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

SISTEMA DE GESTIÓN DE SEGURIDAD

PARA LOS PUESTOS DE BOLSA DE PRODUCTOS Y SERVICIOS

QUE GARANTICE LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD

DE LA INFORMACIÓN

TRABAJO DE GRADUACIÓN PRESENTADO POR:

Medina Echegoyén, Brandy José
Reyes Portillo, Saúl Leonel
Salinas Landaverde, Angela Guadalupe

Para optar al grado de:
LICENCIADO EN CONTADURÍA PÚBLICA

NOVIEMBRE 2017

SAN SALVADOR, EL SALVADOR, CENTRO AMÉRICA

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

AUTORIDADES UNIVERSITARIAS

Rector	:	Master Roger Armando Arias Alvarado
Secretario General	:	Master Cristóbal Hernández Ríos Benítez
Decano de la Facultad de Ciencias Económicas	:	Lic. Nixon Rogelio Hernández Vásquez
Secretaria de la Facultad de Ciencias Económicas	:	Licda. Vilma Marisol Mejía Trujillo
Directora de la Escuela de Contaduría Pública	:	Licda. María Margarita de Jesús Martínez Mendoza de Hernández
Coordinador General de Procesos de Graduación Facultad de Ciencias Económicas	:	Lic. Mauricio Ernesto Magaña Menéndez
Coordinador de Seminario de Procesos de Graduación de la Escuela de Contaduría Pública	:	Lic. Daniel Nehemías Reyes López
Docente director	:	Master Mario Hernán Cornejo Pérez
Jurado evaluador	:	Máster Mario Hernán Cornejo Pérez Lic. Daniel Nehemías Reyes López Lic. Carlos Ernesto Ramírez

Noviembre 2017

San Salvador, El Salvador, Centro América

AGRADECIMIENTOS

A Dios, mis padres, Guillermo, Hilda, Brandy, Saúl, demás amigos, compañeros y docentes con quienes compartí en este arduo y maravilloso camino universitario; agradezco inmensamente todo su apoyo y amor incondicional. *"We were born to make history"* ***Dean Fujioka.***

Angela Guadalupe Salinas Landaverde

A Dios, primeramente, por bendecirme y ser mi guía en todos los aspectos de mi vida y en especial en la culminación de mi carrera, por darme la fortaleza y el espíritu de voluntad necesario. A mis padres, hermanos, amigos y demás familiares, por el esfuerzo y sacrificio que realizaron para contribuir al logro de mi objetivo. A todos los docentes que contribuyeron en mi formación académica profesional y especialmente a mi equipo de trabajo por el tiempo dedicado en el desarrollo de la investigación.

Saúl Leonel Reyes Portillo

Agradezco en primer lugar a mi madre Alicia por su apoyo incondicional durante todo el proceso de formación humana, académica y profesional hasta la actualidad. En segundo lugar, a mis familiares que estuvieron pendiente de mis actividades académicas y mi mejor amiga Cecilia por su compañía y amistad en estos 6 años. En tercero, a mi equipo de trabajo por su esfuerzo en la culminación de esta etapa y demás amigos que conocí en el entorno universitario, acompañándome en esta fase de mi desarrollo humano. Finalmente, a todos los maestros y docentes que han sido parte de mi preparación escolar y universitaria, destacando su importante labor en el proceso de enseñanza-aprendizaje. "*Todos nosotros sabemos algo. Todos nosotros ignoramos algo. Por eso, aprendemos siempre".* ***Paulo Freire***

Brandy José Medina Echegoyén

ÍNDICE

Índice de tablas

Índice de figuras

Índice de anexos

RESUMEN EJECUTIVO

La integridad, disponibilidad y confidencialidad de la información de los puestos de bolsa de productos y servicios es de gran importancia, ya que dichas entidades la necesitan para una toma de decisiones oportuna y comunicar lo requerido por ley a la Superintendencia del Sistema Financiero, la Bolsa de Productos de El Salvador, otros puestos de bolsa, proveedores y clientes. Con la finalidad de que la información posea las características antes citadas se realiza esta propuesta de un sistema de gestión de seguridad de la información (SGSI) basado en la Norma Técnica Salvadoreña (NTS) ISO/IEC 27001:2013.

De forma general se propone diseñar de un SGSI que garantice la integridad, confidencialidad y disponibilidad de la información tanto física como digital de las sociedades dedicadas a la intermediación de productos y servicios que han sido autorizadas por la Bolsa de Producto y Servicios de El Salvador. Tal objetivo se alcanzará mediante se identifiquen los requerimientos establecidos por la NTS ISO/IEC 27001:2013 para el SGSI.

En la investigación se utilizó el método hipotético-deductivo, debido a que se detallarán las características del problema en la gestión de la seguridad de la información que se presentan en la mayoría de los puestos de bolsa de productos y servicios, para ello se emplearon encuestas con las cuales se recolectarán los datos que se analizarán para la comprobación de hipótesis. Se obtuvo la participación de siete de ocho gerentes generales de los puestos de bolsa de productos y servicios de El Salvador quienes respondieron a la encuesta, de cuyos resultados los más destacados fueron: la gran mayoría de los gerentes de las entidades no tienen conocimiento de un SGSI y la NTS ISO/IEC 27001:2013, poseen controles establecidos para procurar el resguardo de la información, pero estos no se encuentran descritos en algún documento en forma de políticas y poseen controles que resultan deficientes para gestionar el activo.

Posterior al análisis y estudio de la situación de los puestos de bolsas de productos y servicios puede concluirse: en su mayoría desconocen de la existencia de los sistemas de gestión de seguridad de la información esto permite que, a pesar de la implementación de ciertos tipos de controles, la información no cuente con el nivel de seguridad adecuada y por lo tanto se encuentre expuesta a cierto tipo de amenazas producto de las vulnerabilidades existentes; las entidades presentan una ausencia de controles enfocados a proteger y resguardar la información que es intercambiada con los usuarios puede tener consecuencias negativas para la entidad en aspectos financieros, legales, contractuales y de imagen frente a las partes interesadas, existe una carencia de metodología de seguridad para los puestos de bolsas puede ser superada con la implementación del sistema de gestión de seguridad de la información.

Con la finalidad de que las entidades superen esas deficiencias y se avoquen a una mejora continua se sugiere las siguientes recomendaciones: es necesario fortalecer y desarrollar adecuadamente la preparación académica de los profesionales que estudian la carrera de Contaduría Pública en la Universidad de El Salvador, respecto al diseño e implementación de los SGSI y la normativa técnica relacionada; la importancia que los puestos de bolsa de productos y servicios puedan diseñar e implementar un SGSI integral a corto plazo, según sus necesidades y homogenizarlas con los requerimientos de seguridad que solicite la Bolsa de Productos y Servicios de El Salvador. Es necesaria la capacitación y concientización sobre temas de seguridad de la información y normativa aplicables a esta, a la alta dirección de los puestos de bolsa, con la finalidad que logren un adecuado diseño e implementación de un SGSI, además de que se agregue el área de seguridad el a información en la gestión de riesgos de los puestos de bolsa, con el objetivo que se le brinde la prioridad requerida en el plan de tratamiento de los riesgos corporativos.

INTRODUCCIÓN

En la actualidad se ha definido a la información como uno de los activos más importantes para las organizaciones y que a su vez están dependiendo de medios digitales para procesarla, todas las entidades independientemente de su tamaño, naturaleza deben ser conscientes de la diversidad de amenazas existentes que puede atentar contra la seguridad y privacidad de la información y representar un riesgo que al materializarse puede tener consecuencias negativas tales como sanciones legales, contractuales y económicas que pueden afectar la imagen corporativa y a su vez la continuidad del negocio. Por lo tanto, este recurso debe ser protegido de una forma adecuada; la integridad, disponibilidad y confidencialidad son características fundamentales de la seguridad de la información

Ante este contexto ha surgido la necesidad de diseñar un sistema de gestión de seguridad de la información (SGSI), con base a la Norma Técnica Salvadoreña ISO/IEC 27001:2013 "Sistemas de Gestión de Seguridad de la Información" que puede ser implementado por los Puestos de Bolsas de Productos y Servicios de El Salvador.

Para su desarrollo, el trabajo se divide en cuatro capítulos, el capítulo I, contiene el planteamiento del problema y consiste básicamente en describir breves antecedentes de la situación problemática, enunciado del problema, justificación, objetivos de la investigación, planteamiento de hipótesis y limitantes de la investigación.

El capítulo II detalla los aspectos más importantes sobre la seguridad de la información y describe los antecedentes de los Puestos de Bolsas de Productos y Servicios de El Salvador, hace referencia a los sistemas de gestión de seguridad de la información a sus ventajas y desventajas y por último se hace mención del marco legal y normativo aplicable a este trabajo.

El capítulo III describe la metodología implementada para obtención de resultados ya que incluye el enfoque y tipo de investigación, delimitación espacial y temporal, unidades de análisis, variables, técnicas, materiales e instrumentos de medición, procesamiento y análisis de la información y finaliza con el diagnostico de los resultados.

Finalmente se encuentra el capítulo IV, donde se desarrolla la propuesta que consiste en el diseño de un SGSI basado en la Norma Técnica Salvadoreña ISO/IEC 27001:2013 “Sistemas de Gestión de Seguridad de la Información” que ayude a gestionar la seguridad de la información de los puestos de bolsa y a reducir los riesgos a un nivel aceptable.

CAPÍTULO I-PLANTEAMIENTO DEL PROBLEMA

1.1. SITUACION PROBLEMÁTICA EN RELACION A LA SEGURIDAD DE LA INFORMACION EN LOS PUESTOS DE BOLSAS DE PRODUCTOS SERVICIOS DE EL SALVADOR

La seguridad de la información un aspecto de vital importancia a considerar en las empresas independientemente de su tamaño o naturaleza, la integridad, confidencialidad y disponibilidad son características esenciales de este importante recurso que sirven para mantener niveles de competencia, rentabilidad, imagen corporativa y dar cumplimientos de aspectos legales y contractuales enfocados al logro de los objetivos y asegurar los beneficios económicos de todas las organizaciones y para el caso de los puestos de bolsas de productos y servicios de El Salvador no es la excepción al ser entidades dedicadas al intermediación bursátil de productos y servicios están obligadas a buscar medidas de protección para este valioso recurso por la existencia de una ley específica que les exige protegerla; aunque en la actualidad les resulte poco relevante esta situación, el problema surge con el nacimiento del sector de la intermediación bursátil en El Salvador, en el año de 1995, constituyéndose la primera la Bolsa de Productos y Servicios Agropecuarios, con el objetivo de ser el canal de comercialización más importante para las asociaciones agropecuarias de ese entonces permitiéndoles realizar convenios de compra y venta de granos básicos dentro de un mercado organizado siendo las negociaciones a través de los procesos de subasta pública, a viva voz y de forma transparente, donde los productos eran negociados por descripción es decir sin la presencia física de compradores, vendedores y productos; para realizar este proceso de negociación la bolsa, como todas de mundo, ejecuta sus operaciones a través de puestos de bolsas autorizados.

Los puestos de bolsa son entidades privadas facultades por las bolsas de productos y servicios con la finalidad primordial de intermediar compras y ventas de productos y servicios solicitados por los clientes.

La problemática se origina con los siguientes tres eventos:

- El 19 de junio del 1997 fue aprobada la Ley de Bolsas de Productos y Servicios Agropecuario que expresa que los puestos de bolsas deben proporcionar información oportuna, clara y veraz, es decir, que conserve su integridad, disponibilidad y sea fiable según los arts. 21 literales e) y f), 32, 33 y 37.
- Posteriormente la publicación del reglamento de la ley antes citada, resultan importantes los artículos 35 literales d), e) y f); 55 numeral 1); 59 numerales 6) y 7); y 60 numeral 4); que otorgan mayores responsabilidades a las entidades respecto a la temática.
- El 10 de noviembre de 2005 la Asamblea Legislativa dio aprobación al decreto No. 868 que reformaba la Ley de Bolsas de Productos Agropecuarios y se renombraba como Ley de Bolsas de Productos y Servicios, permitiendo con esto ampliar el campo de acción de la BOLPROS, volviéndose más general ya no limitándolo sólo al sector agropecuario; lo cual incremento el volumen de la información en los diversos puestos de bolsa y la responsabilidad de estos en cuanto a su custodia.

En la actualidad, existen muchas amenazas y vulnerabilidades para la información que incorporan y procesan los diversos puestos de bolsa, debido a que es creciente el número de productores de granos básicos, empresas industriales y comerciantes que realizan negocios a través de la intermediación bursátil y requieren un control adecuado de la información que les garantiza la transparencia, profesionalismo y seguridad de las operaciones y la información de los mercados.

La importancia del sector es debido a que representa un mecanismo formalizado y vanguardista en el comercio de productos y servicios (Mejía, 2017), entre el gobierno de El Salvador y la empresa privada, permitiéndole al estado ahorrar dinero, disminuir los plazos de entrega del producto o servicios y evitar que se produzca una colusión de precios de mercado (que todos los proveedores participantes acuerden un precio superior al de mercado); además puede hacerse entre comerciantes privados (pero es muy poco usual debido a que no se ha sido un sector incentivado); para el año 2014 se negociaron cerca de US$61 millones y en 2015 aproximadamente US$75 millones, siendo un crecimiento significativo de cerca del 23%. (Bolsa de Productos de El Salvador, 2015)

El inicio del siglo XXI, trajo nuevos retos y la ampliación de los mercados donde operaban los puestos de bolsa, ya que comenzaron a trabajar con la intermediación de las compras que realizaba el gobierno, eso conllevo a procesar información más sensible, y por los avances tecnológicos del momento, a iniciar la dependencia de los equipos y sistemas informáticos, lo que permitió estar más expuestos a diversas amenazas de seguridad como fraude por computadora, espionaje, sabotaje, actividades de vandalismo, manipulación de la información sin autorización, incendios, inundaciones y otras, ya sean generadas por la intervención del ser humano para causar daños u obtener beneficios de forma desleal o como resultado de un fenómeno de la naturaleza. (Organización Internacional de Estandarizacion y Comisión Electrotécnica Internacional, 2007)

Los puestos de bolsa están obligados según la Ley de Bolsas de Productos y Servicios a garantizar la gestión del negocio, llevar los registros necesarios de las operaciones bursátiles que realizan, brindar íntegra y oportunamente la información que requiera la Superintendencia del Sistema Financiero (SSF) como entidad facultada para vigilar el cumplimiento de la ley antes mencionada o la Bolsa de Productos de El Salvador (BOLPROS), además de las obligaciones

mercantiles y fiscales, relacionadas con la elaboración, presentación y/o resguardo de la información que deben cumplir para operar como sociedad dentro del territorio salvadoreño.

Ante esa coyuntura, las entidades que prestan servicios de intermediación bursátil en El Salvador, están sugestionadas a resguardar la información que le suministran sus clientes como la que ellos generan por su actividad comercial, implementado ciertos controles que les permite la gestión de dicho recurso. Al realizar una investigación previa, existen deficiencias en cuanto a ciertos procesos, entre ellos, la mayoría de puestos utilizan el mismo proveedor del sistema contable, lo que vulnera a que se revele información confidencial a los otros puestos, el proceso de eliminación de información confidencial no es supervisado ni es el adecuado, la comunicación de la información física es por medio de mensajeros, para lo cual no existe un plan para mitigar el riesgo de robo o pérdida de documentos, los sistemas operativos no se actualizan automáticamente, no se generan copias de seguridad automáticas para los sistemas de información debido a que son bases de datos en Access y no un sistema integrado, no existe mantenimiento de los ordenadores ni los sistemas de vigilancia de cámaras web, no se capacita al personal para el manejo del sistema contable, no existe una manual para el uso de tal sistema, se ha definido una segregación de funciones pero no se cumple adecuadamente, entre otros.

Entre las desventajas de no poseer un sistema que gestione la seguridad de la información pueden ser las siguientes: (Ernst & Young, 2014)

- No existe una identificación real de los riesgos ni protección hacia los recursos de más alto valor.
- No se invierte de forma prudente en tecnología. No se aseguran las funciones del gobierno de la entidad.

