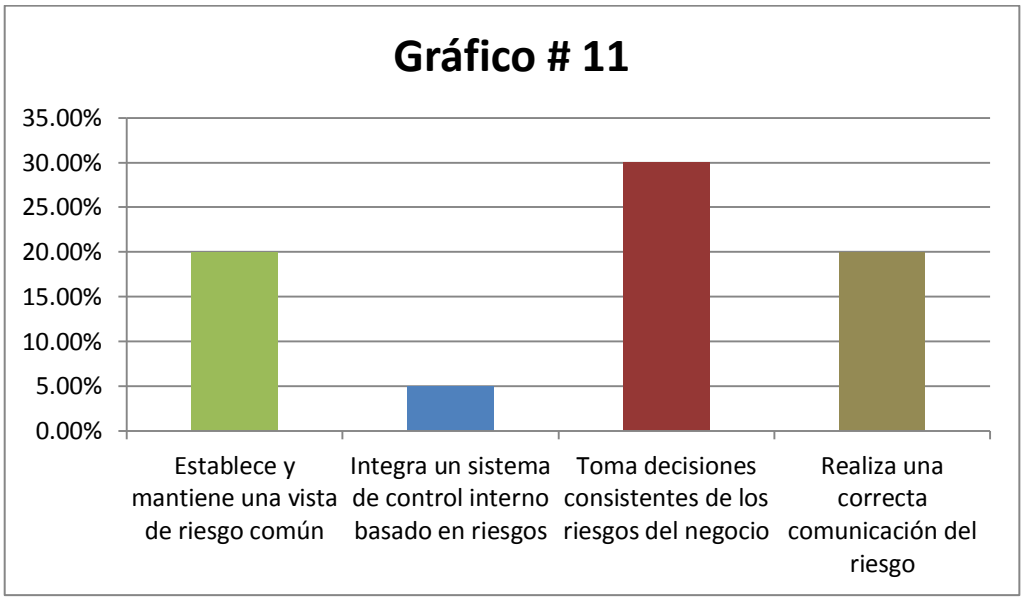


Análisis: Un total de 20 entidades que representan el 71% de la muestra manifiestan haber tenido conocimientos de incidentes, por lo que la confidencialidad se ha visto comprometida de acuerdo a los resultados ya que dicho porcentaje ha tenido conocimientos de extracción o perdida de datos.

11. ¿Cuál ha sido la respuesta por parte de la entidad hacia los incidentes de extracción o pérdida de datos?

Objetivo: Determinar la respuesta que la entidad ha tenido ante incidentes en área de tecnologías de información.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Establece y mantiene una vista de riesgo común	4/20	20%
B	Integra un sistema de control interno basado en riesgos	1/20	5%
C	Toma decisiones consistentes de los riesgos del negocio	6/20	30%
D	Realiza una correcta comunicación del riesgo	4/20	20%

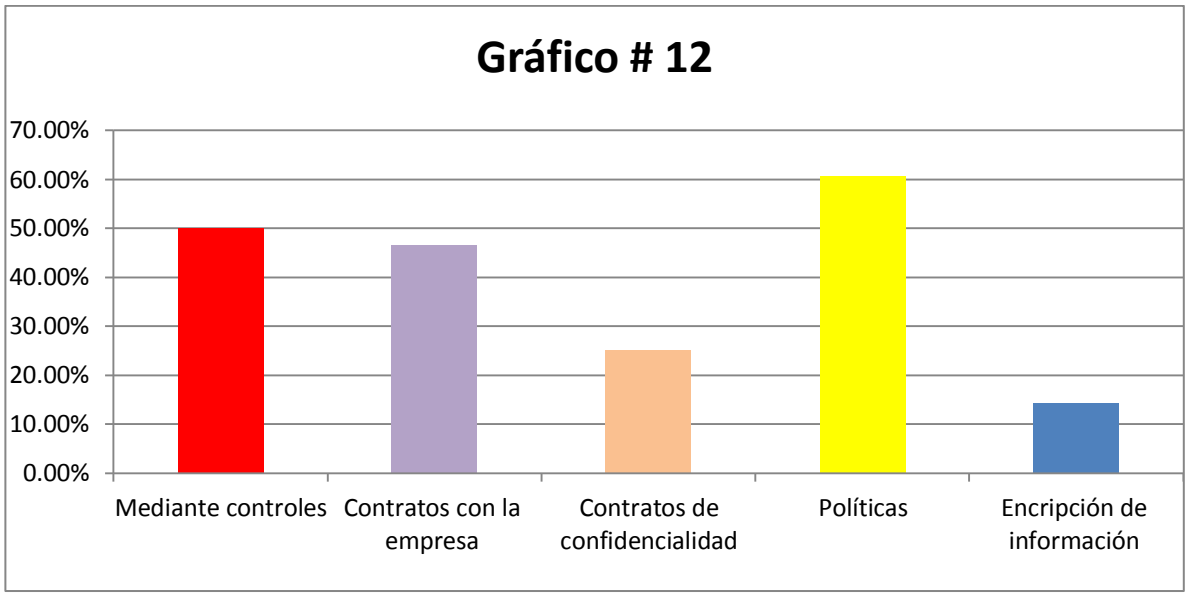


Análisis: En relación conla pregunta 10 donde 20 entidades afirmaron haber tenido conocimientos de incidentes el 30% de los encuestados afirman que la respuesta por parte de la entidad ha sido la toma de decisiones consistentes de los riesgos del negocio.

12. ¿Qué tipo de medidas se implementan para asegurar la protección de los datos de los usuarios y/o clientes?

Objetivos: Conocer de qué manera las empresas resguardan los datos de los clientes.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Mediante controles	14/28	50.00%
B	Contratos con la empresa	13/28	46.43%
C	Contratos de confidencialidad	7/28	25.00%
D	Políticas	17/28	60.71%
E	Encripción de información	4/28	14.29%

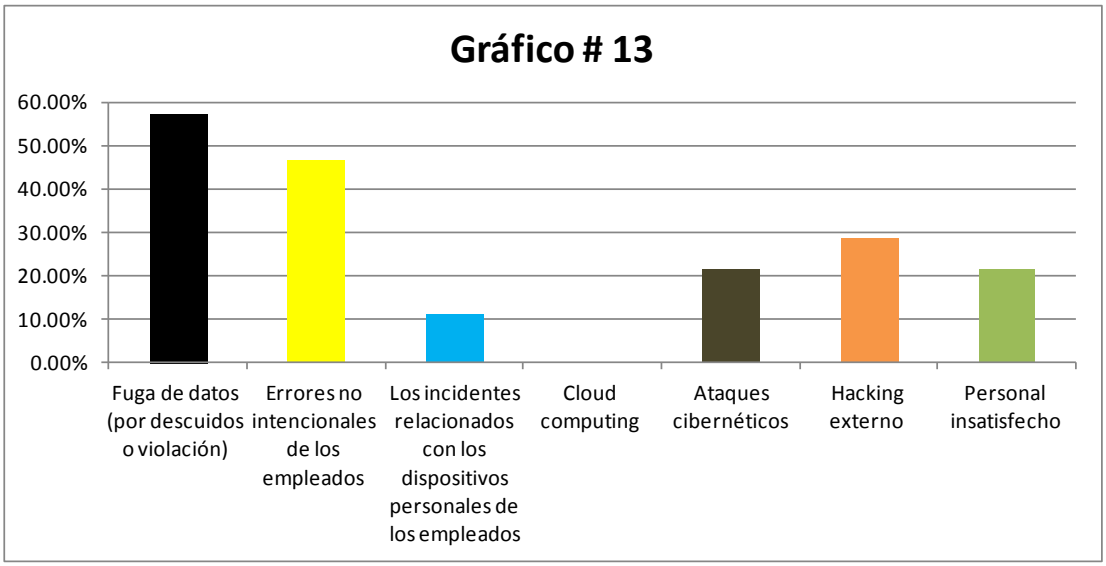


Análisis: Del total de 28 encuestados, los tipos de controles que implementa para asegurar la protección de datos, lo realiza mediante controles y políticas con un 50% y 61% respectivamente; a pesar de lo anterior estas políticas y controles no han impedido incidentes de pérdida o extracción de datos, tal como se muestran en los resultados de la pregunta #10.

13. Del siguiente listado seleccione las amenazas para la seguridad de la información que usted considere más comunes dentro de la entidad.

Objetivo: Determinar las amenazas a las que las empresas están expuestas con mayor frecuencia.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Fuga de datos (por descuidos o violación)	16/28	57.14%
B	Errores no intencionales de los empleados	13/28	46.43%
C	Los incidentes relacionados con los dispositivos personales de los empleados	3/28	10.71%
D	Cloud computing	0/28	0.00%
E	Ataques cibernéticos	6/28	21.43%
F	Hacking externo	8/28	28.57%
G	Personal insatisfecho	6/28	21.43%

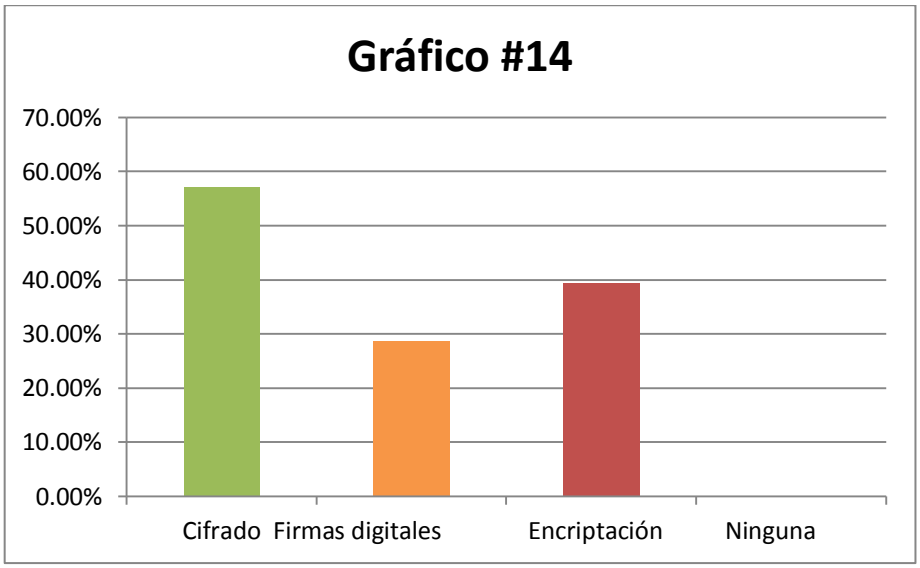


Análisis: Del total de encuestados el 57% manifestaron que las amenazas de la seguridad de la información y la fuga de datos ya sea por descuido o violación son las amenazas más comunes; lo anterior es debido a que estas entidades en su mayoría no poseen un control interno informático es por ello que los controles que poseen no son muy fuertes y suficientes para detectar que los tipos incidentes que más se reciben a diario son los ataques cibernéticos y el hacking externo.