- No se habilita el desempeño óptimo del negocio.

En su calidad de profesional, el contador público, basado en lo determinado por el Estándar de Educación Internacional 2 (IES 2, por sus siglas en inglés), debe tener una formación en conocimiento y competencias en tecnologías de la información. Siendo el desarrollo de un SGSI una oportunidad para mejorar sus capacidades en las áreas tecnológicas y análisis de riesgos informáticos, ampliando de esta forma, los campos de acción, participación e investigación de los contadores públicos en El Salvador.

1.2. ENUNCIADO DEL PROBLEMA

¿En qué medida se ven afectadas las entidades que prestan servicios de intermediación bursátil autorizadas por la Bolsa de Productos de El Salvador en los municipios de San Salvador y Antiguo Cuscatlán, al no disponer de un sistema de gestión de la seguridad de la información que les permita administrar adecuadamente la disponibilidad, confidencialidad e integridad de la información proporcionada por sus clientes y la procesada por ellas?

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Al reconocer la importancia que tiene la información que generan y procesan las entidades que prestan servicios de intermediación bursátil en los municipios de San Salvador y Antiguo Cuscatlán, luego de haber realizado un estudio de administración de dicho recurso, se determinó que este sector carece de herramientas de gestión que garanticen a un nivel aceptable, la integridad, confidencialidad y disponibilidad de la información; al no contar con un sistema que contemple políticas de seguridad de la información, tal recurso se encuentra expuesto a todo tipo de amenazas como resultado de la vulnerabilidad existente, ya que no se generan copias de seguridad automáticas *(back up)* , la inexistencia de una jerarquía de autorización para el acceso a

la información , ausencia de un contrato de mantenimiento de los ordenadores de almacenamiento, el personal no recibe capacitaciones para el manejo y uso de programas informáticos, carencia de un control de visitas de personas externas a los puestos de bolsas de productos y servicios, falta de supervisión sobre el uso de internet y redes inalámbricas, entre otras situaciones.

Ante estas necesidades se procede a manifestar la importancia de diseñar un sistema de gestión de la seguridad de la información para este sector, haciendo énfasis a lo novedoso, a la factibilidad y la utilidad social que tendría el diseño de un SGSI.

1.3.1. Novedoso.

Aunque la seguridad de la información sea un tema poco usual entre los académicos contables e incluso entre muchos contadores que ejercen la profesión (ya sea dentro de una organización o de forma independiente) es novedoso que profesionales de la contabilidad tomen participación en áreas vinculadas a las tecnologías de la información.

Ante esa situación, han surgido a nivel internacional normativas, lineamientos, estándares y guías que vinculan íntegramente a los contadores con temas relacionados a tecnologías de la información. Por lo que, la seguridad de los datos, es también responsabilidad de los contables ya que ellos administran grandes cantidades y deben cumplir con requerimientos legales que les obligan a presentarlos y mantenerlos ordenados, originando así, la necesidad de protegerlos. Diseñar una un SGSI basado en la NTS ISO/IEC 27001:2013, para puestos de bolsa de productos y servicios de El Salvador, permitirá a los contadores tomar parte en la gestión de riesgos de estas entidades y motivar a otros profesionales a participar en esta área de forma similar.

1.3.2. Factibilidad.

El desarrollo de la investigación se considera factible por la existencia de un marco normativo internacional adoptado por el Organismo Salvadoreño de Normalización referente al diseño de un sistema de gestión de la seguridad de la información además de libros, revistas y sitios web oficiales que orientarán y facilitarán el desarrollo de la investigación. Así mismo, se tiene acceso al universo de estudio siendo estos los puestos de bolsa de productos y servicios; se cuenta con la disponibilidad del tiempo y de recursos económicos y tecnológicos para la ejecución de la investigación y con el propósito de obtener resultados favorables, se hará uso de técnicas de investigación como cuestionarios y visitas para extraer la información necesaria y de utilidad.

1.3.3. Utilidad Social.

Los principales beneficiarios con la investigación, son los puestos de bolsa de productos y servicios de El Salvador y su personal, quienes ante las vulnerabilidades existentes producto de la falta de una herramienta de gestión para la seguridad de la información podrán utilizar el modelo sugerido anteriormente, el cual les permitirá administrar y gestionar a un nivel aceptable, la integridad, confidencialidad y disponibilidad de la información que procesan y de esa forma lograr que sus procesos sean más eficientes, confiables y transparentes, teniendo una participación activa el profesional en contaduría pública que labora en este sector al ser la persona que procesa mayor cantidad de información tendrá la oportunidad de ampliar sus conocimientos en relación a la seguridad de la información y como a través del uso de un sistema de gestión de la seguridad de la información se pueden minimizar los riesgos a un nivel aceptable.

En segundo lugar, se tiene como beneficiario a la Bolsa de Productos de El Salvador, quien es la entidad receptora de la información generada por los puestos de bolsa, al gestionar la seguridad de la información se garantiza el cumplimiento a lo citado en el artículo 33 de la ley de bolsas.

En tercer lugar, se beneficiarían los estudiantes de contaduría pública de El Salvador, quienes ampliarán sus conocimientos respecto al rol que puede desempeñar un profesional contable en áreas relacionadas a tecnologías de la información, motivándolos a realizar y ampliar investigaciones en esta área o auditoría de sistemas.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1 Objetivo general.

- Diseñar un sistema de gestión de la seguridad que garantice la integridad, confidencialidad y disponibilidad de la información tanto física como digital de las sociedades dedicadas a la intermediación de productos y servicios autorizadas por la Bolsa de Producto de El Salvador.

1.4.2 Objetivos específicos.

- Identificar los requerimientos y estructura establecidos en el marco normativo internacional que permitan fundamentar el diseño del modelo de sistema de gestión de la seguridad de la información.
- Explicar los requerimientos y la estructura de un sistema de gestión de la seguridad de la información para la compresión de su diseño.
- Indagar modelos de sistemas de seguridad de la información que resulten de utilidad para el diseño de la propuesta del trabajo de investigación.

1.5. HIPÓTESIS DE LA INVESTIGACIÓN

1.5.1. Definición de la hipótesis de trabajo.

El diseño de un sistema de gestión de seguridad de la información basado en la Norma Técnica Salvadoreña ISO/IEC 27001:2013, podrá ser implementado posteriormente, para que la información generada y procesada en los puestos de bolsas conserve su confiabilidad, disponibilidad e integridad.

1.5.2. Determinación de variables.

Las variables de la hipótesis de la investigación son las siguientes:

- **Variable dependiente:** información integra, confiable y disponible.
- **Variable independiente:** sistema de gestión de seguridad de la información basado en la NTS ISO/IEC 27001:2013

1.6. LIMITACIONES DE LA INVESTIGACIÓN

La única limitante que afecto el desarrollo de la investigación fue la siguiente:

- La encuesta puesta a disposición para uno de los gerentes de los puestos de bolsas de productos y servicios al no existir colaboración para el llenado, dificultando la obtención de información necesaria para la presente investigación.

CAPÍTULO II-MARCO TEÓRICO, CONCEPTUAL, TÉCNICO Y LEGAL

2.1. ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS PUESTOS DE BOLSA DE PRODUCTOS Y SERVICIOS

En la actualidad muchas organizaciones afrontan cada día más riesgos provenientes de una amplia gama de fuentes que pueden dañar significativamente sus sistemas de información y propiciando la exposición de la continuidad del negocio al peligro de ser interferido. Ante esa situación es necesario que las entidades evalúen los riesgos a los que están vulnerables y logren establecer estrategias y controles adecuados que permitan asegurar una protección continua y salvaguarda de la información, ya que es un activo que podría hacer crecer o declinar una organización.

Los sistemas de gestión de seguridad de la información (SGSI) representan la forma efectiva de reducir los riesgos, ya que aseguran la identificación y valoración de los activos y sus riesgos, tomando en cuenta el impacto para la organización, adoptando como resultado, los controles y procedimientos más efectivos y congruentes con los objetivos de las entidades. Un SGSI conlleva crear una estructura y plan de diseño, implementación y mantenimiento de un conjunto de procesos que permitan gestionar adecuadamente la información, para asegurar la integridad, confidencialidad y disponibilidad de ésta.

Cualquier organización crea objetivos, usualmente vinculados con el mercado y los negocios, y necesita que, desde los procesos de operaciones hasta las políticas utilización de recursos, sean determinados a un nivel general, de forma confiable. Es conocido que la información suele relacionarse con computadoras y redes, pero existe otra forma que no se representa en forma de bits, sino por ejemplo en documentos físicos, en la memoria de los seres humanos, en el

conocimiento y experiencia de la entidad misma, en la madurez de sus procesos, entre otros. Para cada tipo de información (tangible e intangible), ésta debe ser protegida de modos diferentes, por lo que el SGSI pretende cubrir esa actividad.

Regularmente es posible reducir el impacto de los riesgos potenciales sin requerir de cambios drásticos, pero al mismo tiempo es vital planificar e implantar ciertos controles basados en un meticuloso análisis de riesgo. Un SGSI permite mantener los riesgos a un nivel aceptable o debajo de éste, siempre que se haya determinado a nivel directivo.

Muchas organizaciones tienen la idea que diseñar e implementar un SGSI es muy difícil, y que está enfocado a grandes corporaciones, lo que puede terminar provocando un manejo caótico o demasiado minimalista de la gestión de la seguridad. Sin embargo, es viable en algunos casos solo aplicar algunos principios, sin necesidad de diseñar un SGSI completo, para lograr mejoras muy importantes. Lo anterior requiere de obviar el cumplimiento total de una norma, pero sin dejar considerar sus lineamientos principales.

Desde una perspectiva de la alta gerencia, un SGSI lograría obtener una visión amplia del estado de los sistemas de información sin detenerse en especificaciones técnicas, además de poder visualizar las medidas de seguridad ejecutadas y los resultados obtenidos, y así, integrando todos estos elementos, tomar mejores decisiones estratégicas. Un detalle importante es que un SGSI tiene que estar documentado y ser de conocimiento general en todos los niveles de la organización, y estar agregado en un proceso global que logre una mejora continua. Finalmente, es imprescindible tomar en cuenta la norma ISO/IEC 27001:2013, que detalla los requisitos necesarios para establecer un SGSI.

Los objetivos globales de un SGSI son:

- Asegurar la confidencialidad, integridad y disponibilidad de los datos
- Conocer los riesgos de la seguridad de la información dentro de la entidad para aplicar medidas que permitan reducirlos a un nivel aceptable.
- Lograr un equilibrio entre la seguridad física, digital, técnica, procedimental y del personal.
- Determinar una metodología estructurada según el ciclo de Deming (planificar-hacer-verificar-actuar) que permita integrarse con otros sistemas de gestión ya implantados o a implementar a futuro.

Las operaciones en el mercado bursátil de productos y servicios persiguen ser una alternativa a los procesos de licitación pública por sus grandes ventajas (ahorro para los compradores, oportunidades de negocio para los vendedores, ampliación de clientes para vendedores, reducción significativa de los plazos de entrega de los productos o servicios, formas de pago flexibles y rápidas, no colusión de precios), aunque en la actualidad este mecanismo solo procesa aproximadamente un 3% de las compras totales realizadas por las entidades públicas, se espera siga incrementando a medida se vayan conociendo y desarrollando sus beneficios. Además, les asegura vender a los productores nacionales de arroz y maíz sus cosechas en el mercado local a precios razonables.

Cabe mencionar que cada operación de compra y venta implica el procesamiento de información sensible: contable, financiera, legal, crediticia, bancaria, fiscal, entre otras, según sea requerido, la cual puede provenir de los clientes, puestos de bolsa, Bolsa de Productos de El Salvador (BOLPROS) e incluso de la Superintendencia del Sistema Financiero, siendo todos ellos participantes del mecanismo bursátil.

Por lo que el diseño de un SGSI basado en NTS ISO/IEC 27001:2013 es una excelente alternativa para gestionar la información que entra y sale de los puestos de bolsa.

2.2. PRINCIPALES DEFINICIONES

- **Bolsa de productos y servicios:** es una entidad mediadora que tiene por finalidad organizar un mercado en donde las transacciones se hagan para toda clase de contratos de comercio permitidos por la ley. Se le puede denominar "Bolsa" según el artículo 1 de la Ley de Bolsa de Productos y Servicios de El Salvador.
- **Puestos de bolsa:** son personas nacionales o extranjeras, autorizadas por la Bolsa o por la Superintendencia para realizar las actividades de intermediación y prestación de servicios regulados en el reglamento según el artículo 30 del Reglamento General de la Bolsa de Productos y Servicios de El Salvador.
- **Información:** es un activo, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. (ISO/IEC 17799).
- **Activo de información:** son los recursos que utiliza el sistema de gestión de seguridad de la información para que las entidades funcionen y logren los objetivos que se han sido propuestos por la alta dirección.
- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC 27001:2005).
- **Confidencialidad:** es la propiedad de que la información esté disponible y que no sea divulgada a personas, entidades o procesos no autorizadas (ISO/IEC 27001:2005).
- **Integridad:** propiedad de salvaguardad la exactitud de la información. (ISO/IEC 27001:2005).

- **Disponibilidad:** propiedad de estar disponible y utilizable cuando lo requiera una organización. (ISO/IEC 27001:2005).
- **Sistema de gestión para la seguridad de la información (SGSI):** es un conjunto de políticas de administración de la información, es parte del sistema gerencial basado en un enfoque del riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. (ISO/IEC 27001:2005).

2.3. GENERALIDADES DE LOS PUESTOS DE BOLSA DE PRODUCTOS Y SERVICIOS

2.3.1. Antecedentes de los puestos de bolsas de productos y servicios de El Salvador.

Las operaciones bursátiles de productos agropecuarios en sus inicios no se realizaban dentro de un ambiente formal, debido en su gran mayoría a la ausencia de expertos en esta actividad, agregando a esto la falta de una legislación que se aplicara para garantizar la confiabilidad entre las transacciones realizadas por los participantes. La creación de bolsa de productos y servicios en El Salvador no es un hecho reciente ya que sus orígenes se remontan a la década de los 90's donde existía un mercado de libre interacción entre la oferta y la demanda, mediante un proceso de subasta a viva voz, donde productos agropecuarios e industriales de toda índole eran sujetos a negociaciones, sin la presencia física de los mismos; lo cual fue posible con la intermediación de los puestos de bolsa que fueron autorizados por la BOLPROS, la cual fue constituida por iniciativas del Instituto Interamericano de Cooperación para la Agricultura (IICA) en el año de 1992, formando un grupo que promovía la representación de productores agrícolas, vendedores, compradores, industriales, y entes financieros, entre otros.

En el mes de julio de 1995 se inaugura la primera bolsa de productos y servicios, dando inicio a sus operaciones el 24 de agosto del mismo año; en dicha fecha se comercializaron productos agropecuarios por un valor total de $ 5,508.57, recorriendo así desde un inicio un exitoso camino, para posicionarse posteriormente como la bolsa de productos agropecuarios más dinámica de Centroamérica.

La Ley de Bolsas de Productos y Servicios Agropecuarios fue aprobada el 19 de junio del 1997, con la finalidad de regular el marco de constitución, funcionamiento, limitaciones y prohibiciones, sanciones y demás actividades de la BOLPROS, permitiendo mecanismos de transparencia, eficiencia y seguridad en las transacciones realizadas entre las partes con la finalidad de comercializar los productos y servicios. Cabe resaltar la importancia de la Ley y su reglamento; ya que en ellos se contempla la obligación de procurar la integridad, confiablidad y disponibilidad de la información que es supervisada por la Superintendencia del Sistema Financiero.