14. ¿Qué medidas de seguridad se implementa al momento de compartir información relacionada a datos del cliente?

Objetivo Establecer los mecanismos de seguridad para la transmisión y recepción de la información.

		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	Cifrado	16/28	57.14%
B	Firmas digitales	8/28	28.57%
C	Encriptación	11/28	39.29%
D	Ninguna	0/28	0.00%



Análisis: Los encuestados opinaron que la medida de seguridad que se implementa al momento de compartir información lo realizan mediante y la Encripción con el 57% y el 39% respectivamente. Por lo que las entidades optan para salvaguardar la información dichas medidas. Sin embargo en la pregunta #7 la criptografía fue la opción que menos se implementaba para salvaguardar la información. De manera tal la alternativa que resultaría más segura para compartir la información seria la firma digital como tal.

15. ¿Por qué razón considera que las entidades no implementan un control interno?

Objetivo: Conocer las causas por la que la entidad no posee un control interno.

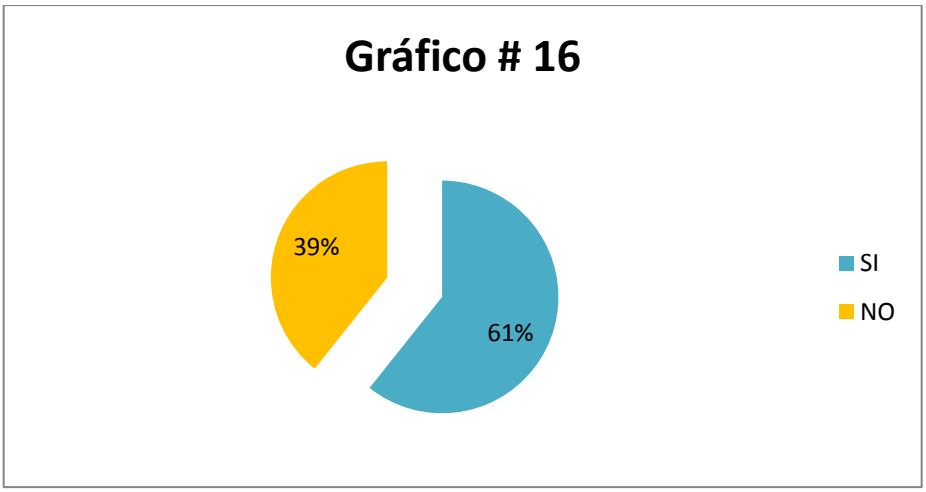
		FRECUENCIA	
	RESPUESTA	ABSOLUTA	RELATIVA
A	La empresa es considerada pequeña	12/28	42.86%
B	Altos costos	11/28	39.29%
C	No poseen los recursos necesarios para implementarlo	12/28	42.86%
D	No es necesario	0/28	0.00%

Análisis: Del total de encuestados consideran que el motivo por el cual las entidades no implementan un modelo de control interno es por ser considerada una entidad pequeña y por no poseer los recursos necesarios para poder implementar con 42.86%, en ese sentido las entidades llevan controles básicos pero no seguros o de fácil manipulación que no mantiene los datos de manera confiable, segura.

16. ¿Estaría interesado la administración en utilizar un modelo de control internos de tecnología de información para la protección, resguardo y aseguramiento de la información?

Objetivo: identificar si la entidad está dispuesta a administrar y conservar de manera adecuada los sistemas de información.

	FRECUENCIA	
RESPUESTA	ABSOLUTA	RELATIVA
SI	17	60.71%
NO	11	39.29%
TOTAL	28	100.00%



Análisis: A pesar que cerca del 40% no está interesado en implementar un modelo de control interno informático; los resultados de la encuesta muestran ciertas debilidades en los controles que aplican y es en este sentido que las entidades que si implementan un control interno estos controles no son seguros por lo que no pueden mantener los datos de manera fiable y segura.

Anexo N° IV

Reunión

Anexo N° VI Junta Directiva de 4G, S.A de C.V

ACTA No. 1

Siendo las 13.00 Hr, del día 15 de Abril de 2015, se reúne en las Oficinas Administrativas de la sociedad 4G, S.A de C.V

Los miembros de la Junta Directiva presentes son:

Nombre	**Condición (principal o Suplente)**
Ricardo Hernández	Prin._____ Supl._____
Carlos Alfredo Rosales	Prin._____ Supl._____
Carlos López Bernal	Prin._____ Supl._____
Betty Marlene Cruz	Prin._____ Supl._____
Héctor David Pineda	Prin._____ Supl._____

Verificado el quórum apto para deliberar y decidir, se decide de manera unánime por los asistentes, nombrar como presidente para esta reunión de Junta Directiva, al Sr. Carlos Alfredo Rosales y como secretario al Sr. Alfredo Rodríguez

Orden del día:

1. Lectura del acta de la reunión anterior

El secretario, el Sr. Wilfredo Rodríguez al acta anterior, la cual es aprobada por los miembros de la Junta Directiva.

2. Compromiso y responsabilidad de la gerencia

La Junta Directiva impartió su aprobación Compromiso de la gerencia en el cumplimiento de políticas sobre el manejo de la seguridad de información estableciendo sus objetivos, alcances generales y la importancia del mismo.

Puntos a tratar:

- Establecimiento de políticas por parte gerencia sobre el conocimiento al personal en cuanto al control interno y sus requerimientos en cuanto a la seguridad de la información de manera que sea relevante, accesible y entendible.

- Establecimiento de un marco gerencial para iniciar controlar e implementar para la seguridad de la información dentro de la organización

- Establecimiento de responsabilidades generales y específicas para el área de la seguridad de la información.

- Establecimiento de fechas para la verificación por parte de auditoria interna

- Verificación de documentación que fundamente los procedimientos, controles y políticas en cuanto a la seguridad de la información.

- Establecimiento de compromiso de confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información

La Junta Directiva autorizó al representante legal para efectuar las gestiones para los puntos tratados.

4. Lectura y Aprobación del Acta.
Habiéndose agotado los asuntos a tratar, el presidente de la reunión levantó la sesión siendo las 15 Hr

_____ _____

Presidente Secretario

Reunión
Junta Directiva de 4G, S.A de C.V
ACTA No. 2

Siendo las 13.00 Hr, del día 15 de Abril de 2015, se reúne en las Oficinas Administrativas de la sociedad 4G, S.A de C.V
Los miembros de la Junta Directiva presentes son:

Nombre	**Condición (principal o Suplente)**
Ricardo Hernández	Prin._____ Supl._____
Carlos Alfredo Rosales	Prin._____ Supl._____
Carlos López Bernal	Prin._____ Supl._____
Betty Marlene Cruz	Prin._____ Supl._____
Héctor David Pineda	Prin._____ Supl._____

Verificado el quórum apto para deliberar y decidir, se decide de manera unánime por los asistentes, nombrar como presidente para esta reunión de Junta Directiva, al Sr. Carlos Alfredo Rosales y como secretario al Sr. Alfredo Rodríguez

Orden del día:
1. Lectura del acta de la reunión anterior
El secretario, el Sr. Wilfredo Rodríguez al acta anterior, la cual es aprobada por los miembros de la Junta Directiva.
2. Continuación de acta Nª 1
Que la junta Directiva, debe procurar la existencia o gestión de un sistema de control interno efectivo que contribuya a:

- Se logre la disponibilidad, integridad y confiabilidad en las operaciones de 4G, S.A de C.V.
- Protección de los recursos, buscando una adecuada administración.
- Se vele por el cumplimiento de la legislación y la regulación, políticas, normas y procedimientos internos.
- Evaluación del funcionamiento del sistema de control interno.
- Establecer como prioridad la seguridad y protección de la información y de los recursos informáticos de la empresa.
- Implementación de métodos técnicas y procedimientos necesarios para contribuir al eficiente desarrollo de las funciones del control interno, para satisfacer los requerimientos de sistemas en la empresa.
- Establecer revisiones generales del control interno informático.

La Junta Directiva autorizó al representante legal para efectuar las gestiones para los puntos tratados.

4. Lectura y Aprobación del Acta.

Habiéndose agotado los asuntos a tratar, el presidente de la reunión levantó la sesión siendo las 15 Hr

_____ _____

Presidente Secretario

Reunión
Junta Directiva de 4G, S.A de C.V
ACTA No. 3

Siendo las 13.00 Hr, del día 25 de Abril de 2015, se reúne en las Oficinas Administrativas de la sociedad 4G, S.A de C.V
Los miembros de la Junta Directiva presentes son:

Nombre	**Condición (principal o Suplente)**
Ricardo Hernández	Prin._____ Supl._____
Carlos Alfredo Rosales	Prin._____ Supl._____
Carlos López Bernal	Prin._____ Supl._____
Betty Marlene Cruz	Prin._____ Supl._____
Héctor David Pineda	Prin._____ Supl._____

Verificado el quórum apto para deliberar y decidir, se decide de manera unánime por los asistentes, nombrar como presidente para esta reunión de Junta Directiva, al Sr. Carlos Alfredo Rosales y como secretario al Sr. Alfredo Rodríguez

Orden del día:
1. Lectura del acta de la reunión anterior
El secretario, el Sr. Wilfredo Rodríguez al acta anterior, la cual es aprobada por los miembros de la Junta Directiva.
2. Contexto empresarial interno y externo
Presentación de la estructura organizativa de la entidad

- Misión y visión de la entidad
- Metas y objetivos establecidos
- Políticas y estrategias de la entidad.
- Detalle de las regulaciones legales aplicables a la entidad.
- Participación de mercado
- Presentación de las áreas de control interno
- Listado del personal encargado de las áreas de control interno
- Recopilación de datos de los empleados en cuanto a sus capacidades, educación y conocimiento adquirido.
- Estudio de los principales competidores
- Memoria de labores

La Junta Directiva autorizó al representante legal para efectuar las gestiones para los puntos tratados.

4. Lectura y Aprobación del Acta.
Habiéndose agotado los asuntos a tratar, el presidente de la reunión levantó la sesión siendo las 15 Hr

_____ _____

Presidente Secretario

Reunión
Junta Directiva de 4G, S.A de C.V
ACTA No. 4

Siendo las 13.00 Hr, del día 25 de Abril de 2015, se reúne en las Oficinas Administrativas de la sociedad 4G, S.A de C.V
Los miembros de la Junta Directiva presentes son:

Nombre	**Condición (principal o Suplente)**
Ricardo Hernández	Prin._____ Supl._____
Carlos Alfredo Rosales	Prin._____ Supl._____
Carlos López Bernal	Prin._____ Supl._____
Betty Marlene Cruz	Prin._____ Supl._____
Héctor David Pineda	Prin._____ Supl._____

Verificado el quórum apto para deliberar y decidir, se decide de manera unánime por los asistentes, nombrar como presidente para esta reunión de Junta Directiva, al Sr. Carlos Alfredo Rosales y como secretario al Sr. Alfredo Rodríguez

Orden del día:
1. Lectura del acta de la reunión anterior
El secretario, el Sr. Wilfredo Rodríguez al acta anterior, la cual es aprobada por los miembros de la Junta Directiva.
2. Establecimiento de políticas y objetivos de control interno

- Definir una política de control interno.
- Implementar controles adecuados para el aseguramiento de los riesgos se reduzcan a un nivel aceptado.
- Diseñar controles de acuerdos a necesidades específicas o requerimientos especiales.
- Implementación de políticas de seguridad de la información.
- Fomentar controles de protección data y privacidad de información
- Establecer objetivos del control interno informático

La Junta Directiva autorizó al representante legal para efectuar las gestiones para los puntos tratados.
4. Lectura y Aprobación del Acta.
Habiéndose agotado los asuntos a tratar, el presidente de la reunión levantó la sesión siendo las 15 Hr

_____ _____
Presidente Secretario

Reunión
Junta Directiva de 4G, S.A de C.V
ACTA No. 5

Siendo las 13.00 Hr, del día 15 de Agosto de 2015, se reúne en las Oficinas Administrativas de la sociedad 4G, S.A de C.V
Los miembros de la Junta Directiva presentes son:

Nombre	**Condición (principal o Suplente)**
Ricardo Hernández	Prin._____ Supl._____
Carlos Alfredo Rosales	Prin._____ Supl._____
Carlos López Bernal	Prin._____ Supl._____
Betty Marlene Cruz	Prin._____ Supl._____
Héctor David Pineda	Prin._____ Supl._____

Verificado el quórum apto para deliberar y decidir, se decide de manera unánime por los asistentes, nombrar como presidente para esta reunión de Junta Directiva, al Sr. Carlos Alfredo Rosales y como secretario al Sr. Alfredo Rodríguez

Orden del día:

1. Lectura del acta de la reunión anterior

El secretario, el Sr. Wilfredo Rodríguez al acta anterior, la cual es aprobada por los miembros de la Junta Directiva.

2. Composición del comité de riesgo:

Estará conformada por tres miembros de la junta directiva para el periodo de un año, designación que se hará por la junta directiva, una vez nombrada por la Asamblea General de accionista.

- Establecimiento, periodo y nombramiento de comité de seguridad de información.
- Aprobación de lineamentos, políticas, procedimientos y metodología aplicados a la seguridad de la información.
- Proponer políticas generales sobre los riesgos en tecnología de información.
- Proponer niveles aceptables de riesgo en tecnología de información
- Determinación y revisión de marcos para la gestión de tecnología de la información
- Compromiso de la gerencia en la formulación de estrategias y políticas para la gestión del riesgo en tecnología de la información.

La Junta Directiva autorizó al representante legal para efectuar las gestiones para los puntos tratados.

4. Lectura y Aprobación del Acta.

Habiéndose agotado los asuntos a tratar, el presidente de la reunión levantó la sesión siendo las 15 Hr

_____ _____
Presidente Secretario

Reunión
Junta Directiva de 4G, S.A de C.V
ACTA No. 6

Siendo las 13.00 Hr, del día 30 de Agosto de 2015, se reúne en las Oficinas Administrativas de la sociedad 4G, S.A de C.V
Los miembros de la Junta Directiva presentes son:

Nombre	**Condición (principal o Suplente)**
Ricardo Hernández	Prin._____ Supl._____
Carlos Alfredo Rosales	Prin._____ Supl._____
Carlos López Bernal	Prin._____ Supl._____
Betty Marlene Cruz	Prin._____ Supl._____
Héctor David Pineda	Prin._____ Supl._____

Verificado el quórum apto para deliberar y decidir, se decide de manera unánime por los asistentes, nombrar como presidente para esta reunión de Junta Directiva, al Sr. Carlos Alfredo Rosales y como secretario al Sr. Alfredo Rodríguez

Orden del día:

1. Lectura del acta de la reunión anterior

El secretario, el Sr. Wilfredo Rodríguez al acta anterior, la cual es aprobada por los miembros de la Junta Directiva.

2. Líneas de comunicación:

Comunicación de controles sobre gestión de tecnología de información.

- Jerarquía de comunicación
- Implementación de controles para asegurar las responsabilidades asignada al personal.
- Implementación de contratos de confidencialidad con el fin de evitar divulgación de información y aseguramiento de la misma.
- Implementación de controles para el procesamiento, resguardo y aseguramiento de la información

La Junta Directiva autorizó al representante legal para efectuar las gestiones para los puntos tratados.

4. Lectura y Aprobación del Acta.

Habiéndose agotado los asuntos a tratar, el presidente de la reunión levantó la sesión siendo las 15 Hr

_____ _____
Presidente Secretario

Reunión
Junta Directiva de 4G, S.A de C.V
ACTA No. 7

Siendo las 13.00 Hr, del día 30 de Agosto de 2015, se reúne en las Oficinas Administrativas de la sociedad 4G, S.A de C.V
Los miembros de la Junta Directiva presentes son:

Nombre	**Condición (principal o Suplente)**
Ricardo Hernández	Prin._____ Supl._____
Carlos Alfredo Rosales	Prin._____ Supl._____
Carlos López Bernal	Prin._____ Supl._____
Betty Marlene Cruz	Prin._____ Supl._____
Héctor David Pineda	Prin._____ Supl._____

Verificado el quórum apto para deliberar y decidir, se decide de manera unánime por los asistentes, nombrar como presidente para esta reunión de Junta Directiva, al Sr. Carlos Alfredo Rosales y como secretario al Sr. Alfredo Rodríguez

Orden del día:

1. Lectura del acta de la reunión anterior

El secretario, el Sr. Wilfredo Rodríguez al acta anterior, la cual es aprobada por los miembros de la Junta Directiva.

2. Proporcionar recursos:

- Participación de la gerencia en el resguardo de la seguridad de la información, a través de una dirección clara, esto a través del cumplimiento de sus responsabilidades.
- Proporcionar recursos necesarios y adecuados para el aseguramiento de la información.
- Implementación de planes y programas enfocados a la conciencia de seguridad de la información.
- Coordinación e implementación de controles destinados a la seguridad de la información en toda la organización.
- Promover capacitaciones, educación, conocimiento de la seguridad de la información de manera efectiva a través de toda la organización.

La Junta Directiva autorizó al representante legal para efectuar las gestiones para los puntos tratados.

4. Lectura y Aprobación del Acta.

Habiéndose agotado los asuntos a tratar, el presidente de la reunión levantó la sesión siendo las 15 Hr

_____ _____
Presidente Secretario

Reunión
Junta Directiva de 4G, S.A de C.V
ACTA No. 8

Siendo las 13.00 Hr, del día 15 de septiembre de 2015, se reúne en las Oficinas Administrativas de la sociedad 4G, S.A de C.V
Los miembros de la Junta Directiva presentes son:

Nombre	**Condición (principal o Suplente)**
Ricardo Hernández	Prin._____ Supl._____
Carlos Alfredo Rosales	Prin._____ Supl._____
Carlos López Bernal	Prin._____ Supl._____
Betty Marlene Cruz	Prin._____ Supl._____
Héctor David Pineda	Prin._____ Supl._____

Verificado el quórum apto para deliberar y decidir, se decide de manera unánime por los asistentes, nombrar como presidente para esta reunión de Junta Directiva, al Sr. Carlos Alfredo Rosales y como secretario al Sr. Alfredo Rodríguez

Orden del día:

1. Lectura del acta de la reunión anterior

El secretario, el Sr. Wilfredo Rodríguez al acta anterior, la cual es aprobada por los miembros de la Junta Directiva.

2. Criterio para la aceptación del riesgo:

- Listado de activos esenciales
- Identificación de los riesgos asociados a los activos
- Determinación de análisis del riesgo
- Evaluación del riesgo
- Establecer el tratamiento del riesgo

La Junta Directiva autorizó al representante legal para efectuar las gestiones para los puntos tratados.

4. Lectura y Aprobación del Acta.

Habiéndose agotado los asuntos a tratar, el presidente de la reunión levantó la sesión siendo las 15 Hr

_____ _____
Presidente Secretario

Política de seguridad de la información **Anexo N° VIII**

Compromiso de la gerencia

La gerencia es la garante del compromiso de mantener segura, confiable e integra la información a fin de cumplir no solo como los marcos legales que rigen la seguridad de la información; sino ser garante del cumplimiento fiel de acuerdo a estándares de calidad y marcos de información integrados.

Enfoque para el manejo de la seguridad de la información

El enfoque respecto a la implementación de la presente política de seguridad de la información está de acuerdo al proceso Planear, Hacer, Chequear y Verificar para manejar la seguridad de la información

La seguridad de la información consiste en preservar de acuerdo a las características cualitativas de confidencialidad, integridad y disponibilidad de la información; en ese sentido se pueden involucrar propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

1. **Objetivos**

- Proteger, administrar y preservar eficazmente la información de la empresa 4G, S.A de C.V junto con las tecnologías implementadas para el procesamiento de la misma, ante amenazas, riesgos y vulnerabilidades de carácter interno o externo, con el propósito de asegurar el cumplimiento de las características cualitativas de confidencialidad, integridad y disponibilidad de la información.

- Mantener la Política de Seguridad de la Información actualizada y vigente así como monitorear el cumplimiento de la misma, dentro del marco determinado por los riesgos determinados para asegurar su estabilidad y nivel de confianza.

- Definir la metodología de la entidad para la correcta valoración, análisis, evaluación y tratamiento de los riesgos de seguridad de la información así como el impacto del

mismo, con el fin de garantizar la continuidad e integridad de los sistemas de información.

2. **Alcances**

La presente política es de aplicación en el conjunto de dependencias que componen la entidad, los recursos, procesos internos o externos relacionados a la empresa a través de contratos o acuerdos con terceros, contratistas y a todo el personal de la entidad de acuerdo a la dependencia en la que se encuentre y el nivel de labores que desempeñe

3. **Visión de la gerencia**

Con la presente política se busca implementar controles y procedimientos a fin de disminuir los riesgos a los que la entidad esta expuestos a diario partiendo de la premisa de la información valiosa que se procesa a diario, así poder cumplir tanto requerimientos legales como de estándares de calidad a fin de salvaguardar la integridad de la información.

4. **Marco de referencia**

El marco de referencia para establecer los controles es el Marco integrado de Cobit en su versión numero 5 conjuntamente alineado con los estándares ISO e ITIL.

5. **Responsabilidades generales de la gestión del control interno**

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la entidad

La junta directiva aprueba esta Política y son responsables de la autorización de sus modificaciones.