2.2.2. Puesto de bolsa de productos y servicios.

Los puestos de bolsa por ley deben constituirse como personas jurídicas y tienen la finalidad de ejercer la intermediación en las negociaciones de compra-venta de productos y servicios (intermediación bursátil), que simultáneamente son representados por agentes de bolsa autorizados, los cuales pueden ser nacionales o extranjeros y realizar operaciones de compra-venta por su propia cuenta. (Guillen, Rivas, & Pérez, 2011)

Los puestos de bolsa están autorizados para realizar las siguientes actividades (Asamblea Legislativa de El Salvador, 2012):

- Actuar como intermediarios en la negociación de los productos y servicios en las Bolsas establecidas en El Salvador según lo dispuesto en la ley y reglamentos que los regulan y normas establecidas por las bolsas.
- Operar por cuenta propia, realizando la intermediación bursátil para sí, con la obligación de proporcionar privilegios a las órdenes de sus clientes con base en las normas que emita la bolsa.
- Recibir el pago de sus clientes como resultado de las operaciones acordadas.
- Operar centros de almacenamiento y depósito autorizados por las Bolsas.
- Prestar servicio de asesoría en temas relacionados con las operaciones de bolsas y comercialización de productos y servicios.

Obligaciones de los puestos de bolsas (Asamblea Legislativa de El Salvador, 2012):

- Cumplir con los acuerdos y resoluciones de las bolsas y las autoridades competentes (SSF y otras)
- Garantizar una buena gestión del a entidad según las disposiciones generales definidas por las bolsas.
- Remitir al menos dos veces al año sus estados financieros o declaraciones patrimoniales.
- Llevar los registros necesarios para generar transparencia y confianza de las negociaciones en las que participen, de manera que sea pueda obtener el conocimiento con claridad y exactitud dichas operaciones, indicándose el nombre de los contratantes, precios, cantidades, calidades y toda la información requerida por ley.
- Suministrar de forma oportuna clara y veraz toda la información que le solicite la bolsa en torno a sus actividades.

- Proporcionar a la Superintendencia del Sistema Financiero la información requerida para que pueda ejecutar sus funciones, en el momento que se le solicite.
- Entregar a los clientes copias de las boletas de liquidación de las operaciones mediadas.
- Facilitar a quien lo solicite y cuando fuere procedente, certificación de los registros de las operaciones realizadas.
- Permitir la fiscalización de la bolsa de todas sus operaciones.
- Llevar un registro de sus agentes o representantes.

2.2.3. Bolsa de productos y servicios.

Toda bolsa de productos y servicios funciona como una entidad mediadora, posibilitando que vendedores y compradores se puedan reunir en un mercado organizado, donde se negocian bienes y servicios. Las negociaciones de intermediación se ejecutan mediante un proceso de subasta pública, a viva voz o en línea.

Los productos a negociarse se deben describir y dar a conocer a los interesados sin la presencia física de los mismos (mediante contratos o cartas de requerimiento); todo esto debe estar bajo un marco reglamentado, que permita la igualdad de oportunidades a todos los participantes del mercado y garantizándoles la calidad de los productos y la liquidación de los mismos.

Una bolsa de productos y servicios es un mercado estructurado para reunir a compradores y vendedores de una negociación; es un sitio donde cualquier persona o entidad que pretenda comprar, logre hacerlo, y cualquier persona o entidad que desee vender, también lo pueda hacer; ya sea un producto o un servicio, todo en un mismo lugar (Mejía, 2017).

2.2.4. Suspensión o cancelación de puestos y licenciatarios en las bolsas.

Las bolsas de productos y servicios tienen la facultad de suspender las autorizaciones de operatividad de los Puestos en las Bolsas a consecuencia del incumplimiento de alguna obligación legal. A continuación, se detallan los casos que apliquen suspensión o cancelación (Asamblea Legislativa de El Salvador, 2012):

- Registrar o negociar operaciones simuladas o fraudulentas.
- Realizar operaciones fuera de las bolsas.
- Proporcionar información deficiente, falsa o no suministrarla en el periodo requerido a quien lo solicito.
- Mora en el pago de los cargos que les cobren las bolsas por su actividad.
- Pérdida de solvencia económica o financiera, aunque no sea declarada con suspensión de pagos o en quiebra;
- Entrar en conflicto con lo establecido en la ley y los reglamentos establecidos por las bolsas.
- Cambio de titular, de la mayoría de los titulares, socios, accionistas o directores de la sociedad titular del Puesto en la Bolsa, sin mediar autorización de la Bolsa.

2.3.5. Seguridad de la información y puestos de bolsa.

Cada puesto de bolsa procesa información sensible, tanto de terceros como de si mismos (transferencias bancarias, elaboración de informes, remisión de documentos físicos, entre otros). Por lo que, ante las diversas amenazas cibernéticas y físicas y los requerimientos de información que soliciten las instituciones facultadas para ello, se ven en la obligación de proteger

adecuadamente la integridad, confidencialidad y disponibilidad de este activo y así se permite mantener el negocio en marcha.

2.3. GENERALIDADES DE LA SEGURIDAD DE LA INFORMACIÓN.

2.4.1. Antecedentes de la seguridad de la información.

- **A nivel internacional.**

Se entiende por seguridad de la información a todas aquellas medidas preventiva establecidas por el hombre, organizaciones y sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, integridad y disponibilidad de la misma.

Esta actividad es un problema vigente para muchas organizaciones, es común encontrar en los medios informativos hechos o sucesos que tienen relación respecto a problemas de seguridad de la información en empresas de todo tipo y todo ámbito, por ejemplo, en Chile en el año 2008 en la prensa hablada y escrita se dio a conocer el caso del hackeo (alteración) de las bases de datos del estado chileno, dando cuenta de la publicación de los datos personales de más de 6 millones de chilenos, los cuales quedaron disponibles en un sitio de acceso público en internet. Este ejemplo muestra la vigencia y relevancia que tiene la seguridad de la información sobre todo para quienes tienen la responsabilidad de resguardarla, tenerla disponible, utilizable y segura. Estas son tareas directamente relacionadas con la plataforma de tecnología que posee una organización. (Mega, 2009)

- **A nivel nacional.**

Las tecnologías de la información han evolucionado de manera exponencial y su dependencia involucra la vulnerabilidad a ciertos tipos de amenazas como: espionaje, ciber ataques, sabotajes,

robo de dinero entre otros. Ante este contexto El Salvador no es la excepción, se encuentra inmerso en una era de la información y uso de las tecnologías en diversos ámbitos como la educación, la industria, la comercialización, entre otros, la información representa un bien invaluable que demanda seguridad. (Figueroa, Flores, & Samayoa, 2013).

Ante esta situación el Banco Central de Reserva de El Salvador en una publicación a través del periódico Diario el Mundo de El Salvador realizada el 21 de junio de 2016 la entidad manifiesta el interés de normar la seguridad de la información en el sistema financiero considerando que la información de los clientes debe ser protegida y ser recuperada de manera oportuna.

2.4.2. Seguridad de la información.

La información representa un recurso imprescindible para cualquier entidad, ya que forma parte integral del negocio en marcha de la misma, por lo cual las áreas tácticas de las organizaciones tienen el menester de administrarla y protegerla adecuadamente.

La seguridad de la información se puede definir según se detalla a continuación:

"Asegura que dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad)". (ISACA, 2012)

2.3.3. Importancia de la seguridad de la información.

El desarrollo de las telecomunicaciones, la integración de las operaciones en sistemas de informáticos, difusión en el uso de redes y equipos de cómputo y la digitalización de mucha información ha conllevado a que la seguridad se convierta en una actividad de gran relevancia en las organizaciones.

La seguridad de la información amplió su campo de acción, ya que paso de utilizarse para proteger datos confidenciales de los gobiernos relacionados a asuntos militares o diplomáticos, a tomar la dirección de transacciones financieras, acuerdos contractuales, documentos universitarios, estudios científicos, información personal, y cualquier forma de comercio electrónico; por lo que las necesidades de seguridad son aplicables a diversas presentaciones de la información. Este avance les ha permitido a las organizaciones desarrollar, integrar y gestionar sistemas de información con mayor capacidad de almacenamiento, procesamiento y funcionalidad; sin embargo, estos están expuestos a diversas amenazas internas y externas. (Areitio, 2008)

Gestionar eventos perjudiciales permite a los responsables de la seguridad tener un fundamento sustentable para presentar ante la alta gerencia la necesidad de un plan de inversión en seguridad de la información, el cual debe estar basado en evidencias y cálculos comprensibles que demuestren el impacto económico que puede ocasionar la materialización de un incidente, y que es posible diseñar con claridad las alternativas viables para la mitigación correctiva o preventiva de estos eventos no deseados, asegurando así, que la inversión disminuya o elimine las brechas de seguridad más relevantes y una medición de la efectividad de sus controles.

En la medida que las organizaciones en América Latina comenzaron a depender de las tecnologías de la información, fue evidente desarrollar prácticas de gestión para reducir los niveles de riesgos por las diversas amenazas que pudieran dañar el negocio en marcha. Este escenario es el efecto del aumento de los presupuestos asignados a áreas de seguridad. Además, que al menos el 42% de los encuestados visualizan la necesidad de adoptar un marco normativo de trabajo como ISO 27001, Biblioteca de Infraestructura de Tecnologías de Información (su acrónimo en inglés ITIL), Objetivos de control para la información y tecnologías relacionadas (su acrónimo en inglés COBIT) o alguna ley exigida por el país donde opera. (ESET Latinoamérica, 2016).

Con independencia del modelo de seguridad que una entidad implemente, es necesaria que la gestión de riesgos sea el parámetro para iniciar un proceso de gestión integral de la seguridad de la información, un valor muy importante para el logro de los objetivos empresariales y la mejora continua de la organización.

2.3.4. Objetivos globales de la seguridad de la información.

La finalidad de la seguridad de la información es posibilitar que las entidades logren cumplir con sus objetivos y estrategias, mediante la implantación de sistemas, controles o políticas que permitan gestionar los recursos de la entidad, y que tengan en consideración el análisis de riesgo de la organización y de sus partes interesadas. (Areitio, 2008)

A continuación, se presentan los objetivos que persigue la seguridad de la información en cualquier organización pública o privada:

- **Disponibilidad y accesibilidad:** es una propiedad que busca la seguridad de la información para permitirle estar a disposición y ser utilizada por la empresa cuando lo requiera o autorice.
- **Integridad:** significa proteger la información contra su modificación no idónea, además de asegurar la autenticidad de ésta.
- **Confidencialidad:** finalidad de la seguridad de la información para conservar las limitaciones relacionadas a su acceso o difusión, y los canales que protegen la privacidad.

2.3.5. Gestión de riesgo en la seguridad de la información.

La gestión del riesgo de seguridad de la información permite a una entidad poder evaluar los recursos que se intentan proteger, y representa un elemento de apoyo en identificar medidas de seguridad adecuadas. Una evaluación completa del riesgo de seguridad de la información permitiría a una organización evaluar sus necesidades y riesgos de seguridad en el plano de sus necesidades empresariales para el logro de los objetivos.

El objetivo de los sistemas de información y los datos que procesan es ayudar a los procesos de negocios, que simultáneamente apoyan la misión de la entidad.

- **Riesgo**

Basado en la metodología de evaluación de riesgos Evaluación Operacional Crítica de Activos, Amenazas y Vulnerabilidades (su acrónimo en inglés, OCTAVE), del Instituto de Ingeniería de Software de la Universidad Carnegie Mellon, el riesgo es: "La posibilidad de sufrir daños o pérdidas". La amenaza es un componente del riesgo, y se puede ser interpretado como: Un agente de amenazas, persona o un no humano, que ejecuta alguna acción, como identificar y explotar una vulnerabilidad, que conlleva a la generación de un resultado no adecuado y no deseado, como ejemplo la pérdida, modificación o divulgación de información, o la pérdida de acceso a la información. Estos resultados producen impactos perjudiciales en la organización, ya que pueden incluir: Pérdida de ingresos o clientes, pérdida de competencia en el mercado, los costos de respuesta y recuperación a raíz de una eventualidad no deseada, y el costo de pagar multas y sanciones regulatorias.

- **Componentes del riesgo de seguridad de la información**

El riesgo de seguridad de la información posee varios elementos relevantes:

a) **Agente de amenaza:** un ser humano o un objeto no humano que se aprovecha de una vulnerabilidad.
b) **Vulnerabilidad:** lo que explota el autor de la amenaza.
c) **Resultados:** el producto de explotar una vulnerabilidad.
d) **Impacto:** efectos perjudiciales de los resultadnos al explotar una vulnerabilidad.
e) **Activo:** el recurso afectado por el riesgo. Suponiendo que el activo en riesgo no puede ser suprimido, el único componente del riesgo de seguridad de la información que puede ser controlado es la vulnerabilidad.

2.3.6. Requerimientos para la seguridad de la información.

Los requerimientos de seguridad son los atributos que justifican la necesidad de proteger y administrar la integridad, confidencialidad y disponibilidad de la información, lo que con lleva a las organizaciones a definirlos adecuadamente.

Las tres fuentes de los requerimientos son las siguientes (ISO/IEC, 2007):

- **Evaluación de riesgos:** partiendo de los objetivos, la evaluación de riesgos permitirá reconocer las amenazas para los activos mediante la valoración de la vulnerabilidad, probabilidad de que se materialice el evento y el impacto que ocasionaría.
- **Regulaciones legales, estatutos o vínculos contractuales:** son aquellos requerimientos que parten de las obligaciones legales según el país donde opere, de los acuerdos de constitución o determinados en algún estatuto y por compromisos derivados de

contratos, todo esto con el objetivo de satisfacer las exigencias y necesidades de las partes de las partes interesadas (accionistas, contratistas, proveedores, clientes y empleados).

- **Requerimientos organizacionales:** son aquellos que establece la misma entidad para permitirse procesar la información y que pueda mantener su operatividad, entre los cuales se encuentran principios, normas internas, objetivos organizaciones y requerimientos comerciales.

2.4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El sistema de gestión de la seguridad de la información representa un conjunto de políticas, procesos, procedimientos y recursos que establece la alta dirección con el propósito de dirigir y controlar la seguridad de los activos que canalizan la información de la entidad, además asegurar la continuidad de las operaciones de la empresa (Barrantes Porras & Hugo Herrera, 2012). Comúnmente los sistemas de gestión para la seguridad de la información se abrevian como SGSI.

Esta metodología de gestión permite determinar políticas y procedimientos que van encaminados a cumplir con los objetivos de la organización, esto para mantener un bajo nivel de tolerancia al riesgo. Además, este sistema posibilitara conocer, aceptar, minimizar, trasferir o controlar de forma documentada, identificada y sistemática los diversos riesgos a los que es vulnerable la información (ISO/IEC, 2005).

La seguridad de la información estará garantizada por el SGSI a través de un compendio de buenas prácticas establecidas por (ISACA, 2014):

- Gestión de riesgos
- Políticas

- Procesos
- Procedimientos
- Controles
- Revisiones
- Mejoras

Un SGSI tiene la finalidad de proporcionar aseguramiento en el diseño de controles de seguridad para que gestionen adecuadamente los activos de información y generen confianza a las partes interesadas.

2.5.1. Ventajas y desventajas de un SGSI.

El SGSI es una herramienta que posibilita reducir los riesgos a un nivel mino en la organización, sin embargo, implementar esta metodología contrae beneficios y costos que se detallan a continuación (Henriquez, Herrera, & Lemus, 2016):

- **Ventajas**
  a) Establece una metodología de gestión de la seguridad estructurada y clara.
  b) Disminuye el riesgo de pérdida robo o manipulación de la información crítica.
  c) Los riesgos y controles son periódicamente monitoreados.
  d) Existe garantía y confianza frente a los pates interesadas de la entidad.
  e) Facilita la integración con otros sistemas de gestión.
  f) Garantiza la continuidad de las operaciones del negocio posterior a un incidente grave.
  g) Eleva el nivel de competitividad al protegerse contra daños que generen las amenazas.

h) Implementar un SGSI transforma la seguridad en una actividad de gestión de riesgos.

Entre los diversos aspectos adicionales que resultan mejorados son (Centro Europeo de Empresas e Innovación, 2010):

a) **Humano:** favorece la sensibilización de y responsabilidades del personal frente a la gestión de riesgos en la organización.
b) **Financiero:** disminución de los costos relacionados a los efectos provocados por eventos de seguridad
c) **Organizacional:** se demuestra la efectividad del esfuerzo realizado para desarrollar todos los niveles de la organización.
d) **Funcional:** se desarrolla un sistema de gestión de riesgos

- **Desventajas**

Desarrollar un SGSI es una sobrecarga al ritmo de trabajo normal en la organización, por lo que debe existir consciencia que este proceso exige o esfuerzo extra. Se muestra algunas desventajas que conlleva implementarlo:

a) **No puede abandonarse el proceso:** esto implica que el SGSI no debería pausarse o desistir de él, pues cuando se inicia el proceso lo ideal es llevarlo hasta que su continuidad sea normal; si se desiste en el proceso de implantación requerirá de un esfuerzo adicional para normalizar su desarrollo.
b) **Trabajo continuo:** con independencia de las tareas habituales que conlleva implementar el SGSI para los administradores de este, mantener el nivel logrado devengara de un esfuerzo continuo muy fuerte para todas las áreas de la organización.

2.5.2. Proceso del sistema de gestión de seguridad de la información.

La migración hacia el sistema de gestión de la seguridad de la información requiere de las siguientes etapas generales (ISO/IEC 27001:2013, 2013) (ISO Tools Excellence Perú, 2015):

- **Inicio del proyecto**: para este primer paso se requiere que la dirección de la entidad acepte el compromiso de comenzar con el SGSI, promoviendo un cambio de cultura y la preparación a su personal sobre los beneficios que producirá el sistema. Por lo cual, las entidades deben definir los aspectos internos y externos imprescindibles para lograr sus objetivos y contener los resultados de su SGSI, tener conocimiento y compresión de las necesidades y perspectivas de las partes interesadas, establecer el alcance del sistema. Luego, es necesario que la alta dirección establezca la política y objetivos de seguridad de la información siempre que sean congruentes con la estrategia organizacional y, finalmente, se deberán determinar las responsabilidades y roles vinculados al sistema., esto para lograr que el SGSI cumpla con los requerimientos de la normativa vigente e informa el su desempeño a la gerencia.
- **Planificación:** se establece el enfoque de evaluación de riesgos, ejecutar un inventario de activos de seguridad, detallando las vulnerabilidades y amenazas a las que se exponen, la probabilidad que una amenaza logre aventajarse de las deficiencias. Finalmente definir el plan de tratamiento del riesgo de seguridad del a información para seleccionar los controles adecuados
- **Soporte:** en esta parte del sistema la entidad necesita definir y proveer los recursos para establecerlo, implementarlo, darle mantenimiento y la mejora continua. Para lo cual debe disponer del personal capacitado y entrenado adecuadamente, que además deben tener conocimiento de la política de seguridad y los efectos que conlleva no cumplir los

requerimientos del sistema. También la entidad debe documentar su información bajo los requisitos de la NTS ISO/IEC 27001.

- **Evaluación del desempeño:** la entidad debe evaluar el desempeño de la seguridad de la información y la aplicación del SGSI, a través de métodos determinados por esta para garantizar autenticidad de los resultados. Por consiguiente, la organización debe realizar auditorías internas definidas de forma periódica para recaudar información relacionada al cumplimiento de los requisitos de la NTS ISO/IEC 35.68.01:14, y su adecuada implementación y mantenimiento. La dirección de la entidad tiene la responsabilidad de revisar continua y de forma planificada el SGSI que permita asegurar su continuidad, adaptación y efectividad, documentando cualquier mejora y necesidad de cambio.
- **Mejora Continua:** ante la necesidad de realizar un cambio en el sistema, la entidad debe implementar acciones para controlar y corregir el problema, analizando cada situación (su origen y sus efectos) y su acción correspondiente. La organización tiene que tener un plan de mejora continua, adaptación y efectividad del sistema, que le permita ejecutar cambios importantes cuando sea requerido.

2.6. NORMATIVA TÉCNICA APLICABLE

2.6.1. Norma Técnica Salvadoreña Tecnología de la Información. Técnicas de Seguridad, Sistemas de gestión de seguridad de la información. Requerimientos. (NTS ISO/IEC 27001:2013)

Es una norma que ha sido preparada para proporcionar los requerimientos mínimos de diseño de un sistema de gestión de la seguridad de la información dentro del contexto de una organización,

así mismo incluye requerimientos para la evaluación y tratamiento de riesgos de seguridad de la información de acuerdo a las necesidades de las organizaciones.

El sistema de gestión de seguridad de la información preserva, la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de procesos de gestión de riesgos y da confianza a las partes interesadas en que los riesgos son administrados de forma adecuada.

Es importante que el sistema de gestión de la seguridad de la información sea parte integra de los procesos de la organización y la estructura de administración completa y que la seguridad sea considerada en el diseño de procesos, sistemas de información y controles. El diseño del SGSI será realizado en concordancia con las necesidades de la organización y de acuerdo a los requisitos establecidos por la NTS ISO/IEC 27001:2013 tal como se especifica en la Tabla N°1, "Estructura de un sistema de gestión de seguridad de la información"

La NTS ISO/IEC 27001:2013 puede ser utilizada por entidades internas y externas para evaluar la habilidad de la organización para logro de sus propios requerimientos de seguridad de la información. Los requerimientos establecidos en la NTS son genéricos y tienen la intención de ser aplicables a todas las organizaciones, independientemente del tipo o tamaño o naturaleza.

Con el objetivo de darle cumplimiento a las directrices establecidas por la norma y para facilitar la comprensión y entendimiento de la misma, es necesario conocer la estructura general de un sistema de gestión de seguridad de la información, que se presenta en la tabla N° 1, la cual se debe diseñada a partir de la estructura de la NTS ISO/IEC 27001: 2013.

La exclusión de cualquier requerimiento especificado en los apartados 4 al 10 de la tabla "Estructura de un sistema de gestión de seguridad de la información" no es aceptable cuando una

organización declara conformidad con la NTS. Con el propósito de cumplir con lo establecido en los numerales 4 al 10 descritos por la norma y según la estructura de la tabla N°1, los cuales hacen referencia a los requisitos generales para el establecimiento e implementación de un SGSI y con la finalidad de interpretar lo establecido por la Norma Técnica Salvadoreña se aplican las definiciones siguientes:

- **Contexto de la organización:** determina la comprensión de la organización y su contexto, las necesidades y las expectativas de las partes interesadas y el alcance del sistema de seguridad de la información.
- **Liderazgo:** la importancia de mostrar un compromiso con respecto al sistema de gestión de seguridad de la información el establecimiento de políticas, roles, responsabilidades y autoridades organizacionales.
- **Planeación:** describe las acciones para abordador los riesgos y oportunidades de la seguridad de la información.
- **Soporte:** determinación de los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.
- **Operación:** establece la planeación y control operacional, realización de evaluaciones de riesgo de la seguridad de la información y el tratamiento al riesgo.
- **Evaluación del desempeño:** obtención de resultados a través del monitoreo, análisis y evaluación del desempeño y efectividad del sistema de Gestión de Seguridad de la Información
- **Mejora:** realización de monitoreo, medición, análisis y evaluación.

Tabla N° 1. Estructura de un sistema de gestión de seguridad de la información

APARTADO	TITULO
4	CONTEXTO DE LA ORGANIZACIÓN
4.1	Comprensión de la organización y su contexto
4.2	Comprensión de las necesidades y expectativas de las partes interesadas
4.3	Determinar el alcance del sistema de gestión de seguridad de la información
4.4	Sistema de gestión de seguridad de la información
5	LIDERAZGO
5.1	Liderazgo y compromiso
5.2	Política
5.3	Roles, responsabilidades y autoridades organizacionales
6	PLANEACIÓN
6.1	Acciones para abordar riesgos y oportunidades
6.2	Objetivo de seguridad de la información y planeación para lograrlos
7	SOPORTE
7.1	Recursos
7.2	Competencia
7.3	Conciencia
7.4	Comunicación
7.5	Información documental
8	OPERACIÓN
8.1	Planeación y control operacional
8.2	Evaluación del riesgo de seguridad de la información
8.3	Tratamiento de riesgo de seguridad de la información
9	EVALUACIÓN DEL DESEMPEÑO
10	MEJORA
10.1	No conformidad y acción correctiva
10.2	Mejora continua

Fuente: *NTS ISO/IEC 27001:2013*

2.7. LEGISLACIÓN APLICABLE

- **Leyes y reglamentos específicos.**

Los puestos de bolsa de El Salvador son regulados específicamente por la Ley de Bolsa de Productos, su respectivo reglamento y código de ética, los artículos relacionados a la problemática son los siguientes:

a) Ley de Bolsas de Productos y Servicios.

Tiene el objeto de regular la constitución, funcionamiento, limitaciones y prohibiciones que poseen las bolsas. (Art.1)

Es obligación de los puestos de bolsa y los licenciatarios el proporcionar información de clara, veraz y oportuna de sus actividades a la bolsa; así como también deberá proporcionarla a la SSF. Los registros que se realicen deben procurar la confianza de las operaciones mediante que estos sean claros, procuren la exactitud de las operaciones indicándose la información necesaria requerida por ley o el reglamento (Art. 21 literales d, e y f).

Entre las regulaciones antes citadas se encuentra como objeto los registros de las transacciones en las bolsas, los cuales deberán ser público y se inscribirán: los bienes y servicios que puedan negociarse en bolsas, los contratos con sus condiciones y requisitos de productos o servicios que puedan negociarse y los títulos representativos de derechos sobre productos o servicios. Así mismo indica que ante cualquier información falsa, alterada, simulada; y quienes divulgaren o revelaren hechos falsos, información maliciosa, simulen hechos o suministren información o datos con el propósito de confundir al público serán los responsables de los perjuicios o daños que estos causaren. (Art. 32, 33 y 37).

b) Reglamento general de la Bolsa de Productos de El Salvador.

El reglamento tiene como objetivos regular: el debido funcionamiento y la organización de la bolsa; procedimientos a través de los cuales se negocian; documentos, servicios, productos o instrumentos que la bolsa autorice, las actividades de aquellos participantes en el puesto de bolsa y las sanciones a imponerse a los agentes de bolsa o licenciatarios. (Art. 1).

Forma parte de las obligaciones de la bolsa y licenciatarios el llevar aquellos registros que fueren necesarios para mantener la transparencia y confianza de los negocios que intervienen, proporcionar la información de forma oportuna, clara y veraz que sea solicitada por la bolsa y la SSF, y suministrar a las autoridades pertinentes aquella información que sea requerida. (Art. 35, literales d, e y f). Es una sanción leve para los puestos de bolsa y licenciatarios el no informar o suministrar la información de forma completa o fuera del tiempo establecido, en que la haya solicitado la bolsa. (Art. 55, No.1).

Considera como sanción grave: la revelación de información confidencial de las transacciones y el suministro de datos o información falsa a la bolsa u otras entidades con la autoridad de exigirla. (Art. 59, No. 6 y 7). Así también es una infracción grave a los puestos de bolsa el suministro de información y datos falsos a sus clientes. (Art. 60, No. 4).

c) Código de Ética de la Bolsa de Productos de El Salvador.

El código tiene el objetivo de resguardar los principios y lineamientos fundamentales para los negocios que se realicen mediante la bolsa.

En relación a la seguridad de la información en la bolsa se regula dentro de los principios y valores a promover y resguardar, entre ellos el manejo de la información y el resguardo de esta;

donde los sujetos que posean información de carácter confidencial o privilegiada son responsables de salvaguardarla y a utilizarla exclusivamente en el desarrollo de sus actividades laborales. A demás deberá velarse para que dicha información no sea utilizada por terceros en beneficio propio o ajeno. (Art. 4, literales “h” e “i”).

Considera también que el encargado de la confidencialidad será del Gerente General, así como los empleados que este designe. El código considera como información confidencial como un activo empresarial y propia de las actividades del negocio y que por tanto no debe ser accesible al público, algunos ejemplos de este tipo de información son: los planes estratégicos, expedientes laborales o información de la clientela; y para conseguir asegurar el resguardo de esta por parte de los empleados de bolsa están obligados a firmar un contrato de confidencialidad. (Art. 5).

Se define a la información privilegiada como aquella que está vinculada con las actividades propias del negocio, de posesión exclusiva que es transmitida por los distintos empleados de la bolsa quienes deben utilizarla sin generarse ningún beneficio propio o causar daños o perjuicios a otros. Lo anterior tiene como objetivo que la información sea manejada y generada con sigilo y confianza, por tanto, queda prohibido para los empleados y demás personal el retirar documentos con información privilegiada de su área de trabajo o comunicarlo incluso de forma verbal a terceros no autorizados por Junta Directiva. Algunos ejemplos de este tipo de información son: las ofertas presentadas por la bolsa antes de su publicación, información personal sobre los oferentes y los procesos de compra/venta o aquella relativa a precios mínimos o máximos dentro de las pujas. (Art. 6).

- **Leyes generales.**

a) Código de Comercio

Regula aquellos comerciantes obligados a llevar contabilidad de forma organizada; conservando de forma ordenada la correspondencia y otros documentos probatorios, para ello podrán auxiliarse de sistemas electrónicos u otros medios técnicos para registrar contablemente las transacciones. (Art. 435).

Así mismo deberán conservarse la información has por diez años y cinco después de la liquidación de la entidad. (Art. 451). Para el almacenamiento de la información y documentos, los comerciantes pueden hacer uso de *microflim*, discos ópticos o cualquier medio que permita archivarla, de tal forma que los registros sean más eficientes. Cabe aclarar que el código determina que las copias generadas por estos medios tendrán el mismo valor probatorio siempre que estén certificadas por un notario. (Art. 455).

b) Código Tributario

Regula la obligación de quienes deben lleva contabilidad formal, información que debe tener orden cronológico, debe ser completa y oportuna; no debe estar modificada de tal forma que resulte incierto determinar si han sido hechas con posterioridad u originalmente; y las partidas deberán poseer la documentación de soporte de manera que soporten las distintas transacciones. (Art. 139). El código establece que existe una obligación de conservar información y pruebas por un periodo de diez años, si esta fuera conservada de forma computarizada puede hacerse uso de medios magnéticos, así como documentos que se resguarden por medio de sistemas tales como microfichas o *microflim*. (Art. 147).

CAPÍTULO III-METODOLOGÍA DE LA INVESTIGACIÓN

3.1. ENFOQUE Y TIPO DE INVESTIGACIÓN

Para la investigación se utilizó el método hipotético-deductivo, debido a que este método permite detallar las características del problema en la gestión de la seguridad de la información que se presentan en la mayoría de los puestos de bolsa de productos y servicios, para ello se emplearon encuestas con las que se recolectó los datos, que fueron analizados para la comprobación de hipótesis.

3.2. DELIMITACIÓN ESPACIAL Y TEMPORAL

3.2.1. Espacial.

La delimitación espacial comprende la ubicación de los ocho puestos de bolsa existentes hasta la fecha, cuyos domicilios se encuentran en los municipios de San Salvador y Antiguo Cuscatlán.

3.2.1. Temporal.

El período en el que se realizó la investigación está comprendido desde el año 2014, debido a que ese año se adoptó la Norma Técnica Salvadoreña ISO/IEC 27001: 2013 por el Organismo Salvadoreño de Normalización que establece los requerimientos necesarios para el diseño e implementación de un sistema de gestión de la seguridad de la información.

3.3. SUJETOS Y OBJETO DE ESTUDIO

3.3.1. Unidades de análisis.

Para esta investigación, las unidades de análisis fueron los gerentes de los ocho puestos de bolsa de productos y servicios que operan en los municipios de San Salvador y Antiguo Cuscatlán.

3.3.2. Población y marco muestral.

Como fue citado en el apartado anterior, se cuenta con un universo finito; por tanto, la muestra es igual al universo, es decir los ocho puestos de bolsa de productos y servicios establecidos en El Salvador.

3.3.3. Variables e indicadores.

Las variables de la hipótesis de la investigación son las siguientes:

- **Variable dependiente:** información integra, confidencial y disponible.
- **Variable independiente:** sistema de gestión de seguridad de la información basado en la NTS ISO/IEC 27001: 2013.

En cuanto a los instrumentos de investigación se utilizó la técnica de la encuesta para garantizar la obtención de información en los puestos de bolsa de productos y servicios de El Salvador.