El **comité de seguridad de la información** es el responsable de revisar y proponer la aprobación y modificación de la presente política de seguridad de la información así como de establecer las funciones generales y la estructura y mejora del control interno informático de la empresa.

El **presidente propietario** de junta es el responsable de coordinar lo referente a las acciones que impondrá el comité de seguridad de la información.

Los **encargados del uso y manipulación de los activos** son los responsables del equipo, del mantenimiento y actualización del mismo, así como de documentar la clasificación del activo, el nivel de acceso que tienen a la información dependiendo de sus funciones y competencias. Son los responsables de mantener íntegro y disponible el activo de información.

El **encargado de los recursos humanos** tiene la función de comunicar al personal de las obligaciones respecto de la presente política, así como de todos los estándares, procesos procedimientos y controles a implementar dentro del control interno informático. De igual forma es el responsable de comunicar cambios producto de actualizaciones.

Encargado de inventarios le corresponde determinar el inventario de activos y recursos tecnológicos

La **Administración** será la encargada de planificar la ejecución del control interno informático conjuntamente con el área de **auditoria interna**; será su responsabilidad informar sobre el cumplimiento de las especificaciones de medidas de seguridad de la información establecidas en la presente política.

6. Principales políticas, estándares y requerimientos de conformidad.

6.1 Identificación, clasificación y valoración de los activos

Cada departamento debe elaborar y mantener un inventario actualizado. En este sentido todos los activos deben estar inventariados y contar con un propietario nombrado.

Los usuarios de los activos deben identificar y cumplir la responsabilidad por el mantenimiento y actualización de los activos.

6.2 Recursos humanos

Todo el personal de la entidad 4G, S.A de C.V sea cual sea su condición laboral debe tener asociado un perfil de uso respecto a la información, incluyendo el software y el hardware asociado.

El encargado de los recursos humanos debe definir los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros

Los empleados bajo la dependencia de la entidad, o terceros debe firmar un acuerdo sobre roles y responsabilidades con relación a la seguridad.

El encargado de recursos humanos es quien define las responsabilidades de realizar la terminación del empleo o el cambio de empleo.

6.3 Seguridad física y del entorno

Acceso

Se debe tener un acceso controlado a los cuartos de los servidores principales y será el encargado del área quien tendrá los controles y registro de accesos a dichas áreas. Los perímetros de seguridad para proteger las áreas que contengan la información y los medios de procesamiento de la información las delimitara la administración.

Seguridad en equipos

Los servidores que contengan información deben ser mantenidos en un ambiente seguro y contar como mínimo con lo siguiente:

- Controles de acceso y seguridad física
- Detección de incendios
- Controles de humedad y temperatura
- Bajo riesgo de inundación
- Sistemas electrónicos regulados y UPS

Las estaciones de trabajo deben estar correctamente asegurada y operadas por el personal de la entidad el cual debe estar capacitado acerca de la presente política y de las responsabilidades personales en el uso y administración la información de la seguridad.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el Comité de Seguridad en la Información.

6.4 Administración de comunicación y operaciones

Reporte e investigación de incidentes de seguridad

El personal de la entidad debe reportar con diligencia las violaciones de seguridad a través de los las jefaturas de cada departamento.

La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.

6.5 Control de acceso

El acceso a los recursos de tecnologías de información debe estar restringido según el perfil de los usuarios por la administración.

Gestión de acceso del usuario

El acceso a la información restringida debe estar controlado. Es recomendable el uso de sistemas automatizados de autenticación que manejen credenciales o formas digitales.

El control de las contraseñas de red y uso de equipos es responsabilidad de cada departamento a cargo según las clasificaciones realizadas por la administración.

Las claves de administrador de los sistemas deben ser conservadas por la dirección

Se debe gestionar los intentos de acceso a la red no autorizados; así como controlar el acceso a los servicios de redes internas y externas.

6.6 Cumplimiento

Todo uso y seguimiento de uso a los recursos deben estar de acuerdo a las normas y estatutos internos en concordancia con lo siguiente:

- La Constitución de la Republica de El Salvador
- Ley de Telecomunicaciones
- Ley del Acceso a la Información
- Código de Comercio
- Ley de la Firma Electrónica.
- ISO 27000 y su serie: Sistema de Gestión de la seguridad de la Información
- Cobit en su versión 5
- Biblioteca de la infraestructura de tecnología de información (ITIL)

Anexo N° VI

Enunciado de aplicabilidad
Entidad: 4G, S.A de C.V

Dominios	Objetivo de control	Controles	SI / NO	Razón de la selección	Objetivo de control o control implementado actualmente.	Justificación de exclusión
1.Política de seguridad	1.1 Política de seguridad de la información	1.1.1 Documento de la política y seguridad de la información	SI	Proporciona una directriz respecto a la seguridad de la información.	✓	
		1.1.2 Revisión de la política de la seguridad de la información	SI	Controlar el cumplimiento de la política.		
2. Organización de la seguridad de la información	2.1 Organización interna	2.1.1 compromiso de la gerencia con la seguridad de la información.	SI	Para evidenciar y determinar el compromiso de la gerencia con la organización para la implementación del control interno.	✓	
		2.1.2 coordinación de la seguridad de la información	SI			
		2.1.3 asignación de la responsabilidades de la seguridad de la información.	SI		✓	
		2.1.4 Autorización de procesos para facilidades procesadoras de información	NO			
		2.1.5 Contacto con las	SI		✓	

		autoridades.				
		2.1.6 Contacto con grupos de interés especial	SI			
		2.1.7 Revisión independiente de la seguridad de la información.	NO			
	2.2 Grupo o personas externas.	2.2.1 Identificación de los riesgos relacionados con grupos externos	SI	Determinar los riesgos relacionados con terceros para el tratamiento de la información.		
		2.2.2 Tratamiento de la seguridad cuando se lidia con clientes.	SI			
		2.2.3 Tratamiento de la seguridad en acuerdos con terceros.	SI		✓	
3. Gestión de activos.	3.1 Responsabilidad por los activos	*3.1.1 Inventario de los activos*	SI	Dado la importancia de conocer y clasificar los activos mantenidos por la entidad	✓	
		3.1.2 Propiedad de los activos	SI			
		3.1.3 Uso aceptable de los activos	NO			
	3.2 Clasificación de la información.	*3.2.1 Lineamientos de clasificación.*	SI	Para controlar los detalles de la información que posee la entidad.	✓	
		3.2.2 Etiquetado y manejo de la información.	SI			

4. Seguridad de recursos humanos.	4.1 Antes del empleo.	*4.1.1 Roles y responsabilidades.*	SI	Para evitar incidentes de seguridad con la preselección del personal.		
		4.1.2 Investigación de antecedentes.	NO		✓	
		4.1.3 Términos y condiciones del empleo	SI			
	4.2 Durante el empleo.	*4.2.1 Responsabilidades de la gerencia.*	SI	Para propiciar las responsabilidades, capacitaciones y roles en el ambiente de trabajo de la entidad.		
		4.2.2 Conocimiento, educación y capacitación en seguridad de la información	SI		✓	
		4.2.3 Proceso disciplinario	SI			
	4.3 Terminación o cambio de empleo	*4.3.1 Responsabilidades de terminación.*	NO	Para evitar incidentes de seguridad una vez terminado su contrato.	✓	
		4.3.2 Devolución de los activos	SI		✓	
		4.3.3 Retiro de los derechos de acceso.	SI			
5. Seguridad física y del entorno	*5.1 áreas seguras*	*5.1.1 Perímetro de seguridad física*	SI	Para evitar incidentes relacionados al entorno y seguridad física dentro de la entidad.		
		5.1.2 Controles de ingreso físico	SI			
		5.1.3 Asegurar las oficinas, habitaciones y	SI			

		medios.				
		5.1.4 Protección contra amenazas externas e internas.	NO	Para propiciar un ambiente seguro libre de amenazas	✓	
		5.1.5 Trabajo en áreas aseguradas.	SI			
		5.1.6 Áreas de acceso público, entrega y carga.	NO	Para minimizar los incidentes de seguridad en esta área.		
	5.2 Equipo de seguridad.	*5.2.1 Ubicación y protección de activos.*	SI	Con el fin de proporcionar una seguridad en el equipo tanto interno como externo.	✓	
		5.2.2 Servicios públicos de soporte.	SI			
		5.2.3 Seguridad del cableado.	SI		✓	
		5.2.4 Mantenimiento de equipo.	NO			
		5.2.5 Seguridad del equipo fuera del local.	NO			
		5.2.6 Seguridad de la eliminación o re-uso del equipo.	NO			
		5.2.7 Retiro de propiedad.	NO			
6. Gestión de las comunicaciones y operaciones	*6.1 Procedimientos y responsabilidades*	*6.1.1 Procedimientos de operación documentados.*	SI	Para determinar procedimientos, responsabilid	✓	

	operacionales .			ades y medios de cambio.		
		6.1.2 Gestión del cambio.	SI			
		6.1.3 Segregación de los deberes.	SI			
		6.1.4 Separación de los medios de desarrollo, prueba y operación.	NO			
	6.2 Gestión de la entrega de servicios de terceros.	*6.2.1 Entrega del servicio.*	SI	Con el fin de determinar los controles respecto a la entrega de servicios de terceros.		
		6.2.2 Monitoreo y revisión de los servicios de terceros.	SI			
		6.2.3 Manejo de cambios en los servicios de terceros.	NO			
	6.3 Planeación y aceptación del sistema.	*6.3.1 Gestión de la capacidad.*	SI	Para determinar la gestión con respecto del sistema		
		6.3.2 Aceptación del sistema.	SI			
	6.4 Protección contra código malicioso y móvil.	*6.4.1 Controles contra códigos maliciosos.*	SI	Para evitar infecciones que alteren su información.		
		6.4.5 controles contra códigos móviles.	SI	Para evitar incidentes de seguridad.		
	6.5 Respaldo o Back –Up	*Back-Up*	SI	Garantizar la disponibilidad de la		

				información.		
	6.6 Gestión de seguridad de la red	*6.6.1 Controles de red.*	SI	Están orientados para mitigar accesos no autorizados.		
		6.6.2 Seguridad de los servicios de red.	NO			
	6.7 Gestión de los medios.	*6.7.1 Gestión de medios removibles.*	SI	Para determinar el uso correcto de medios, el manejo y documentación de la información.		
		6.7.2 Procedimiento para el manejo de la información.	NO			
		6.7.3 Seguridad de la documentación del sistema.	SI			
	6.8 Intercambio de información.	*6.8.1 Políticas y procedimientos de intercambio de información.*	SI	Para establecer los procedimientos relacionados al intercambio de la información a través de medios físicos y electrónicos		
		6.8.2 Acuerdos de intercambio.	SI			
		6.8.3 medios físicos en tránsito.	NO			
		6.8.4 Mensajes electrónicos.	SI			
		6.8.5 Sistema de información comercial.	NO			
	6.9 Servicios de comercio electrónico	*6.9.1Comercio electrónico.*	SI	Para evitar incidentes relacionados al comercio electrónico.		
		6.9.2Transacciones en-línea.	NO			
		6.9.3Información públicamente	SI			