3.4. TÉCNICAS, MATERIALES E INSTRUMENTOS

3.4.1. Técnicas y procedimientos para la recopilación de la información.

Se utilizó la encuesta para la obtención de información por parte de los puestos de bolsa de productos y servicios que demuestren la perspectiva de la problemática de manera que se pudiera realizar un estudio a través de los datos cuantitativos obtenidos, utilizándolos para su posterior análisis, con la finalidad de determinar el comportamiento y posibles soluciones del problema.

3.4.2. Instrumentos de medición.

El instrumento de medición utilizado fue el cuestionario, el cual se realizó con la finalidad de recolectar datos sobre la gestión de la seguridad en la información sobre tres objetivos:

disponibilidad, confidencialidad e integridad de la información física y digital que procesan los puestos de bolsas de productos y servicios de El Salvador (ver anexo N° 1).

3.5. PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

La información obtenida mediante las encuestas fue procesada mediante de una hoja de cálculo de Microsoft Excel, en la cual se vertieron lo datos obtenidos para formar una tabulación donde se determinó la frecuencia absoluta y relativa, para una mejor comprensión de las respuestas de las cuales dichos estadísticos, acompañados de una representación gráfica y su respectivo análisis e interpretación de resultados.

También se utilizó el software *IBM SPSS Statistics 22* para efectuar un cruce de variables provenientes de las respuestas de la encuesta, que brindarán una mayor comprensión del estado de la problemática relacionada a la seguridad de la información dentro de los puestos de bolsa de productos y servicios de El Salvador.

De cada una de las preguntas y sus gráficos y tablas, se determinará un respectivo análisis y conclusión, que se detallan en el diagnóstico de la investigación; el cual fue construido mediante el cruce de distintas variables que integra las preguntas de la encuesta, agrupadas en tres áreas: confidencialidad, disponibilidad e integridad de la información en los puestos de bolsas y servicios de El Salvador.

3.6. CRONOGRAMA DE ACTIVIDADES

Tabla N° 2. Cronograma de actividades del SGSI

TRABAJO DE INVESTIGACIÓN ACTIVIDADES	MESES /2017																																			
	FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE			
	Semanas				Semanas				Semanas				Semanas				Semanas				Semanas				Semanas				Semanas				Semanas				Semanas			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Inicio del seminiario de graduación																																								
Desarrollo del anteproyecto																																								
Elaboracion del capitulo I																																								
Correcciones al cápitulo I																																								
Entrega de cápitulo I																																								
Elaboracion del capitulo II																																								
Correccion del cápitulo II																																								
Entrega del cápitulo II																																								
Elaboracion del Capitulo III																																								
a. Determinacion de las unidad de análisis																																								
b. Determinacion del universo y muestra																																								
c. Elaboracion de encuestas																																								
d. Aprobacion de encuestas																																								
e. Recolección de la informacion																																								
f. Procesamiento de la información																																								
g. Análisis e interpretación de los datos procesados																																								
h. Diagnóstico de la investigación																																								
i. Formulación de hipótesis																																								
Correcciones al cápitulo III																																								
Entrega del cápitulo III																																								
Elaboracion del cápitulo IV																																								
Desarrollo del la propuesta: Caso práctico																																								
Correcciones al cápitulo IV																																								
Entrega del cápitulo IV																																								
Finalizacion de la investigación																																								
Preparación para exposición y defensa																																								
Presentacion y defensa																																								

3.7. PRESENTACIÓN DE RESULTADOS

3.7.1. Tabulación y análisis de resultados.

Tabla N° 3. Cruce de preguntas 8 y 16.

Cruce Preguntas N° 8 y N° 16				
Preguntas cruzadas		16) Si se diseñara un Sistema de Gestión de Seguridad de la Información personalizado para los puestos de bolsa de productos y servicios ¿le sería atractivo implementarlo para mejorar la integridad, confidencialidad y disponibilidad de la información que se procesa en la organización?		**Total**
		Si	No	
8) ¿Qué controles aplican en el puesto de bolsa para mantener la integridad de la información?	Modificación solo mediante personal autorizado	5 71.4%	1 14.3%	**6** **85.7%**
	Registro de actividades y eventos	1 14.3%	0 0.0%	**1** **14.3%**
	Controlar el acceso físico a los equipos y componentes de la red	3 42.9%	0 0.0%	**3** **42.9%**
	Control para resguardo de los dispositivos de almacenamiento	3 42.9%	0 0.0%	**3** **42.9%**
	Actualizaciones del sistema operativo	1 14.3%	0 0.0%	**1** **14.3%**
	Antivirus y firewall	3 42.9%	1 14.3%	**4** **57.1%**
	Restricción de accesos a programas y archivos	1 14.3%	0 0.0%	**1** **14.3%**
Total		**6** **85.7%**	**1** **14.3%**	**7** **100.0%**

Fuente: *Encuestas realizadas a puestos de bolsa*

Cruce de preguntas 8 y 16. seis de siete puestos de puestos de bolsa de productos y servicios de El Salvador manifestaron estar interesados en la propuesta del diseño de un sistema de gestión de la seguridad de la información que proteja la integridad de los datos procesados. Al cruzar las variables de la pregunta ocho y la dieciséis, se detecta que los controles más utilizados son: solo personal autorizado puede modificar la información, el acceso limitado a equipos, componentes de la red, uso de antivirus y firewall, y aquellos destinados al resguardo de dispositivos de

almacenamiento. En el cuestionario se tenían diez opciones de controles, donde solo uno de los siete manifestó aplicar: el registro de actividades y eventos y las constantes actualizaciones del sistema operativo; evidenciando así las entidades necesitan de un SGSI para gestionar de manera adecuada la integridad de dicho recurso.

Tabla N° 4. Cruce de preguntas 8 y 10

Cruce Preguntas N° 8 y N° 10							
Preguntas cruzadas		10) ¿Cuáles son los métodos utilizados para la protección de la documentación física?					**Total**
		Almacenamiento con sistemas biométricos	Clasificación de la información en base a la confidencialidad y susceptibilidad de la misma	Autorización de acceso para el personal para el uso y manejo de la información	Verificación de controles para las requisiciones de información	No utilizan ningún método	
8)¿Qué controles aplican en el puesto de bolsa para mantener la integridad de la información?	Modificación solo mediante personal autorizado	1 14.3%	2 28.6%	3 42.9%	2 28.6%	1 14.3%	**6** **85.7%**
	Registro de actividades y eventos	1 14.3%	1 14.3%	1 14.3%	1 14.3%	0 0.0%	**1** **14.3%**
	Controlar el acceso físico a los equipos y componentes de la red	0 0.0%	0 0.0%	1 14.3%	2 28.6%	1 14.3%	**3** **42.9%**
	Control para resguardo de los dispositivos de almacenamiento	1 14.3%	1 14.3%	3 42.9%	2 28.6%	0 0.0%	**3** **42.9%**
	Actualizaciones del sistema operativo	1 14.3%	1 14.3%	1 14.3%	1 14.3%	0 0.0%	**1** **14.3%**
	Antivirus y firewall	1 14.3%	1 14.3%	3 42.9%	2 28.6%	1 14.3%	**4** **57.1%**
	Restricción de accesos a programas y archivos	0 0.0%	0 0.0%	1 14.3%	1 14.3%	0 0.0%	**1** **14.3%**
Total		**1** **14.3%**	**2** **28.6%**	**4** **57.1%**	**3** **42.9%**	**1** **14.3%**	**7** **100.0%**

Fuente: *Encuestas realizadas a puestos de bolsa*

Cruce de preguntas 8 y 10. los puestos de bolsas de productos y servicios de El Salvador hacen uso de controles de accesos a la información física para que está resguarde su integridad, de los controles más utilizados se tienen: la modificación de los datos solo por personal autorizado que como se observa en la tabla del cruce de variables un 28.6% de la población verifica dicho control y respecto a los accesos en la pregunta diez coincide que un 42.9% de la población restringe los accesos del personal para evitar un uso o manejo inadecuado del activo. Sin embargo, uno de los siete puestos de bolsa manifestó en la pregunta diez que no utilizan ningún tipo de método para la protección de la documentación física. Los demás controles descritos en ambas interrogantes se observaron una baja aplicación por las entidades, evidenciando la carencia de modelos de controles que cuenten con la suficiente madurez para velar por la protección de la integridad de los datos y documentación física que poseen los puestos.

Tabla N° 5. Cruce preguntas 1 y 9.

Cruce Preguntas N° 1 y N° 9				
Preguntas cruzadas		1) En la entidad ¿Se tienen accesos limitados a la información de acuerdo a las funciones de cada uno de los empleados?		**Total**
		Si	No	
9) ¿Cuál es la forma en que la organización informa a los usuarios sobre restricciones de uso de información confidencial?	Contratos de confidencialidad	3 42.9%	1 14.3%	**4** **57.1%**
	No existe un medio de información	1 14.3%	0 0.0%	**1** **14.3%**
	Política de confidencialidad de la información	3 42.9%	0 0.0%	**3** **42.9%**
	Segregación de funciones	2 28.6%	0 0.0%	**2** **28.6%**
Total		**6** **85.7%**	**1** **14.3%**	**7** **100.0%**

Fuente: *Encuestas realizadas a puestos de bolsa*

Cruce de preguntas 1 y 9. el 85.7% de los siete de los gerentes de los puestos de bolsas de productos y servicios encuestados manifestó que en la entidad se cuentan con accesos limitados para los empleados de acuerdo con lo que requieren sus funciones; donde tres de los siete puestos cuentan: con una política de información que es comunicada y contratos de confidencialidad al momento de la contratación de su personal. Un 28.6% de las entidades cuenta con una segregación de funciones para evitar así la fuga de información y la modificación de esta; porcentaje que aún resulta muy pequeño para concluir que las entidades gestionan de forma adecuada la seguridad del activo.

Tabla N° 6. Cruce de preguntas 6 y 7.

Cruce Preguntas N° 6 y N° 7				
Preguntas cruzadas		6) ¿Realiza respaldos de las bases de datos de los sistemas informáticos de forma manual o automática?		**Total**
		Manual	Automático	
7) ¿Cuáles son los medios y/o lugares de almacenamiento para el resguardo de la información digital propia y de terceros?	Disco duro externo	3 42.9%	2 28.6%	**5** **71.4%**
	Alojamiento web	1 14.3%	1 14.3%	**2** **28.6%**
	Servidores en red	2 28.6%	0 0.0%	**2** **28.6%**
	Correo electrónico	3 42.9%	0 0.0%	**3** **42.9%**
	Ninguna de las anteriores	0 0.0%	1 14.3%	**1** **14.3%**
Total		**4** **57.1%**	**3** **42.9%**	**7** **100.0%**

Fuente: *Encuestas realizadas a puestos de bolsa*

Cruce preguntas 6 y 7. con este cruce se realizó con la finalidad de comprender la manera en que se realizan los respaldos y donde son almacenados por los puestos de bolsa de productos y servicios de El Salvador obteniéndose los siguientes resultados: el 57% de las entidades realiza los respaldos de forma manual de los cuales un 42% los aloja en un disco duro externo, un 14% en la web, un 28.6% en servidores en red y un 42% en correos electrónicos. Por otra parte, un 42.9% realiza sus respaldos de forma automática; donde un 28.6% los almacena en un disco duro externo, un 14% en alojamiento web y otro 14% no los almacena en ninguna de las opciones presentadas en la encuesta. De lo cual se concluye que el porcentaje de entidades que los realiza de forma manual es casi la mitad de la población que se encuentra vulnerable a que la información no se encuentre disponible ante un evento de pérdida de datos que pudiese ocurrir.

Tabla N° 7. Cruce preguntas 13 y 16.

Matriz Cruce Preguntas N° 13 y N° 16				
Preguntas cruzadas		16) Si se diseñara un Sistema de Gestión de Seguridad de la Información personalizado para los puestos de bolsa de productos y servicios ¿le sería atractivo implementarlo para mejorar la integridad, confidencialidad y disponibilidad de la información que se procesa en la organización?		**Total**
		Si	No	
13) ¿Cuál sería el plan de acción para recuperar la información perdida a causa de un siniestro?	Recuperación mediante correos electrónicos	6 85.70%	0 0.00%	**6** **85.70%**
	Respaldos de dispositivos a otros dispositivos (terminales, discos duros externos)	2 28.60%	0 0.00%	**2** **28.60%**
	Respaldos en alojamiento web	2 28.60%	0 0.00%	**2** **28.60%**
	Se le solicita al cliente de nuevo	2 28.60%	0 0.00%	**2** **28.60%**
	Mediante un servidor externo	0 0.00%	1 14.30%	**1** **14.30%**
	Se regenera de la documentación física (en caso la pérdida fuera digital)	3 42.90%	0 0.00%	**3** **42.90%**
Total		**6** **85.70%**	**1** **14.30%**	**7** **100.00%**

Fuente: *Encuestas realizadas a puestos de bolsa*

Cruce preguntas 13 y 16. con este cruce se pretende comprender la necesidad de un SGSI de las entidades tras un posible siniestro de fuga de datos versus el interés que los gerentes mostraron ante el desarrollo de la propuesta del presente trabajo de investigación. De las medidas a tomar por el 85.7% los gerentes es la recuperación de la información mediante correos electrónicos estando a su vez interesados en el diseño del sistema. Sin embargo, otras medidas para afrontar el siniestro como recuperar los datos mediante un respaldo almacenado en un servidor externo fue señalada por solo un gerente de los puestos de bolsa de productos y servicios. De lo anterior puede concluirse que las entidades no se encuentran debidamente preparadas ante un evento de fuga de datos que afecte la disponibilidad de la información.

3.7.2. Diagnóstico de los resultados.

Mediante la recolección de datos a través la encuesta que fue contestada por cada uno de los gerentes de siete de ocho puestos de Bolsa de El Salvador, se procede a identificar tendencias del comportamiento dentro de las entidades respecto a los controles establecidos para resguardar la información que procesan en tres aspectos: disponibilidad, confidencialidad e integridad; áreas en las que se realiza la siguiente agrupación de los resultados obtenidos con la finalidad de conocer las necesidades de los puestos de bolsa de productos y servicios para obtener un SGSI a través de un diagnóstico.

Confidencialidad.

Es importante resguardar la confidencialidad de la información dentro de los puestos de bolsas de productos y servicios, y con la finalidad de conocer si dichas entidades implementan controles adecuados para cuidar de ella, se procede a diagnosticar los siguientes resultados:

Uno de los controles implementados es el acceso limitado de los empleados o a la información respecto a cada una de sus funciones; el cual es implementado por el 86% de las entidades. Tal restricción es informada a los empleados de la siguiente manera: un 43% utiliza una política de confidencialidad de la información, un 57% realiza una segregación de funciones, el 14% considera no tener accesos limitados y el mismo porcentaje no cuenta con un medio para informar tales restricciones.

Otros aspectos relevantes son los medios que se utilizan para transferir información de los clientes, obteniéndose los siguientes porcentajes: mediante correo electrónico y entrega personal de documentos un 57% y un 14% hace uso del envío por correspondencia el cual acarrea un riesgo mayor al exponer la información en manos de un tercero. Considerándose por consiguiente

controles implementados al acceso que terceras personas puedan tener a la información; donde la gran mayoría en un 86% hace uso de controles para el acceso de los visitantes a las instalaciones, un 43% de las entidades cuenta con sistemas de video vigilancia, personal de vigilancia y sistema de alarmas; y una pequeña minoría del 14% representado por un solo puesto de bolsa hace uso de tecnología biométrica para el acceso a las instalaciones.

Es importante conocer los métodos para la protección de la información física utilizada donde el 57%, una clasificación de la información por su confidencialidad y susceptibilidad, el 43% cuenta con autorización de acceso y uso para el personal de la información, un 29% realiza requisiciones de los controles implementados para la protección de dicha información y un 14% no cuenta con un método alguno para protegerla.

Concluyendo que, mediante los resultados obtenidos de la encuesta, se determina que los puestos de bolsa de productos y servicios posee controles que contribuyen al resguardo de la confidencialidad de la información, sin embargo, son controles que carecen de madurez y una mejora continua que puede mejorarse mediante un sistema de gestión de seguridad de la información.

Con la finalidad de obtener una mejor comprensión del diagnóstico vinculado con la problemática respecto a la confidencia, tomar como referencia el detalle de la tabla N° 8.