		disponible				
	6.10 Monitoreo	*6.10.1Registro de auditoría.*	SI	Para establecer las áreas necesaria a monitorear.		
		6.10.2 Uso de sistema de monitoreo.	SI			
		6.10.3 Protección de registro de información.	SI			
		6.10.4 Registro del administrador y operador.	SI			
		6.10.5 Registro de fallas.	SI			
		6.10.6 Sincronización de relojes.	NO			
7. Control de acceso	*7.1 Requerimiento del negocio para el control de acceso.*	*7.1.1 Política de control de acceso.*	SI	Para determinar políticas de control de acceso mediante la asignación de registros, claves de usuarios.		
	7.2 Gestión de acceso del usuario	*7.2.1 Registro del usuario.*	SI			
		7.2.2 Gestión de privilegios.	SI			
		7.2.3 Gestión de clave secretas de los usuarios.	SI			
		7.2.4 Revisión de los derechos de acceso del usuario.	NO			
	7.3 Responsabilidad del	*7.3.1 Uso de claves secretas.*	SI	Para designar las responsabilid		

	usuario.			ades del personal en cuanto a los sistemas de información.		
		7.3.2 Equipo del usuario desatendido.	NO			
		7.3.3 Política de escritorio y pantallas limpias.	SI			
	7.4 Control de acceso a la red	*7.4.1 Política sobre el uso de los servicios de red.*	SI	Para determinar procedimientos en cuanto al control de acceso, usuarios y protección para la conexión de la red.	✓	
		7.4.2 Autenticación del usuario para las conexiones externas.	SI			
		7.4.3 Identificación del equipo en las redes.	NO			
		7.4.4 Protección del puerto de diagnóstico y configuración remoto.	SI		✓	
		7.4.5 Segregación en redes.	NO			
		7.4.6 Control de conexión a la red.	SI			
		7.4.7 Control de routing de la red.	NO			
	7.5 Control del acceso al sistema operativo	*7.5.1 Procedimiento para un registro seguro.*	SI	Para evitar riesgos relacionados al sistema operativo como:		
		7.5.2 Identificación y	SI			

		autenticación de usuario.		accesos no autorizados, y limitación en tiempo de conexión.		
		7.5.3 Sistema de gestión de claves secretas.	SI		✓	
		7.5.4 Uso de las utilidades del sistema.	NO			
		7.5.5 Cierre de una sesión por inactividad.	NO			
		7.5.6 Limitación del tiempo de conexión.	SI			
	7.6 Control de acceso a la aplicación y la información.	*7.6.1 Restricción del acceso a la información.*	SI	Con el fin de resguardar la integridad de la información y asegurar la disponibilidad.		
		7.6.2 Aislar el sistema confidencial.	NO			
	7.7 Computación y tele-trabajo móvil	*7.7.1 Computación y comunicación móviles.*	SI	Para determinar los controles aplicables a las comunicaciones y terminales. Con el objeto de determinar aplicaciones para asegurar que los datos sean correctos y apropiados.		
		7.7.2Teletrabajo	NO			
8. Adquisición, desarrollo y mantenimiento de los sistemas de información.	*8.1 Requerimiento de seguridad de los sistemas de información.*	*8.1.1 Análisis y especificación de los requerimientos de seguridad.*	SI		✓	
	8.2 Procesamiento correcto en las aplicaciones.	*8.2.1 Validación de input data.*	NO			
		8.2.2 Control del	SI	Para minimizar la		

		procesamiento interno.		corrupción de la información		
		8.2.3 Integridad del mensaje.	NO			
		8.2.4 Validación de output-data.	NO	Con el fin de asegurar el almacenamiento correcto y apropiado de la información.		
	8.3 Controles criptográficos.	*8.3.1 Política sobre el uso de controles criptográfico*	SI	Para delimitar el acceso a la información.		
		8.3.2 Gestión de claves.	NO			
	8.4seguridad de los archivos del sistema.	*8.4.1 Control del software operacional.*	SI	Para determinar los procedimientos encaminados a la protección de los archivos del sistema		
		8.4.2 Protección de la data del sistema.	SI			
		8.4.3 Control de acceso al código fuente del programa.	NO			
	8.5 seguridad en los procesos de desarrollo y soporte.	*8.5.1 Procedimiento del control de cambio.*	SI	Para evitar acceso a configuraciones para los procesos de desarrollo de soporte en el sistema.		
		8.5.2 Revisión técnica de la aplicación después de cambios en el sistema	NO			
		8.5.3 Restricciones	NO			Debido a la restricción

		sobre cambios en los paquetes de software.				en cuanto al acceso a las modificaciones de los sistemas
		8.5.4 Filtración de información.	SI			
		8.5.5 Desarrollo de software abastecido externamente.	NO			Debido a que está delimitada la adquisición de software por parte de la telefónica.
	8.6 Gestión de la vulnerabilidad técnica.	*8.6.1 Control de las vulnerabilidades técnicas.*	SI	Desarrollo de medidas para documentar las vulnerabilidades.	✓	
9. Gestión de un incidente en la seguridad de la información.	*9.1 Reporte de los eventos y debilidades de la seguridad de la información.*	*9.1.1 Reporte de eventos en la seguridad de la información.*	SI	Documentar incidentes y responsabilidades ante eventos relacionados a la seguridad de la información		
		9.1.2 Reporte de debilidades en la seguridad.	SI			
	9.2 Gestión de los incidentes y mejoras en la seguridad de la información.	*9.2.1 Responsabilidades y procedimientos.*	SI		✓	
		9.2.2 Aprendizaje de	SI			

		los incidentes en la seguridad de la información				
		9.2.3 Recolección de evidencia.	SI			
10. Gestión de la continuidad del negocio	*10.1 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio.*	*10.1.1 Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio.*	SI	Determinar los aspectos relacionados a la gestión de la continuidad del negocio e integrar planes de continuidad y evaluación del riesgo para la entidad.	✓	
		10.1.2 Continuidad del negocio y evaluación del riesgo.	SI			
		10.1.3 Desarrollar e implementar planes de continuidad incluyendo la seguridad de la información.	SI			
		10.1.4 Marco referencial de la planeación de la continuidad del negocio.	SI		✓	
		10.1.5 Pruebas, mantenimiento y re-evaluación de los planes de continuidad del negocio.	SI			

11.Cumplimiento	*11.1 Cumplimiento de los requerimientos legales*	*11.1.1 Identificación de la legislación aplicable.*	SI	Para determinar los procedimientos necesarios respecto del cumplimiento de la legislación, propiedad intelectual y la protección de la información regulando el acceso a través de controles criptográficos.	✓	
		11.1.2 Derecho de propiedad intelectual	SI		✓	
		11.1.3 Protección de registros organizacionales.	SI		✓	
		11.1.4 Protección de la data y privacidad de la información personal.	SI		✓	
		11.1.5 Prevención del mal uso de los medios de procesamiento de la información	SI			
		11.1.6 Regulación de controles criptográficos.	SI		✓	
	11.2 Cumplimiento de las políticas y estándares de seguridad y cumplimiento técnico.	*11.2.1 Cumplimiento con las políticas y estándares de seguridad.*	SI	Para gestionar el cumplimiento y verificación de políticas y medidas de seguridad	✓	
		11.2.2 Chequeo del cumplimiento técnico.	SI			

	11.3 Consideración de auditoría de los sistemas de información.	*11.3.1 Controles de auditoría de los sistemas de información.*	SI	Para determinar el cumplimiento del rol de auditoria dentro del control interno informático		
		11.3.2 Protección de las herramientas de auditoría de los sistemas de información.	SI			

Asunto: Enunciado de aplicabilidad

Responsable: Gerencia administrativa

F: _____
Firma de la gerencia

Plan de tratamiento de riesgos

Anexo N° VII

Objetivo: Definir un plan de tratamiento aplicable a la entidad 4G, SA de C.V
Responsable: Gerencia administrativa

Riesgo	Estrategia	Descripción de la estrategia aplicar	Responsable	Plazo para implementar
Saturación en el núcleo de comunicaciones	Reducir	Revisión mensual	Administración y Mantenimiento preventivo.	26/10/2015
Saturación de carga en el enlace	Reducir	Monitoreo	Mantenimiento Preventivo	26/10/2015
Corte de energía	-	-	-	-
Inundaciones, terremotos , Incendios, interrupción del servicio de internet, entre otros	-	-	-	-
Back ups desactualizados	Reducir	Semanal	Personal a cargo.	26/10/2015
Accesos no restringidos	Mitigar	Cuando sea necesario	Personal a cargo.	26/10/2015
Deficiencias en las medidas de seguridad para el tratamiento de la información	Reducir	Mensualmente	Administración	26/10/2015
Procesamiento incorrecto de datos	Reducir	Cuando sea necesario	Administración	26/10/2015
Infecciones con virus, troyanos u otro malware	Reducir	Cuando sea necesario	Personal a cargo.	26/10/2015
Procedimientos para el tratamiento de	Reducir	Cuando sea necesario	Administración	26/10/2015

la información no valida				
Ataques externos	Prevenir	Cuando sea necesario	Administración	226/10/2015
Personal insatisfecho	Reducir	Cuando sea necesario	Administración	26/10/2015
Falla en el control de las licencias	Evitar	Cuando sea necesario	Administración	26/10/2015
Caídas y cuelgues del sistema	Mitigar	Cuando sea necesario	Mantenimiento preventivo.	26/10/2015
Ataques internos	Reducir	Cuando sea necesario	Administración	26/10/2015
Fallas en los conectores eléctricos	Reducir	Cuando sea necesario	Mantenimiento preventivo.	26/10/2015
Medios extraíbles	Reducir	Cuando sea necesario	Mantenimiento preventivo	26/10/2015
Mantenimiento	Aumentar	Cuando sea necesario	Mantenimiento preventivo y administración	26/10/2015
Hacker, Cracker	Mitigar	Cuando sea necesario	Mantenimiento preventivo.	26/10/2015
Incumplimiento	Reducir	Cuando sea necesario	Administración	26/10/2015

.

ANEXO N° VIII

MANUAL DE CONTROL INTERNO BASADO EN RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN

4G, S.A DE C.V

ÍNDICE

Hoja de autorización 2

Introducción 3

Objetivos 4

Objetivo General 4

Objetivos específicos 2

Alcance 4

TÉRMINOS Y DEFINICIONES 5

ESTRUCTURA ORGANIZATIVA PARA LA PREVENCIÓN DE RIESGOS RELACIONADOS LAS TECNOLOGÍAS DE INFORMACIÓN 6

DESCRIPCIÓN DE FUNCIONES 6

POLÍTICAS 8

Política de seguridad de la información 8

Políticas específicas 6

1. Organización de la seguridad de la información 8
2. Gestión de activo 9
3. Seguridad ligada a los recursos humanos 10
4. Seguridad física y del entorno 12
5. Gestión de comunicaciones y operaciones 13
6. Control de acceso 17
7. Adquisición, desarrollo y mantenimiento de los sistemas de información 19
8. Gestión de incidentes en la seguridad de la información 21
9. Gestión de la continuidad del negocio 22

10.Cumplimiento 23

SANCIONES26

APENDICES27

Hoja de autorización

Preparado por:

Luis Balmore Pineda Portal — Firma:

Cargo: Coordinador de seguridad de la información — Fecha: 31-10-2015

Revisado por:

Miguel Ángel NajarroArdón. — Firma:

Cargo: Gerente Administrativo. — Fecha: 06-11-2015

Aprobado por:

Nombre: Jorge Alejandro Zelaya. — Firma:

Cargo: Presidente de Junta directiva — Fecha:16-11-2015

INTRODUCCIÓN

4G, SA. DE CV identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que se establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada. Este documento describe las políticas de seguridad de la información. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, la norma ISO 27002. Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos. La seguridad de la información es una prioridad y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el establecimiento de cada una de estas políticas.

OBJETIVOS

Objetivo General

- Proporcionar las herramientas necesarias para salvaguardar la información y los medios para garantizar la integridad, disponibilidad y confidencialidad de la información.

Objetivos específicos

- Determinar un modelo de gestión de riesgo de seguridad de la información para su identificación, valoración y tratamiento.
- Asistir en el cumplimiento de normas, estándares y leyes en materia de seguridad de la información.

ALCANCE

El control interno informático es aplicable a todos los procesos comprendidos dentro de la entidad y en determinado caso fuera de la misma, a los activos de la empresa y a las tecnologías de la información.

El cumplimiento del presente manual es de carácter obligatorio para la gerencia, administración empleados permanentes de la entidad, empleados temporales y terceros relacionados a la empresa.

TÉRMINOS Y DEFINICIONES

CRIPTOGRAFÍA: Es el arte o ciencia de descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que solo puedan ser leídos por las personas que van dirigidos.

METRICA: Una entidad cuantificable que permite la medida de la consecución de una meta de proceso. Las métricas deben ser específicas, medibles, accionables, relevantes, oportunas (SMART). Una guía completa para una métrica define la unidad a usar, la frecuencia de medida, el valor objetivo ideal (si resulta apropiado) y también el procedimiento para la realización de la medida y el procedimiento para la interpretación de la evaluación.

INCIDENTE DE SEGURIDAD: Uno o una serie de eventos de seguridad de la información no deseados o inesperados que posee una probabilidad significativa de comprometer operaciones de la entidad amenazando la seguridad de la información.

PASARELA (Gateway): O puerta de enlace es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a el de un acceso hacia una red exterior se podría decir que un Gateway es un router que conecta dos redes.

ESTRUCTURA ORGANIZATIVA PARA LA PREVENCIÓN DE RIESGOS RELACIONADOS LAS TECNOLOGÍAS DE INFORMACIÓN.

DESCRIPCIÓN DE FUNCIONES

Comité de riesgo

Entre sus funciones principales se establecen las siguientes:

- Es el responsable de revisar y proponer la aprobación y modificación de la política de seguridad de la información
- Establecer las funciones generales y la estructura y mejora del control interno informático de la empresa
- Velar por el cumplimiento de las políticas de seguridad de la información
- Aprobar directrices respecto a las metodologías implementadas en la gestión del riesgo

Junta directiva

Tiene las siguientes funciones principales:

- Aprobar el manual de procedimientos y actualizaciones
- Pronunciarse respecto al establecimiento de las responsabilidades de la gerencia
- Pronunciarse sobre el establecimiento de los objetivos y planes relacionados a l control interno informático
- Establecer las líneas de comunicación respecto al cumplimiento de la política de seguridad de la información
- Aprobar metodologías de identificación, análisis y evaluación del control interno informático
- Implementar los recursos necesarios para que la entidad pueda implementar, procedimientos y controles

Gerencia administrativa

Dentro de sus funciones se establecen las siguientes:

- planificar la ejecución del control interno informático conjuntamente con el área de auditoria interna
- informar sobre el cumplimiento de las especificaciones de medidas de seguridad de la información establecidas en las políticas
- Segregar funciones
- Otorgar accesos a la información
- Monitorear el cumplimiento de las políticas de seguridad de la información
- Establecer estrategias del tratamiento del riesgo para reducirlo en niveles aceptables

Encargado de recursos humanos

- Responsable de la gestión del riesgo relacionado al factor humano
- Responsable de implementar controles respecto a la contratación y despido del personal
- Responsable de la gestión del personal insatisfecho dentro de la entidad
- Encargado de la promoción de capacitaciones y actualización de información relacionada al factor humano

Encargado de activos

- Responsable de uso y manipulación del activo
- Autorización de accesos
- Notificación de incidentes con activos
- Comunicar las gestiones de uso y goce del equipo a la gerencia administrativa
- Documentar el equipo en uso, el propietario y el tiempo de uso.

Departamento de TI y mantenimiento

- Identificar y definir los medios tecnológicos apropiados para el desarrollo de procedimientos orientados a disminuir los riesgos a los que están expuestos

- Propiciar una estructura interna adecuada para el correcto funcionamiento del área de tecnologías de información
- Adecuar el ambiente físico a los equipos
- Propiciar una adecuada seguridad lógica en la infraestructura de los sistemas

POLÍTICAS

Política de seguridad de la información

Estipulada en el Anexo N° X

Auditoria interna

- Revisar la fiabilidad de la información financiera
- Revisar el cumplimiento de las políticas de seguridad
- Mantener actualizado los procedimientos de control interno en cada departamento de la entidad
- Mantener una revisión constante de los equipo
- Documentar mejoras y actualizaciones al control interno informático
- Monitorear las operaciones del control interno informático

Políticas específicas

1. **Organización de la seguridad de la información**

   Se encarga del resguardo y uso de los recursos y funcionamiento de los equipos tecnológicos del área de tecnologías de información, además de asegurar y mantener de manera íntegra la información de los usuarios.

   a. Compromiso de la gerencia con la seguridad de la información.
      La gerencia debe establecer compromisos para establecer los objetivos que la entidad debe seguir para el cumplimiento de los requerimientos.

b. Coordinación de la seguridad de la información.

La seguridad de la información debe involucrar la colaboración de los administradores y determinar la metodología que se utilizaran para la seguridad y resguardo de la información.

c. Asignación de las responsabilidades de la seguridad de la información

Deberá crearse un documento con las responsabilidades del manejo de la información y establecer de manera clara las responsabilidades y niveles de autorización, además de identificar y revisar los requerimientos de confidencialidad.

d. Contacto de las autoridades

Se deberá tener una línea de comunicación con los altos niveles gerenciales para aquellas decisiones consideradas de relevancia e importancia para las actividades y puesta en marcha de la entidad.

2. Gestión de activos

La responsabilidad de la gestión, que incluye desde la adquisición, instalación, mantenimiento y el eficiente manejo deberá estar a cargo de la administración, lo cual deberá registrar cada gestión que se efectué en los activos.

a. Inventario de los activos

Se deberá establecer que los activos estén debidamente registrados en el sistema y que esté debidamente codificado según clasificación.

b. Propiedad de los activos

Los activos relacionados con los medios de procesamiento de la información deben estar a cargo de la responsabilidad de la entidad.

c. Lineamientos de clasificación

La entidad debe asegurar la protección adecuada de la información dependiendo de: la necesidad, prioridades niveles de protecciónde la información manejada; incluyendo además la clasificación de los requerimiento legales y su valor considerando para ello:

- Integridad
- Disponibilidad
- Confidencialidad

.

d. Etiquetado y manejo de la información

La entidad deberá optar por conjunto de procedimientos considerando la clasificación que se haya optado por aplicar.

Se deberá mantener en formatos físicos y electrónicos las siguientes actividades:

- Copia
- Registro de los datos almacenados
- Registro de transferencias ya sea por correo, fax, entre otros

3. Seguridad ligada a los recursos humanos

El área de recursos humanos debe realizar un conjunto de procedimientos al momento de la contratación de empleados.

a. Antes del empleo.

Selección, roles y responsabilidades, término y condiciones de empleo.

Recursos humanos debe seguir los siguientes procesos de selección.

- Documentos personales
- Grado de conocimiento y experiencia del área aplicar
- Verificación de antecedentes de los empleados de acuerdo a leyes y regulaciones aplicables.
- Documentar mediante contrato los roles y responsabilidades, así como también los términos y condiciones de contratación que estarán a cargo del nuevo empleado.
- Contratos de confidencialidad

b. Gestión de responsabilidades, capacitaciones, educación en seguridad de la información y proceso disciplinario

La entidad debe establecer las obligaciones de los empleados y las obligaciones de la entidad ante los empleados para el manejo adecuado de la información

Se debe capacitar a los empleados, contratistas y terceros en cuanto a educación y capacitación en el uso y manejo del equipo para el procesamiento de la información.

Se debe documentar un proceso formal disciplinario cuando existan deficiencias en la seguridad de la información.

c. Terminación o cambio de empleo

El área de recursos humanos en conjunto con el responsable del área de TI deben cerciorarse que al término de o cambio de empleo se realice de manera organizada, realizando lo siguiente:

- Devolución del equipo asignado
- Evaluar si los equipos han sido actualizados y verificado en periodos regulares
- Eliminación de los derechos de accesos.
- Seguimiento del historial de acceso de salida de información.

4. Seguridad física y del entorno

Todos los equipos informáticos deben estar destinados a la prevención y detección, cumpliendo con los requerimientos de seguridad como los son inspecciones al área física en el que los equipos se encuentran ubicados dentro de la instalaciones de la entidad y a la verificación de controles de acceso a dichas instalaciones mediante el registro de entradas y salidas del personal.

a. Medidas de seguridad física y acceso físico

La entidad debe evitar el acceso no autorizado a las instalaciones y a la información de la organización mediante los siguientes procesos:

- Controles de entrada y salida
- Utilización de tarjetas de identificación tanto para empleados como para visitantes, identificadas para tal efecto.
- Inspecciones periódicas de seguridad física de instalaciones.

b. Ubicación y protección del equipo

La entidad debe asignar y aplicar medidas de seguridad para proteger contra incendios, inundaciones, terremotos entre otras formas de desastres naturales o humanos, además de evitar la pérdida, daño o robo de los activos o interrupción de las actividades.

- El equipo debe ubicarse y protegerse para minimizar la materialización de amenazas del entorno.
- Se debe proteger los equipos en casos de fallas o anomalías eléctricas en los equipos soportes.
- Monitorear en periodos cortos los equipos para garantizar la disponibilidad e integridad.

c. Políticas y procedimientos para personal contratado y mantenimiento de la infraestructura.