Tabla N° 8. Confidencialidad de la información de los puestos de bolsa

Pregunta	Criterio	Alternativa	Frecuencia absoluta	Frecuencia Relativa
1	Accesos limitados a la información	Sí	6	86%
		No	1	14%
9	Medios para informar las restricciones al acceso a la información	Política de confidencialidad de la información	3	43%
		Contratos de confidencialidad	4	57%
		Segregación de funciones	2	29%
		Disponibilidad de manuales de información relevante	0	0%
		No existe un medio de información	1	14%
2	Medios para transferir información de clientes	Correo electrónico	4	57%
		Dispositivo extraíble posteriormente enviado por correspondencia	0	0%
		Dispositivo extraíble entregado personalmente	0	0%
		Envío de documentos físicos mediante correspondencia	1	14%
		Entrega personal de documentos físicos	4	57%
4	Acceso por terceros a la información física	Cuenta con video vigilancia	3	43%
		Sistemas de accesos biométrica	1	14%
		Sistema de alarmas	3	43%
		Personal de vigilancia	3	43%
		Controles de acceso a visitantes	6	86%
10	Métodos para la protección de la documentación física	Almacenamiento con sistemas biométricos	1	14%
		Clasificación de la información en base a la confidencialidad y susceptibilidad de la mismo	4	57%
		Autorización de acceso para el personal para el uso y manejo de la información	3	43%
		Verificación de controles para las requisiciones de la información	2	29%
		No utilizan un método	1	14%

Fuente: *(Henríquez de Guzmán, Herrera Rivera, & Lemus Campos, 2016)*

Integridad.

Según los resultados obtenidos, respecto a cómo los puestos de bolsa gestionan la integridad de la información, se puede determinar que a pesar de mantener varios controles, la mayoría va encaminado a resguardar la información física prioritariamente, tomando poca importancia a la información digital, ya que ninguno practica la criptografía de datos, solo el 14 % de los puestos de bolsa realiza actualizaciones a los sistemas operativos de las computadoras, cerca del 43% (no es ni la mitad) utiliza un programa de antivirus y un poco más de la mitad aún no ha automatizado el proceso de los respaldos de sus bases de datos de los sistemas informáticos que utiliza, ya que lo hacen manualmente. También es necesario destacar que el 86% realiza mantenimientos a los sistemas informáticos, pero según lo descrito anteriormente, no pareciera existir un ciclo de mejora continua respecto a la integridad de la información digital. Las causas de esto podría ser el desconocimiento de las algunas amenazas, nunca han sufrido una pérdida significativa de documentos digitales y no han sido blancos de software malicioso (pues solo el 14% ha sufrido un ataque de este tipo), lo cual no genera el interés de proteger la integridad.

El control de la documentación física mediante la autorización del uso y manejo de esta por parte de los empleados es la segunda opción más utilizada por los puestos de bolsa (con un 43%), pero su integridad se ve vulnerada cuando entra en contacto con los usuarios de la información debido a que los errores humanos, en la manipulación de esta, es la principal causa de su pérdida o modificación no autorizada. Según lo anterior, considerando que el 86% de los puestos limita la información a los empleados según su rol, es necesario implantar medidas y procesos organizados que permitan controlar adecuadamente la gestión de los documentos físicos y digitales por parte de los usuarios, evitando que se alteren sin autorización. Para mayor detalle, ver tabla N° 9 “Integridad del a información de los puestos de bolsa”

Tabla N° 9. Integridad de la información de los puestos de bolsa

Pregunta	Criterio	Alternativas	Frecuencia Absoluta	Frecuencia Relativa
No. 1	Acceso limitado a la información	Si	6	86%
		No	1	14%
No. 2	Mantenimiento a sistemas informáticos	Si	6	86%
		No	1	14%
No. 6	Respaldos de bases de datos	Manual	4	57%
		Automática	3	43%
		Modificación mediante personal autorizado	7	100%
		Criptografía de datos	0	0%
		Registro de actividades y eventos	1	14%
		Control acceso físico a equipos	4	57%
		Firma digital	0	0%
No. 8	Controles para mantener la integridad de la información	Resguardos de dispositivos de almacenamiento	3	43%
		Actualizaciones de sistemas operativos	1	14%
		Antivirus y firewall	4	57%
		Restricción de acceso a programas y archivos	2	29%
		Restricción de ubicación y horario	0	0%
		No aplican	0	0%
		Sistemas biométricos	1	14%
No. 10	Métodos para protección de documentos físicos	Clasificar información según su confidencialidad	4	57%
		Manejo solo a personal autorizado	3	43%
		Control de requisición de documentos	2	29%
		No utilizan	1	14%
No. 12	Causas de pérdida de la información	Software malicioso	1	14%
		Falla de equipos	2	29%
		Falla de software instalado	2	29%
		Robo o hurto	0	0%
		Fenómenos naturales	0	0%
		Errores humanos	5	71%

Fuente: *(Henríquez de Guzmán, Herrera Rivera, & Lemus Campos, 2016)*

Disponibilidad.

De acuerdo a los resultados obtenidos se determinó que a pesar de que existen diferentes mecanismos de resguardo y medidas de seguridad para mantener la disponibilidad de la información y en su mayoría son practicadas por los distintos puestos de bolsas de productos y servicios, existe un porcentaje significativo que no hace uso correspondiente de tales medidas ya sea por falta de una cultura de seguridad o simplemente por desconocimiento o desinterés de resguardar y proteger tan valioso recurso, lo mencionado anteriormente tiene sus efectos en relación al mantenimiento que se le debe dar a los sistemas informáticos donde es procesada la información, aunque en su mayoría los puestos de bolsas representado por el 86% prestan la debida atención al constante mantenimiento que deben recibir los sistemas informáticos, un 14% se expone al riesgo de perder dicho recurso por la vulnerabilidad que existe de exponer este tipo de activo a los a ataques de virus por no brindar un mantenimiento a sus sistemas informáticos o por incidentes de seguridad provocados de forma voluntaria o involuntariamente (desastres naturales), que conllevaría al daño de los sistemas informáticos y por consiguiente a la perdida de información, a pesar de que un 43% de los puestos de bolsa generan copias de respaldo de sus bases de datos de forma automática existe la amenaza de que un 57% no garanticen la disponibilidad de la información ya que las copias de respaldo son generas de forma manual esto significa que ocasiones esta buena práctica puede ser olvida por el personal asignado para ejecutarla. Un aspecto muy importante a mencionar es que solamente el 43% de los puestos de bolsa brinda la debida protección de la documentación física a través de la asignación de personal excluso para el uso y manejo de la información esto quiere decir que en su mayoría el 57% es vulnerable a la perdida, robo o extravío de dicha información por el hecho de no contar con un personal encargado de vigilar, supervisar y proteger tal recurso, por lo tanto es importante el

establecimiento de una cultura de seguridad y la concientización por parte de los puestos de bolsa que no aplican medidas de seguridad, para que resguarden y protejan la información y pueda estar disponible en el momento oportuno. Para una mayor especificación ver tabla N° 10.

Tabla N° 10. Disponibilidad de la información de los puestos de bolsa

Pregunta	Criterio	Alternativas	Frecuencia Absoluta	Frecuencia Absoluta
No. 2	Medios de transferencia de información	Correo electrónico	4	57%
		Dispositivo extraíble posteriormente enviado por correspondencia	0	0%
		Dispositivo extraíble entregado personalmente	0	0%
		Envío documentos físicos mediante correspondencia	1	14%
		Entrega personal de documentos físicos	4	57%
No. 5	Mantenimiento a sistemas informáticos	Si	6	86%
		No	1	14%
No. 6	Respaldos de bases de datos	Manual	4	57%
		Automática	3	43%
No. 7	Medios de almacenamiento para el resguardo de la información	Disco duro externo	5	71%
		Alojamiento Web	1	14%
		Servidores en Red	4	57%
		Correo electrónico	2	29%
		Ninguna de las anteriores	1	14%
		Almacenamiento con sistemas biométricos	1	14%
No. 10	Métodos de protección de la documentación física	Clasificación de la información en base a la confidencialidad y susceptibilidad de la mismo	4	57%
		Autorización de acceso para el personal para el uso y manejo de la información	3	43%
		Verificación de controles para las requisiciones de la información	2	29%
		No utilizan un método	1	14%

		Respaldos de la información digital en un alojamiento web.	2	28.57%
		Autorización de personal clave.	3	42.86%
No. 11	Controles para mantener la disponibilidad de la información	Mantenimiento y mejoras de hardware y software que se utiliza	2	28.57%
		Verificación continua de los servidores.	3	42.86%
		Monitoreo constante de bodegas de almacenamiento de información física	3	42.86%
		No implementan controles.	0	0%
		Recuperación mediante correos electrónicos	1	14%
		Respaldos de dispositivos otros dispositivos (terminales, discos duros externos)	5	71%
No. 13	Recuperación de la información	Respaldos en alojamiento web	3	43%
		Se le solicita al cliente de nuevo	2	29%
		Mediante un servidor externo	2	29%
		Se regenera de la documentación física (en caso la pérdida fuera digital)	4	57%

Fuente: *(Henríquez de Guzmán, Herrera Rivera, & Lemus Campos, 2016)*

Se concluye con base en lo descrito anteriormente que no existe una cultura de seguridad que le permita a los puestos de bolsa gestionar adecuadamente la información que procesan.

CAPÍTULO IV-SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PUESTOS DE BOLSA DE PRODUCTOS Y SERVICIOS.

4.1. PLANTEAMIENTO DEL CASO.

La presente propuesta consiste en el diseño de un sistema de gestión de seguridad de la información basado en la Norma Técnica Salvadoreña ISO/IEC 27001:2013 Sistema de gestión de seguridad de la información, que tiene por finalidad gestionar la integridad, confidencialidad y disponibilidad de la información.

Las organizaciones junto a sus sistemas de información se encuentran expuesto cada vez más a cierto tipo de amenazas que se valen de la vulnerabilidad existente para poner en riesgo este valioso recurso y para IBES, S.A. no es la excepción ya que se encuentra expuesta a diversos riesgos de sufrir algún tipo de incidente de seguridad provocado de forma voluntaria o involuntariamente que puede ser generado desde la propia organización o de forma externa o aquellos provocados accidentalmente como los desastres naturales o fallas técnicas.

Al ser conscientes que en muchas ocasiones los niveles de seguridad alcanzados gracias a los medios tecnológicos son insuficientes y con la finalidad de tener una gestión más efectiva de la seguridad de la información surge la necesidad de proteger tal activo mediante el diseño de un SGSI donde se espera tenga participación toda la organización, con la alta dirección de IBES, S.A. de C.V., liderando y teniendo en cuenta la intervención de las partes interesadas.

El SGSI contempla una adecuada estructura y planificación mediante la implementación de controles basados en la evaluación de riesgos; el sistema de gestión ayudará a través del establecimiento de una política alineada a los objetivos estratégicos del negocio a mantener un

nivel de seguridad aceptable y un nivel de exposición al riesgo menor e incluso al que la propia entidad ha decidido asumir. El diseño del SGSI consta de tres fases:

- **Fase 1. Conocimiento de la entidad y su entorno**: esta fase consiste básicamente en realizar un estudio y análisis del ambiente interno como externo y determinar fortalezas, debilidades, cuestiones legales, contractuales y económicas que puedan afectar la imagen corporativa de la entidad.

- **Fase 2. Asignación de Responsabilidades y liderazgo:** un SGSI donde no se establecen claramente la asignación de roles y responsabilidades no será eficaz y por lo tanto la documentación y sus controles tampoco lo serán, con el objetivo de evitar tal inconsistencia este apartado requiere del apoyo y la participación de la Alta Dirección en la gestión de seguridad mostrando una actitud de liderazgo en la asignación de responsabilidades y tener claro que la autoridad se establece bajo condiciones de rendición de cuentas en los diferente niveles organizacionales y además estar conscientes y seguros que los roles se asignen, se comuniquen y se entiendan en toda la organización .

- **Fase 3. Planificación.** basado en los requerimientos normativos esta fase consiste en identificar las amenazas a las cuales se exponen los activos de información y la probabilidad que el riesgo se materialice basado en ese contexto en este apartado también se desarrollan las formas apropiadas de la gestión de riesgo y reducirlos a un nivel aceptable.

4.2. ESTRUCTURA DEL PLAN DE SOLUCIÓN.

La estructura del SGSI se presenta en la figura N°1 la cual como se explicó en el capítulo II, se basa utilizando la estructura de la NTS ISO/IEC 27001:2013.

Figura N°1. Estructura del proyecto del SGSI.

Fuente: *NTS ISO/IEC 27001:2013*

4.3. BENEFICIOS Y LIMITANTES.

La propuesta del sistema de gestión de la información basado en la NTS ISO/IEC 27001:2013 beneficiará a los puestos de bolsa de productos y servicios en los siguientes aspectos:

- Reducirá el riesgo de que se produzcan pérdidas de información; conservando así su integridad y confidencialidad, ya que se realiza una evaluación continua de ellos.
- El SGSI otorga a los puestos de bolsa y servicios, una garantía frente clientes, socios estratégicos y las entidades regularizadoras (BOLPROS y SSF), debido a que muestra

a la misma como un organismo preocupado por la confidencialidad y seguridad de la información que es depositada en la misma; como lo establece la ley de los puestos de bolsa de productos y servicios.

- La seguridad en la información que ofrece implantar un SGSI de acuerdo a NTS ISO/IEC 27001:2013, contribuye a una reducción de los costos y una mejoría de los procesos.

Existe una relevante limitante en la propuesta del SGSI para los puestos de bolsa de productos y servicios de El Salvador, puesto que para seguir el modelo completo del sistema es necesario su implantación y mejora continua; fases que por motivos de factibilidad no fueron ejecutadas, concluyendo la propuesta hasta la planificación de este.

4.4. DESARROLLO DE CASO PRÁCTICO.

Sistema de Gestión de Seguridad de la Información de Intermediarios Bursátiles de El Salvador, S.A. de C.V.

Índice del SGSI

Índice de tablas del SGSI

Índice de figuras del SGSI

FASE 1. CONTEXTO DE LA ORGANIZACIÓN

1.1. COMPRENSIÓN DE LA ORGANIZACIÓN

1.1.1. Naturaleza de la entidad.

La sociedad Intermediarios Bursátiles de El Salvador, S.A. de C.V., Puesto de Bolsa de Productos y Servicios (en adelante IBES, S.A. de C.V. o solo IBES), fue constituida el 5 de enero de 2005, de conformidad con las leyes mercantiles de la República de El Salvador, cuando un grupo de empresarios ven la necesidad de intervenir en un mercado creciente y emprendedor en cuanto a la representación de entidades privadas e instituciones del Estado para la transacción de bienes y servicios. Inicialmente se realizaron reuniones de acercamiento para conocer de forma inmediata los beneficios del mecanismo bursátil que ofrece la Bolsa de Productos y Servicios de El Salvador, S.A. de C.V. (en adelante BOLPROS, S.A. de C.V. o BOLPROS) y las necesidades en aumento de un mercado insatisfecho.

La BOLPROS, S.A. de C.V., autorizó a IBES, S.A. de C.V. para operar como puesto de bolsa de productos y servicios en el mercado bursátil a partir del 25 de enero de 2005, otorgando la credencial de puesto N° 12.

Su finalidad principal es la intermediación por cuenta de terceros en la Bolsa de Productos de El Salvador, brindar asesoría relacionada con las operaciones bursátiles y operar en centros de depósito aprobados por las autoridades competentes. IBES es una empresa dedicada a la representación y asesoría de instituciones de gobierno y empresas privadas que tengan el interés y la intensión de vender o adquirir sus productos y/o servicios mediante el mecanismo de la bolsa. Durante sus primeros años de operación, el crecimiento que ha tenido lo sitúa como el puesto de

bolsa con gran cantidad de negociaciones en un periodo definido de tiempo. Debido a la experiencia de sus agentes de bolsa y el profesionalismo con las que ejecutan sus actividades, la entidad ha tenido la oportunidad de intermediar en sus adquisiciones a instituciones del sector gubernamental con exitosas negociaciones que han generado para el estado ahorros significativos los cuales les ha permitido invertirlos en otros bienes y servicios y eso produce más beneficios en sus inversiones, caso similar ha sucedido en la representación de empresas privadas.

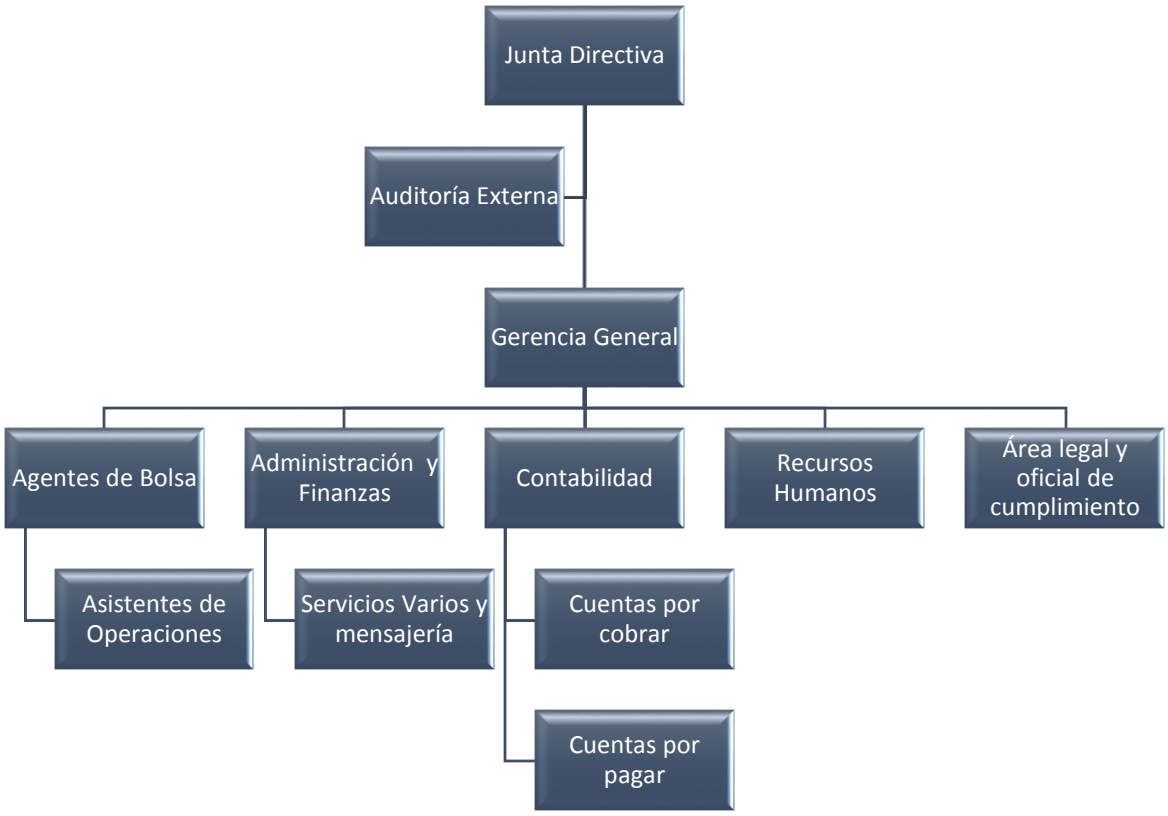
1.1.2. Misión y visión.

Misión: ser el Puesto de Bolsa con la mejor opción de representación para las instituciones de gobierno y empresa privada a través del servicio eficiente, transparente, competitivo y de calidad.

Visión: ofrecer alternativas de representación a nuestros clientes, enfocado en la excelencia en el servicio de intermediación bursátil de forma transparente, eficiente y confiable.

1.1.3. Estructura organizacional.

Figura propuesta N° 1. Organigrama de IBES, S.A. de C.V.



Fuente: *Pagina web de un puesto de bolsa activo.*

El área que desempeña las funciones de seguridad de la información en la entidad es Administración y Finanzas.

1.1.4. Áreas críticas de la entidad.

Las áreas críticas de la entidad respecto a seguridad, son aquellas donde se han establecido con mayor enfoque medidas y controles de seguridad cuya finalidad es proteger y garantizar la integridad, confidencialidad y disponibilidad de la información que en estas se procesa. A continuación se describen las áreas críticas de IBES, S.A. de C.V.:

- **Alta dirección: r**epresentan el área donde se reúnen los altos directivos de la organización, que para el caso de IBES sería la Junta Directiva. Esta área es crítica por la información confidencial y sensible que se procesa, pues es imprescindible para la toma de decisiones y determinación de planes estratégicos, su acceso debe ser limitado con la finalidad que no se materialicen amenazas como el robo, manipulación, divulgación y perdida no autorizada de información.
- **Operaciones bursátiles:** es donde operan los agentes de bolsa, los cuales son los responsables de representar en nombre del puesto de bolsa a los clientes en los procesos de compra-venta en el mercado bursátil de bienes y servicios. Es un área critica debido a que los agentes de bolsa procesan información delicada de sus representados como precio y cantidades de los bienes y servicios a intermediar, cuentas bancarias, documentos fiscales (comprobantes de crédito fiscal, facturas de consumidor final, comprobantes de retención, notas de débito, notas de crédito) documentos de la intermediación bursátil (contratos de la negociación, ordenes de negociación, contratos de comisión, declaraciones de no colusión), contactos de altos directivos de empresas y funcionarios de gobierno, gestión de perfiles virtuales en ruedas de negociación (subasta de precios de productos y servicios en línea). Todo lo anterior se debe gestionar con la integridad y confidencialidad necesaria para evitar la pérdida o modificación de la información.
- **Operaciones financieras.** acá es donde actual con mayor énfasis el departamento de Administración y Finanzas, pues como se describió anteriormente tienen la función de emitir cheques, realizar transferencias bancarias en línea, recibir y ejecutar los pagos a sus clientes. Representa un área crítica debido a las amenazas de perdida, robo o hurto

del dinero propio y de los clientes. El dinero propio se maneja de 3 formas: en efectivo, a través de cheques y por transferencias electrónicas. El dinero de terceros se tiene la obligación de gestionarlo de 2 formas: cheques y transferencias electrónicas. Para esto último cada puesto tiene cuentas bancarias exclusivas donde se realizan únicamente el pago de los bienes o servicios intermediados, y son monitoreadas por la BOLPROS de forma continua, siendo además esta la que autoriza cada transacción en estas cuentas especiales (llamadas operativas). En todo esto es indispensable proteger estas transacciones de ciberataques, malware y manipulación no autorizada. Se cuenta con equipos protegidos con antivirus y antimalware y sistema operativo Windows 7 actualizado, además de segregación limitada de funciones.

- **Servicio de mensajería:** el traslado de información es indispensable para el puesto de bolsa, y se realizar mediante una persona asignada únicamente a la entrega y recepción de documentación física diversa, producto de las negociaciones entre puestos de bolsa y clientes. Es un área critica debido a que existe un alto nivel de riesgo de la información, ya que es susceptible a ser manipulada, robada, hurtada, puede existir una perdida, deteriorada (por situaciones de la naturaleza o accidente de tránsito) e incluso errores humanos al momento de entregar o recibir, lo que vulnera su integridad, disponibilidad y confidencialidad.
- **Área de recepción y correspondencia**: esta área se encarga de recibir documentos internos y externos e ingresarlos en el sistema de gestión documental del puesto de bolsa para su clasificación, distribución y entre física o digital a los usuarios a quienes van dirigidas. Por la exposición de esta área en la recepción de documentos, paquetes y otra

información de carácter confidencial, se cuentan con medidas de seguridad para replegar accesos no autorizados.

- **Recursos informáticos y de telecomunicación**: no es un espacio físico determinado a un área específica (a excepción del servidor local), ya que todos los departamentos utilizan este recurso y no existe un administrador experto de estos recursos; es Administración y Finanzas la responsable de las medidas y controles de seguridad. Se encuentran el servidor central, equipos de cómputo, de seguridad y de telecomunicaciones que permiten gestionar los servicios tecnológicos y de comunicación para el procesamiento y respaldo del a información. Esta área está protegida con medidas de seguridad físicas y lógicas, que tienen la finalidad de obstaculizar accesos no autorizados a estas instalaciones.
- **Área de contabilidad:** acá es donde se procesa la información contable, tributaria y financiera de las operaciones bursátiles, y donde se debe enfocar en gran medida la seguridad. Esta área maneja documentación sensible de las transacciones producto de la intermediación, documentos que reflejan los gastos del negocio, formularios, informes y otros documentos de intereses fiscal, y toda aquella información que permite la integración de los estados financieros de la entidad. Esta información está expuesta ser modificada sin autorización, ser eliminada, procesada erróneamente, y esto puede provocar una mala toma de decisiones por parte de la alta gerencia, la cual de pende de lo que acá se procese. Por lo cual se implementan medidas de segregación de puestos, un sistema de organización documental y limitación a cierta información.

1.1.5. Análisis de las fortalezas, oportunidades, debilidades y amenazas organizacionales.

Mediante la tabla propuesta N° 1 se expone el análisis de las fortalezas, oportunidades, debilidades y amenazas del puesto de bolsa IBES, S.A. de C.V., dicho análisis esta actualizado a junio de 2017.

Tabla propuesta N° 1. Matriz de análisis FODA de IBES, S.A. de C.V.

FORTALIEZAS	DEBILIDADES
Experiencia y profesionalismo con más de 10 años en el mercado bursátil	Falta de cultura hacia la seguridad por parte del recurso humano
Instalaciones modernas y a comodidad de los clientes	Nulo mantenimiento a los equipos tecnológicos de la organización
Innovación con uso de un sistema ERP personalizado	Desorganización en cuanto a la segregación de funciones
Expertos en el uso de plataforma virtual de BOLPROS para las subastas públicas	No existe un enfoque de gestión de riesgos
Atención personalizada a los clientes	Impuntualidad a subastas públicas de los agentes de bolsa
Amplio conocimiento del mercado nacional y de la calidad de los productos y servicios	Gastos innecesarios en equipo tecnológico
Uso de equipo tecnológico moderno	Ambiente laboral inadecuado
Puesto de bolsa líder en operaciones bursátiles de compra y venta del 31 % al 2016	Dificultades en el manejo del sistema ERP
Implantación de la fase de Planificación del sistema de gestión de seguridad de la información	
OPORTUNIDADES	**AMENAZAS**
Aumento de la adquisición de bienes y servicios en los últimos 3 años por parte de las instituciones el Estado	Práctica ilegal "Dumping" de los otros puestos de bolsa
Inestabilidad en las operaciones de otros puestos de bolsa	Mala gestión de las operaciones por parte de BOLPROS
Reconocimiento de la calidad del servicio por parte de los clientes	Pago retrasado de las instituciones del Estado a los proveedores
Ampliación de negocios a escala centroamericana	Dependencia del mercado bursátil de productos y servicios a las adquisiciones de las Instituciones del Estado
Ubicación geográfica en zona estratégica	Poca innovación de negocios y gestión de riesgos en del mercado bursátil de productos y servicios

Fuente: *Proyección de negocios 2014-2018 de un puesto de bolsa activo*

1.2. PARTES INTERESADAS DE LA ENTIDAD

1.2.1. Definir partes interesadas.

Las partes interesadas son aquellos sujetos (personas naturales, personas jurídicas, entidades gubernamentales o grupos empresariales) a quienes beneficia la implementación de un sistema de gestión de seguridad de la información (en adelante SGSI) en IBES, debido a la naturaleza de sus operaciones bursátiles a las cuales dicho sistema les otorga mayor confiabilidad. Las partes interesadas definidas por el puesto de bolsa son las siguientes:

- Alta gerencia
- Empleados
- Clientes
- Proveedores
- Bolsa de Productos y Servicios
- Superintendencia del Sistema Financiero
- Auditoría externa
- Instituciones financieras
- Otros puestos de bolsa

1.2.2. Definición de requerimientos de seguridad de las partes interesadas.

De las partes interesadas de IBES se han determinados las siguientes necesidades y expectativas:

- **Alta dirección:** obtendrá prestigio y rentabilidad mediante la implementación del SGSI el cual implicará una inversión y su compromiso para el cumplimiento de este. Cabe

mencionar que debido a la naturaleza de negocio el accionista es el mismo gerente de la entidad.

- **Empleados:** se encuentran estrechamente comprometidos con el SGSI, debido a que son quienes le darán el principal cumplimiento a los controles establecidos en este según cada uno de los procesos en los que son participes según los roles desempeñados por cada uno dentro de IBES.
- **Clientes:** serán beneficiados por el sistema debido a que su información será protegida para que terceros no autorizados ingresen a ella.
- **Proveedores:** de igual manera que los clientes son beneficiarios del SGSI ya que obtendrán seguridad en la información que estos proporcionen al puesto de bolsa.
- **Bolsa de Productos de El Salvador (BOLPROS):** el SGSI proporcionará disponibilidad, confidencialidad e integridad a la información requerida por la BOLPROS a IBES, dando cumplimiento al art. 21 e) de la Ley de Bolsas de Productos y Servicios, así como también dará seguridad a las plataformas en línea de subasta que brindará mayor grado de confianza al nicho de mercado.
- **Superintendencia del Sistema Financiero:** el sistema contribuirá al complimiento del art. 21 literal f) de la Ley de Bolsas de Productos y Servicios que obliga a IBES a proporcionar información a la SSF; la cual debe ser integra y oportuna.
- **Auditoría** externa: el sistema permitirá fortaleces los procesos de control interno de IBES que posteriormente son evaluados por los auditores externos.
- **Instituciones financieras:** el SGSI generará mayor confianza en la información proporcionada por el puesto de bolsa para la adquisición de futuros servicios financieros que contribuyan al crecimiento de la entidad.

- **Otros puestos de bolsa**: proporcionará disponibilidad e integridad a la información proporcionada por IBES a los distintos puestos de bolsa.

1.3. ALCANCE DEL SGSI

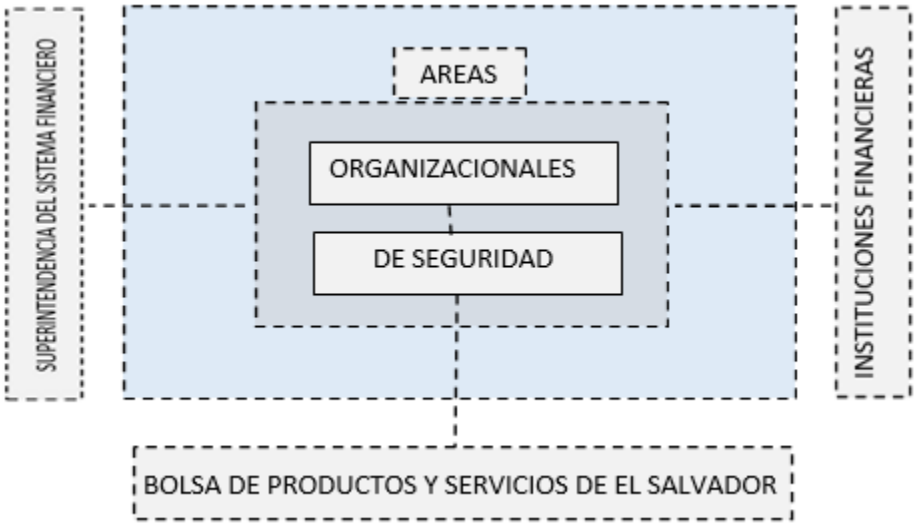
1.3.1. Establecimiento del alcance del SGSI.

Como se ha mencionado anteriormente que la finalidad principal de IBES, es la intermediación y comercialización de productos y servicios a través del asesoramiento y representación del cliente para la ejecución de compra y venta, así como también de acuerdo al establecimiento de medidas de seguridad se han determinado áreas claves las cuales son: áreas organizacionales (contabilidad, recepción y correspondencia, servicios de mensajería, operaciones bursátiles, operaciones financieras y la alta dirección) y áreas de seguridad de la información (seguridad lógica y seguridad física). Por tal razón el sistema gestionará los activos informativos de las áreas mencionadas.