   Se debe establecer procesos para la contratación e incorporación para nuevos elementos de la entidad.

   Mantenimiento adecuado de la infraestructura

d. Protección de las tecnologías de información

   Se debe llevar un registro del software instalado. El cual el registro debe contener:

   - Fecha de instalación
   - Licencia
   - Fecha de actualizaciones
   - Registro de Mantenimiento
   - Back-ups

5. Gestión de comunicaciones y operaciones

La administración de 4G, S.A de C.V debe asegurar que la información sea correcta y segura por lo que se debe establecer responsabilidades, además de procedimientos para la gestión y operación de todos los recursos, también documentar procedimientos y directrices de la seguridad de la información.

a. Procedimientos de operaciones documentados

   La entidad debe asegurar mediante procedimientos que las operaciones se realicen de manera correcta y segura los recursos de tratamiento de información, deberá establecer instrucciones apropiadas de operación y de procedimientos para dar respuesta a incidencias.

b. Gestión de cambio

La entidad deberá llevar un registro de los cambios que realice en los sistemas y en los recursos de tratamiento de la información especificando los cambios realizados.

Además de realizar evaluaciones previas para no arriesgar la seguridad de los mismos.

c. Segregación de deberes

Se debe segregar las tareas y las áreas responsables, a manera de evitar o minimizar los riesgos de oportunidad de modificaciones no autorizados o no intencionados por parte del personal o personas ajenas a la entidad, así como también al mal manejo de los activos de la organización.

d. Entrega del servicio

La entidad debe verificar que los acuerdos del servicio se monitoreen con el fin de dar cumplimiento de ellos y en caso de efectuarse cambios gestionarlos, con el fin de que se cumplan los requisitos acordados.

e. Gestión de capacidad

El responsable efectuara el monitoreo de las necesidades de las capacidades de los sistemas de información y estar preparados para sucesos futuros, con el objetivo de garantizar el procesamiento y almacenamiento adecuados.

- La entidad debe evaluar proyecciones de la capacidad de reducir riesgos fallas del sistema.

- La entidad debe establecer y documentar los requisitos operativos de los nuevos sistemas.

f. Aceptación de sistemas

Antes de la aceptación del sistema, la entidad debe desarrollar pruebas para determinar que el sistema es eficiente y eficaz para la entidad.

g. Controles sobre software maliciosos y código móvil

La entidad debe proteger la integridad del software, por lo que se debe efectuar ciertas precauciones para prevenir códigos maliciosos. Por lo que considere lo siguiente:

- Descargas no autorizadas
- No abrir correos de remitentes desconocidos
- Solo usar medios de almacenamiento propiedad de la entidad
- Evitar abrir paginas emergentes
- Prohibición de navegar en internet para fines ajenos a la entidad
- Configuración del código móvil

h. Respaldo o Back-up

La administración debe realizar copias de respaldo de la información que maneja de forma regular.

i. Gestión de seguridad de la Red

La entidad establecerá mecanismos de control para proveer la disponibilidad de las redes, considerando la seguridad que protejan la integridad y la confidencialidad de la información como las siguientes:

- Redes segmentadas por dominios
- Grupos de servicios
- Grupos de usuarios
- Ubicación geográfica

j. Gestión de medios

Gestión de medios removibles

El responsable del área de TI implementara procedimientos para la administración de los medios, como USB, discos, cintas entre otros que haga uso la entidad

k. Seguridad de la documentación del sistema.

La entidad puede contener información sensible en los sistemas, por lo que para su protección es indispensable restricciones al acceso de la documentación por lo que para el accesos a ellos se debe realizar mediante lo aprobación de autorización de acceder a ella.

l. Intercambio de información

La entidad debe desarrollar procedimientos para la transferencia o intercambio de la información por lo que se debe considerar:

- El manejo de las responsabilidades
- Procedimientos para notificar
- Procedimientos para asegurar el rastreo
- Acuerdos de depósitos
- Obligaciones en incidentes de seguridad
- Uso del sistema de etiquetado

m. Mensajes electrónicos

La entidad debe establecer una protección de la información involucrada en el mensaje electrónico respecto a los accesos no autorizados, la correcta dirección y transporte del mensaje la confiabilidad y disponibilidad y los niveles de autenticación mediante

- Técnicas de cifrado (Alfanuméricas)

- Token
- Técnicas de encriptado (llaves públicas o privadas)

n. Monitoreo

La entidad debe realizar chequeos con el fin de detectar actividades de procesamiento de información no autorizadas.

- Debe monitorear los sistemas y registrar los eventos
- El registro de fallas debe ayudar a garantizar que esas fallas no se repetirán
- Registrar y documentar las actividades del administrador u operador.
- Registrar las fallas del sistema y tomar decisiones

6. Control de acceso

La entidad debe establecer el acceso a los recursos de tecnologías de información con el fin de restringir según el perfil de los usuarios por la administración. Los procedimientos deberían cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas servicios de información

a. Política de control de acceso

La entidad debe establecer y documentar la política de control de accesos a la base de datos.

b. Gestión de acceso del usuario

- Para la gestión de privilegios la entidad debe implementar procedimientos para el registro y remoción para revocar el acceso de los sistemas, así como el control de privilegios
- Gestión de claves de usuarios, se deben asignar claves que sean a nivel de usuarios, considerando la identificación de usuarios.

c. Responsabilidades del usuario

- Requerir buenas prácticas de seguridad para mantener la confidencialidad, mediante claves complejas mínimo 15 caracteres.
- Cuando el usuario no utilice su equipo, configurar con un tiempo de 5 segundos para que el equipo se bloquee y no esté vulnerable a amenazas de extracciones de información.

d. Control de acceso a la red

Se debe establecer que los usuarios deben tener accesos a red únicamente para lo que están autorizados.

e. Autenticación de usuario para conexiones externas

La administración deberá determinar los métodos que se utilizaran para la autenticación de los controles de accesos remotos.

f. Protección del puerto de diagnóstico remoto

La entidad debe controlar el acceso físico y lógico a los puestos de diagnóstico y configuración de estos para evitar incidentes de seguridad.

g. Control de conexiones de red

Se debe restringir la capacidad de usuarios para conectarse a una red.

h. Control de acceso al sistema operativo

Procedimiento en la terminal:

La administración debe establecer que los servicios solo se realizaran a través de un proceso de conexión segura. Lo cual reducirá el acceso no autorizado.

i. Identificación y autenticación del usuario

Todo el personal de las diferentes áreas de la entidad tendrán ID de usuario para uso personal exclusivo.

j. Sistema de gestión de claves

Las claves o contraseñas deberán ser las más seguras y debe:

- El usuario crear su contraseña para determinar responsabilidades.
- Cambiar en un periodo estipulado las contraseñas
- Mantener un registro de las contraseñas cambiadas
- No mostrar la contraseña en pantalla
- Las contraseñas deben ser alfanuméricas con mínimo de 15 caracteres

k. Restricción al acceso a la información

Los usuarios de los sistemas tendrán acceso a la información y a las funciones considerando la política de control de acceso.

l. Computación móvil y comunicaciones

Se imprentaran medidas adecuadas para este tipo de dispositivos móviles, que tomen nada mas los controles necesarios en cuanto a la protección física, el acceso seguro a los dispositivos y acceso a los sistemas de información.

7. Adquisición, desarrollo y mantenimiento de los sistemas de información

La administración definirá los controles y procedimientos que serán implementados en los sistemas de la entidad, mediante técnicas criptográficas con el fin de proteger el sistema.

a. Análisis y especificaciones de los sistemas

La entidad debe especificar lo requerimientos de los controles y análisis del proceso del sistema en cuanto a fallos, para incorporar seguridad a los sistemas de la entidad.

b. Procesamiento correcto de las aplicaciones

Se asegurara que el sistema mediante procedimientos y controles determine la validez de los datos que se ingresa y valide a fin de reducir riesgos de fallas del procesamiento de la información.

c. Políticas sobre el uso de controles criptográficos

La administración en conjunto con el comité de riesgo técnicas de criptografías, cifrado y firmas digitales para la protección y mantenimiento de las características de integridad, disponibilidad y confidencialidad.

La entidad establecerá técnicas criptográficas para:

- La transmisión de información
- Para el resguardo y aseguramiento de la información
- Para la protección de claves de usuarios entre otras

d. Controles de software operacional

La administración deberá establecer procedimientos para el control de la instalación del software en los sistemas de la entidad, el cual será el responsable y la persona únicamente autorizada para aprobar las actualizaciones al sistema.

Se evitara el uso de bases de datos que contenga información personal o confidencial como propósitos de pruebas por lo que se debe establecer procedimientos para dicha actividad.

e. Procedimientos de control de cambio

Al momento de modificaciones, actualizaciones o eliminación de los datos operativos se documentara los procesos formales del control de cambio, además de verificar que los datos del sistema no se hayan visto afectados.

f. Filtración de información

A fin de minimizar la filtración de la información la entidad debe:

- Evitar las oportunidades para la filtración de la información
- Monitorear la utilización de recursos en los sistemas
- Monitorear las actividades efectuadas por los empleados.
- Inspeccionar los medios en busca de información escondida.

g. Control de la vulnerabilidades técnicas

La administración deberá obtener información mediante la evaluaciones del sistema si existen vulnerabilidades técnicas, a fin de definir roles y responsabilidades y evaluación de los riesgo existentes

8. Gestión de incidentes en la seguridad de la información

a. Reporte de eventos de seguridad de información

Determinar y documentar mediante reportes sobre factores que ponen en riesgo la seguridad de la información.

b. Reporte de debilidades en la seguridad

La administración debe desarrollar requerimientos encaminados a que los usuarios, empleados y encargados del departamento de sistema y seguridad de la información tomen nota y generen reportes sobre cualquier debilidad o anomalía que ponga en riesgo la seguridad de la información

c. Responsabilidades y procedimientos

Para el caso de incidentes en la seguridad de la información se debe establecer el responsable quien será el encargado de dar respuesta a los riesgos de manera eficiente y efectiva ante los incidentes de seguridad.

d. Educarse a través de los incidentes de seguridad de la información

Para los incidentes de seguridad se establecerá un mecanismo que nos permita medir y monitorear el nivel de impacto que los incidentes ocasiones

e. Recolección de evidencia

Auditoría interna en conjunto con los responsables de TI determinaran controles para la recolección de evidencia mediante seguimientos contra empleados involucrados en incidentes de seguridad.

9. Gestión de la continuidad del negocio

a. Proceso de gestión de continuidad del negocio incluyendo la seguridad de la información.

La administración en conjunto con el responsable de TI deberán definir un plan de contingencia en cuanto a posibles hechos como:

- Identificar las amenazas que pueden interrumpir los procesos y continuidad de las operaciones del negocio.
- Evaluar los riesgos de los impactos que puede generar las interrupciones
- Identificación de los controles preventivos
- Desarrollo de plan estratégico para la continuidad de las operaciones del negocio.

b. Evaluación del riesgo sobre la continuidad de la entidad

Identificar y documentar los sucesos que provoquen interrupciones en las actividades comerciales de la entidad así como evaluación del riesgo ante la probabilidad de dichos sucesos que puedan generar una interrupción.

c. Desarrollar e implementar planes de continuidad de la entidad

A manera de dar respuesta a dichos riesgos, se debe contar con un plan de continuidad de actividades de la entidad que contenga:

- Los eventos que pueden causar estas interrupciones
- Evaluar los riesgos para determinar el impacto.
- Identificas los controles que pueda evitar estos acontecimientos.

d. Marco referencial de planeación de continuidad de la entidad.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada requerimiento descrito del mismo. Se mantendrá un solo marco para los planes de continuidad de las actividades de la entidad, a fin de garantizar que los mismos sean uniformes.

e. Prueba, mantenimiento, re-evaluación de planes de continuidad de la entidad

S**e** realizaran procedimientos para evaluar la continuidad del negocio de manera que sean probados, actualizados y efectivos antes los acontecimientos.

10. Cumplimiento

a. Identificación de la legislación aplicable

Se establecerá y documentará todos los requerimientos normativos y contractuales para cada sistema de la entidad, incluyendo los controles referentes a las responsabilidades de cada empleado para dar cumplir con los requerimientos.

b. Derecho de propiedad intelectual

La administración diseñará e implantara controles adecuados para asegurar el cumplimiento de las restricciones legales al uso de los software u otros protegido por normas de propiedad intelectual como los siguientes:

- Definir normas y procedimientos para el cumplimiento de los derechos de propiedad intelectual.
- Mantener un adecuado registro de activos
- Conservar pruebas de propiedad de licencias.
- Se debe instalar solo productos con licencias autorizados
- Cumplir con los términos y condiciones de las licencias y software

c. Protección de registros organizacionales.

La información que maneja la entidad debe estar protegida contra cualquier pérdida y extracción de datos, asegurando la confidencialidad e integridad de la información.

d. Protección de la data y privacidad de la información personal

Se deberá conocer por parte de todos los empleados las restricciones que incorpora el manejo de los datos que la entidad tiene, por lo que se realizara un compromiso de confidencialidad por parte de los empleados.

e. Prevención del mal uso de los procesamiento de información

Toda la información utilizada con propósitos ajenos a la función de la entidad, será definida como uso indebido de la información, lo cual se sancionara de acuerdo a la clasificación de la falta.

f. Regulación de controles criptográficos

La entidad al implementar controles criptográficos como firmas digitales o electrónicas, se deberá considerar la ley vigente referente a la Ley de firmas electrónicas, la cual establece las condiciones del uso de tal mecanismo.

g. Cumplimiento con las políticas y estándares de seguridad.

El responsable de cada área de la entidad, verificará la correcta implementación de los procedimientos y controles de seguridad definidos. Todas las áreas de la entidad deben verificar lo anterior mencionado.

Auditoría interna apoyara a la revisión periódica del cumplimiento de las políticas y procedimientos aplicables.

h. Chequeo del cumplimiento técnico

Se debe realizar revisiones periódicas que los sistemas de información que cumplan con las políticas y controles, lo que incluirá además las revisiones a los controles de hardware y software se estén realizando de manera correcta para su buen funcionamiento.

i. Controles de auditoría de los sistemas de información

Al momento de las revisiones periódicas de los sistemas de información deberá planificarse las tareas y el tiempo de realización y dar aviso a todos los empleados para minimizar el tiempo de interrupción de las actividades.

j. Protección de las herramientas de auditoría de los sistemas de información.

Desarrollo de controles para el acceso de herramientas de auditoría de los sistemas de información con el fin de minimizar el mal uso o transgresión posible.

SANCIONES

Leves

Son incidentes relacionados con los siguientes aspectos

- Uso de correo electrónico gratuito
- Omisión de documentar accesos en bitácoras
- Omisión de remoción de la información en medios removibles
- Realizar back-ups de la información no autorizados
- Usuario no cierre sesión
- Uso de claves que cumplen los requerimientos de seguridad
- No reportar fallas de seguridad
- Jugar en las computadoras
- No respetar las medidas de seguridad de los equipos

Graves

Cualquiera de los siguientes incidentes:

- Acceso indebido a la información
- Sustracción de información
- Compartir claves y acceso a los sistemas y a la información
- Accesos a la información fuera del horario de trabajo sin autorización previa
- Transferencia de usuarios y claves de autenticación
- Modificación de la información con fines ilícitos
- Alterar información por medio de accesos remotos no autorizados
- Instalar, modificar la configuración sin la autorización
- Introducir cualquier tipo de virus o malware intencionalmente
- Apropiarse de piezas del equipo de trabajo
- Todos los incidentes leves que se acumulen se convertirán en faltas graves

Muy graves

Los siguientes incidentes son clasificados como uy graves:

- Robo y transferencia de información
- Brindar acceso a internet a personas ajenas a la entidad sin la debida autorización
- Dañar de forma reiterada los dispositivos de seguridad del equipo
- Trasladar el equipo a lugares no autorizados
- Venta de bases de datos a terceros
- Alteración a los sistemas de información
- Todas las faltas leves o graves que se acumulen en múltiples ocasiones se convertirán en faltas muy graves

Sanciones para las faltas leves son:

- Amonestación verbal
- Amonestación escrita

Sanciones para las faltas graves son:

- Amonestación escrita
- Sanción sin goce de sueldo

Sanciones para las faltas muy graves son:

- Amonestación escrita
- Sanción sin goce de sueldo
- Suspensión del uso de los servicios a que tiene acceso
- Despido
- Prisión

APÈNDICE

APÈNDICE A

Programa de capacitación

Objetivo

Capacitar al recurso humano a fin de que estos estén a la vanguardia de las tecnologías de información y los riesgos que conlleva esta área.

Propiciar la capacitación en temas imprescindibles para cumplir con requisitos legales y normativos respecto al uso y goce de las tecnologías de información.

Personal al que se dirige: La gerencia, empleados de los distintos departamentos.

Temario

1. Riesgos y administración de riegos
   - Objetivo de la gobernanza
   - Riesgo
   - Aplicación de los principios de Cobit 5 en la gestión del riesgo

2. Perspectiva de la administración de riesgos
   - Escenario del riesgo
   - Factores de riesgo
   - Estructura
   - Aspectos principales

3. Marco legal aplicable a las tecnologías de información
   - Ley de la firma electrónica

APENDICE B

FORMATO PARA DATOS PERSONALES.

Nombre completo:	**Dirección:**
Teléfono:	**Lugar y fecha de nacimiento:**
Nacionalidad:	
DUI:	**Seguro Social:**
Licencia:	**NIT :**
AFP:	**Tipo de AFP :**
Edad:	**Estado Civil**

Estudios:

Nombre de la institución	Desde	Hasta	Certificado o título
Bachillerato			
Universidad			
Postgrado			
Maestría			
Cursos			
Otros			

Especifique sus conocimientos en Sistema Operativo o Manejo de Herramientas:

_____

_____

Nombre completo de las personas que dependen de usted:

_____

_____

Nombre completo de su padre:_____**Profesión:**_____

Dirección:_____**Teléfono:**_____

Nombre completo de su madre:_____**Profesión:**_____

Dirección:_____**Teléfono:**_____

Personas que deben ser notificadas en caso de emergencia:

Nombre	Parentesco	Dirección	Teléfono

*Nombre completo del cónyuge:*_____*Edad:*_____

Trabaja en:_____Desde:_____

Dirección:_____Teléfono:_____

*Cargo que desempeña su cónyuge:*_____*Salario:*_____

*¿Qué enfermedades serias ha tenido usted (nombre y fecha):*_____

_____

Tipo de Sangre: _____ Alergias: _____

Nombre de las personas con quienes vive:

Nombre completo	Edad	Ocupación

Referencias: Nombre de dos (2) personas que no sean familiares

Nombre completo	Lugar de trabajo	Teléfono

¿Trabaja usted actualmente? Sí_____ No_____

¿Dónde?_____Cargo:_____Salario $ _____

¿Por qué desea cambiarse?_____

APENDICE C

Empleos Anteriores

Favor anotar primero el más reciente

Empresa:____ Teléfono:________________________________

Dirección: ____**Cargo:** ________________________________

Salario inicial $________________**Salario final $**___ ________**Trabajó desde:** __________________________

Hasta: ________________________ **Nombre del jefe inmediato:** ____________________________________

Describa sus funciones: ____

____

Motivo de salida:____

Empresa:____ Teléfono:________________________________

Dirección: ____**Cargo:** ________________________________

Salario inicial $________________**Salario final $**___ ________**Trabajó desde:** __________________________

Hasta: ________________________ **Nombre del jefe inmediato:** ____________________________________

Describa sus funciones: ____

____

Motivo de salida:____

Empresa:____ Teléfono:________________________________

Dirección: ____**Cargo:** ________________________________

Salario inicial $________________**Salario final $**___ ________**Trabajó desde:** __________________________

Hasta: ________________________ **Nombre del jefe inmediato:** ____________________________________

Describa sus funciones: ____

____

Motivo de salida:____

¿Está dispuesto a someterse a un examen del polígrafo? Sí____ No____

Hago constar que los datos arriba detallados, son ciertos y pueden ser confirmados.

Empleo solicitado: __________________________________Salario deseado $__________

ADJUNTAR: FOTOGRAFIA, CARTAS DE RECOMENDACIONES, CERTIFICADOS MEDICOS, COPIA DE DUI, NIT, SEGURO SOCIAL Y AFP.

Firma: ___________________________________Fecha: __________________________

APÉNDICE D

Bitácora de acceso de usuarios

	BITÁCORA DE ACCESO	
FECHA DE INICIO :		**FECHA FINAL**

Fecha	Usuario	Acción	Observación

APENDICE E

	BITÁCORA DE ACCESO	
FECHA DE INICIO :		**FECHA FINAL**

Fecha	Tipo	Usuario	Resumen	Objeto	Empleado

APÉNDICE F

BITÁCORA DE CONTROL DE SOPORTE TECNICO.

FECHA DE INICIO :	**FECHA FINAL**

Fecha	Hora	Datos de quien opera.	Área de Equipo Informático	Característica del Equipo.	Problema del Equipo	Solución

APÉNDICE G

Ubicación :	BITÁCORA DE ACTIVOS.	
FECHA DE INICIO :		**FECHA FINAL**

Código	**Fecha de Adquisición**	**Tipo de Bien**	**Descripción del bien**	**Ubicación física del bien**	**Persona Responsable**