En cuanto al alcance del sistema en función de los usuarios de la información, el SGSI tendrá impacto en los usuarios internos de los activos a nivel operativo, usuarios de información de los mandos medios y usuarios gerenciales de dichas áreas, los usuarios de los activos informativos que se vinculan a IBES a nivel exterior también resultan afectados, siendo los siguientes: La Bolsa de Productos y Servicios de El Salvador, La Superintendencia del Sistema Financiero y las instituciones financieras.

Para una mejor explicación del alcance del SGSI ver la siguiente figura propuesta N° 2 (Relación entre las áreas claves y entidades externas).

Figura propuesta N° 2. Relación entre las áreas claves y entidades



Fuente: *(Seis, 2015)*

FASE 2. LIDERAZGO

2.1. COMPROMISO DE LA ALTA DIRECCIÓN CON EL SGSI

Para conseguir el compromiso de la alta dirección la NTS ISO/IEC 270003 define en su apartado 5 que la organización debe crear un caso de negocio, en el cual se incluyan prioridades y objetivos para la ejecución del SGSI acompañado de un plan inicial del mismo; con la finalidad de que ellos comprendan la importancia y objetivos del sistema. Situación que se considera realizada para efectos del presente trabajo ya que es previo al diseño del SGSI.

Con la finalidad de garantizar el funcionamiento del SGSI en IBES, es necesario contar con el apoyo y compromiso de la alta dirección, debido a que está debe participar en las siguientes actividades:

- **Aceptar y establecer la política del SGSI:** en la cual el gerente general como la máxima representación de IBES, se compromete a dar cumplimiento a la política, objetivo y controles establecidos en el sistema.
- **Contribuir a la delegación de roles y responsabilidades:** consiste en establecer cuáles serán las actividades por realizar dentro de cada uno de los procesos que se encuentren cubiertos por el SGSI.
- **Contribuir a alcanzar los objetivos de la seguridad de la información mediante el cumplimiento de la política creada en conjunto a un compromiso de mejora continua del SGSI:** respecto al compromiso de esta con el departamento de gerencia general para definir objetivos afines al negocio que se pretenderán alcanzar mediante la ejecución del SGSI donde ambos deben formar parte para su planificación; así como también establecer reuniones en los que se analicen los resultados obtenidos en las auditorías para subsanar hallazgos y así procurar la mejora continua del sistema.
- **Proporcionar un adecuado suministro de recursos para la ejecución del SGSI:** colaborando al departamento encargado del sistema para que, durante de la ejecución de este no existan limitantes económicas o cualquier otro requerimiento necesario para que este alcance sus objetivos.
- **Participar en la decisión de criterios para la aceptación y los niveles de riesgo:** mediante la planificación y alcance del SGSI se requiere de su participación, durante la medición de los riesgos con la finalidad de indicar cuáles son y como están dispuestos a asumirlos; así como los parámetros de medición que les proporcionaran a estos.
- **Avalar la ejecución de auditorías internas al SGSI:** para la evaluación del cumplimiento de los controles internos del SGSI, es necesario que existan auditorías

internas al sistema; para las cuales la alta dirección debe proporcionar los accesos **necesarios a la auditoría para la evaluación de dichos controles.**

- **Colaborar en las revisiones del SGSI:** donde se responsabiliza de evaluar la efectividad de los controles del SGSI durante la auditoría interna; para contribuir a la mejora continua y cumplir con los objetivos de seguridad de la información.

Para acreditar el cumplimiento de los compromisos antes citados por parte de la alta dirección, se presenta la respectiva autorización.

INTERMEDIADORES BURSATILES DE EL SALVADOR, S.A. DE C.V.

GERENCIA GENERAL

AUTORIZACIÓN DE IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI

Yo Berardi Macchiato_, gerente general y presidente de la junta directiva de INTERMEDIADORES BURSATILES DE EL SALVADOR, S.A. DE C.V. en la sesión No. _10__, de la junta directiva celebrada el día __24__, de _septiembre____ del año __2017__, en uso de las atribuciones legales y reglamentarias autorizo EL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORACIÓN (SGSI) PARA INTERMEDIADORES BURSATILES DE EL SALVADOR, S.A. DE C.V. Comprometiéndome a dar cumplimiento y seguimiento a los siguientes enunciados:

- Aceptar y establecer la política del SGSI.
- Contribuir a la delegación de roles y responsabilidades.
- Contribuir a alcanzar los objetivos de la seguridad de la información mediante el cumplimiento de la política creada en conjunto a un compromiso de mejora continua del SGSI.
- Proporcionar un adecuado suministro de recursos para la ejecución del SGSI.
- Participar en la decisión de criterios para la aceptación de riesgos y los niveles de estos.
- Avalar la ejecución de auditorías internas al SGSI.
- Colaborar en las revisiones del SGSI.

F. _____

Berardi Macchiato
Gerente General

INTERMEDIADORES BURSATILES DE EL SALVADOR, S.A. DE C.V.

2.2. POLÍTICA DE SEGURIDAD DEL SGSI

2.2.1. Presentación de la política de seguridad.

Para Intermediarios Bursátiles de El Salvador, S.A., de C.V. la información es un activo fundamental para la prestación de sus servicios, así como para la toma de decisiones, motivo por el cual existe una responsabilidad de proteger sus propiedades más significativas como parte de una estrategia orientada al giro de su negocio, estableciendo una cultura de seguridad y dando cumplimiento a los requerimientos legales, contractuales y regulatorios vigentes que le sean de aplicación.

La presente política deberá ser revisada anualmente como parte del proceso de mejora continua o cuando existan cambios en su estructura, objetivo o alguna situación que afecte la política, con el fin de garantizar que sigue siendo apropiada a los requerimientos identificados.

2.2.2. Política de seguridad.

IBES, S.A. de C.V. como entidad dedicada a la intermediación de productos y servicios a través de un mecanismo transparente eficiente y seguro, en el cumplimiento de su misión, visión y objetivos estratégicos apegados a sus valores corporativos y con la finalidad de satisfacer las necesidades y expectativas de las partes interesadas, motivo por el cual la alta dirección de IBES. S.A. de C.V., a través del comité de seguridad de la información y en función de la seguridad de la información de la entidad, ha decidido impulsar y difundir a todos los niveles de la empresa la política siguiente:

“Los usuarios de la información en IBES, S.A. de C.V., son responsables de cumplir con los requerimientos legales, contractuales, normativos y procedimentales establecidos dentro

de sus áreas asignadas, que permita garantizar la disponibilidad, integridad y confidencialidad de los activos de información, para mantener una cultura de seguridad que posibilite continuidad del negocio"

La política de seguridad establecida anteriormente se fundamenta en los siguientes objetivos:

- Proteger todos activos de información frente a amenazas internas o externas ocasionadas de forma voluntaria o accidental.
- Integrar medidas de seguridad en los sistemas de información con el propósito de minimizar los riesgos de error humano y sucesos de origen natural.
- Asegurar que los riesgos se mantengan a un nivel aceptable.
- Concientizar a los usuarios sobre la responsabilidad en el manejo y uso de la información y sobre el establecimiento de una cultura de seguridad.
- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Contar con una herramienta de gestión con el propósito de minimizar riesgos operativos y tecnológicos.
- Revisar periódicamente la política a fin de mantenerla actualizada y garantizar su vigencia eficiencia y eficacia, así mismo incorporar cualquier modificación que sea necesaria en función de posibles cambios que puedan afectar su definición.

2.2.3. Políticas específicas.

Con el objetivo de gestionar la seguridad de la información y minimizar los riesgos a un nivel aceptable se establecen las siguientes políticas las cuales soportan al SGSI:

- Las responsabilidades en relación a la seguridad de la información serán compartidas, publicadas y deberán ser aceptadas por cada uno de los usuarios de los activos de información.
- Los usuarios de la información tienen la obligación de reportar todos los incidentes en materia de seguridad utilizando las directrices establecidas por IBES, S.A. de C.V.
- IBES, S.A. de C.V. dispondrá de una estructura organizacional ideal para gestionar la seguridad de la información asegurando que se proveerán los recursos necesarios.
- A los encargados de las áreas organizacionales se les asignaran responsabilidades en cuanto a la gestión de los activos que se relacionan con los sistemas de información y clasificación de la información
- En relación a las áreas de seguridad de la información, se establecerán controles de acceso, lógico, físico y ambientales con el fin de asegurar los activos que almacena información de IBES, S.A. de C.V.
- IBES, S.A de C.V, garantizará que la seguridad sea parte fundamental del ciclo de vida de los sistemas, atreves de una adecuada gestión de riesgos e identificando las debilidades asociadas con los sistemas de información.
- Los responsables de las áreas organizacionales y de seguridad de la información deben asegurar el cumplimiento de los requerimientos legales, regulatorios y contractuales, así como los establecidos en los documentos del SGSI.

2.3. OBJETIVOS DE SEGURIDAD DEL SGSI

2.3.1. Objetivo del SGSI.

El objetivo general de este SGSI es aplicar en las áreas operativas y de seguridad de IBES, S.A. de C.V. los requerimientos establecidos en la Normas Técnicas Salvadoreñas ISO 27001 e ISO

27003 que permitan gestionar la integridad, confidencialidad y disponibilidad de la información del puesto de bolsa de forma permanente.

2.3.2. Objetivos de Seguridad de la Información.

Objetivo General:

- Obtener los niveles adecuados de confidencialidad, integridad y disponibilidad para toda la información importante de Intermediarios Bursátiles de El Salvador, S.A. de C.V., con la finalidad de garantizar la continuidad operacional de los procesos y servicios que realiza la organización, mediante la correcta gestión de los activos de información vinculados a los procesos críticos del negocio y su soporte.

Objetivos específicos:

- Controlar, evitar y/o mitigar los riesgos de seguridad de la información, identificando las amenazas a las que están expuestas los activos de información y las vulnerabilidades asociadas, en beneficio de asegurar la continuidad del negocio.
- Determinar políticas, controles y procedimientos que aseguren la protección de los activos de información del puesto de bolsa.
- Definir un plan de gestión de riesgos de seguridad de la información, con la finalidad de reducir, evitar, transferir o suprimir los riesgos.
- Garantizar el compromiso continuo de la gerencia general en la aprobación, autorización y mejora continua del sistema de gestión de seguridad de la información.
- Fomentar en los diferentes niveles jerárquicos de IBES, S.A. de C.V. las buenas prácticas y comportamientos seguros en el procesamiento de la información.

- Optimizar el nivel de efectividad de los controles del puesto de bolsa.
- Definir roles y responsabilidades a los usuarios de la información según el área donde labore.
- Ejecutar la gestión correcta de las actividades preventivas y correctivas que se provienen del reporte de eventos e incidentes de seguridad de la información.

2.4. Requerimientos legales de la seguridad de la información.

La legislación vigente para IBES, S.A. de C.V. vigente en El Salvador relacionada a la gestión de la seguridad de la información en los puestos de bolsas de productos y servicios, se mencionan los siguientes artículos de la normativa legal aplicable:

- **Ley de Bolsas de Productos y Servicios.**

El art. 1 tiene el objeto de regular la constitución, funcionamiento, limitaciones y prohibiciones que poseen las bolsas de productos servicios, así como aquellos participantes en el mercado bursátil en que operan.

El art. 21 establece en su literal “e” que los puestos de bolsas de productos y servicios, así como los licenciatarios deberán proporcionar información oportuna, clara y veraz en torno a sus actividades a la bolsa de productos y servicios; y en el literal f. haciendo referencia a la información conducente que dichas entidades deben suministrar a la Superintendencia para que lleve a cabo sus funciones.

Cualquier persona que sea afectada por información falsa, alterada, simulada, ocultada o que no atienda al fin de hacer público lo que acontece en las bolsas, podrá acudir ante los tribunales correspondiente para demandar la indemnización por daños y perjuicios que le hubieren

ocasionado. Es responsabilidad de licenciatarios, directores, titulares, administradores, gerentes y demás funcionarios de los puestos de bolsa, cuando divulgaren, revelaren hechos falsos, información maliciosa, simulen hechos, suministren daros o información cuyo objetivo sea confundir al público y serán responsables de los daños y prejuicios que dichas acciones ocasionaren.

Ante el incumplimiento de lo antes citado, existen sanciones impuestas por las bolsas y la SSF (art. 40), el no informar, suministrar información incompleta o hacerlo en forma extemporánea tiene un monto de cinco mil colones equivalente a quinientos setenta y uno con cuarenta y tres centavos; quince mil colones al proporcionar información falsa o alterada equivalente a mil setecientos catorce con veinte y nueve centavos; cincuenta mil colones equivalentes a cinco mil setecientos catorce con veinte y nueve centavos al carecer de registros y controles necesarios exigidos por la ley y el reglamento, o que estos resulten deficientes. En caso de reincidencia se duplicará el monto.

- **Reglamento general de la Bolsa de Productos de El Salvador**

El reglamento en su artículo 1 tiene como objetivos regular: el debido funcionamiento y la organización de la bolsa; procedimientos a través de los cuales se negocian; documentos, servicios, productos o instrumentos que la bolsa autorice, las actividades de aquellos participantes en el puesto de bolsa y las sanciones a imponerse a los agentes de bolsa o licenciatarios.

Forma parte de las obligaciones según el art. 35 de los puestos de bolsa y licenciatarios: llevar aquellos registros que fueren necesarios para mantener la transparencia y confianza de los negocios que intervienen (literal d), proporcionar la información de forma oportuna, clara y veraz que sea

solicitada por la bolsa y la SSF (literal e), y suministrar a las autoridades pertinentes aquella información que sea requerida (literal f).

Es una sanción leve de acuerdo con el art. 55, para los puestos de bolsa y licenciatarios no informar o suministrar la información de forma completa o fuera del tiempo establecido, en que la haya solicitado la bolsa. Es considerada como sanción grave: la revelación de información confidencial de las transacciones y el suministro de datos o información falsa a la bolsa u otras entidades con la autoridad de exigirla según el art. 57.

Así también es una infracción grave a los puestos de bolsa el suministro de información y datos falsos a sus clientes como lo cita el art. 60.

- **Código de Ética de la Bolsa de Productos de El Salvador**

El código tiene el objetivo de resguardar los principios y lineamientos fundamentales para los negocios que se realicen mediante la bolsa de acuerdo con el art. 2 y obligando a los puestos de bolsa de productos y servicios a dar fiel cumplimiento a tal normativa como indica el art. 3 en su literal b. Donde la seguridad de la información en la bolsa se regula dentro de aquellos principios y valores a promover y resguardar: como el manejo de la información y el resguardo de esta (art. 4 literales “h” e “i”); donde los sujetos que posean información de carácter confidencial o privilegiada son responsables de salvaguardarla y a utilizarla exclusivamente en el desarrollo de sus actividades laborales. A demás deberá velarse para que dicha información no sea utilizada por terceros en beneficio propio o ajeno.

El código delega como encargado de la confidencialidad al Gerente General, así como los empleados que este designe.

La es considerada información confidencial como un activo empresarial y propia de las actividades del negocio y que por tanto no debe ser accesible al público según lo estipulado en el art.5, algunos ejemplos de este tipo de información son: los planes estratégicos, expedientes laborales o información de la clientela; y para conseguir asegurar el resguardo de esta por parte de los empleados de bolsa están obligados a firmar un contrato de confidencialidad. Entiéndase por información privilegiada, aquella que está vinculada con las actividades propias del negocio, de posesión exclusiva que es transmitida por los distintos empleados de la bolsa quienes deben utilizarla sin generarse ningún beneficio propio o causar daños o perjuicios a otros. Lo anterior tiene como objetivo que la información sea manejada y generada con sigilo y confianza (como lo establece el art. 6), por tanto, queda prohibido para los empleados y demás personal el retirar documentos con información privilegiada de su área de trabajo o comunicarlo incluso de forma verbal a terceros no autorizados por Junta Directiva. Algunos ejemplos de este tipo de información son: las ofertas presentadas por la bolsa antes de su publicación, información personal sobre los oferentes y los procesos de compra/venta o aquella relativa a precios mínimos o máximos dentro de las pujas.

2.5. ESTRUCTURA ORGANIZACIONAL DEL SGSI

2.5.1. Determinación de roles del SGSI.

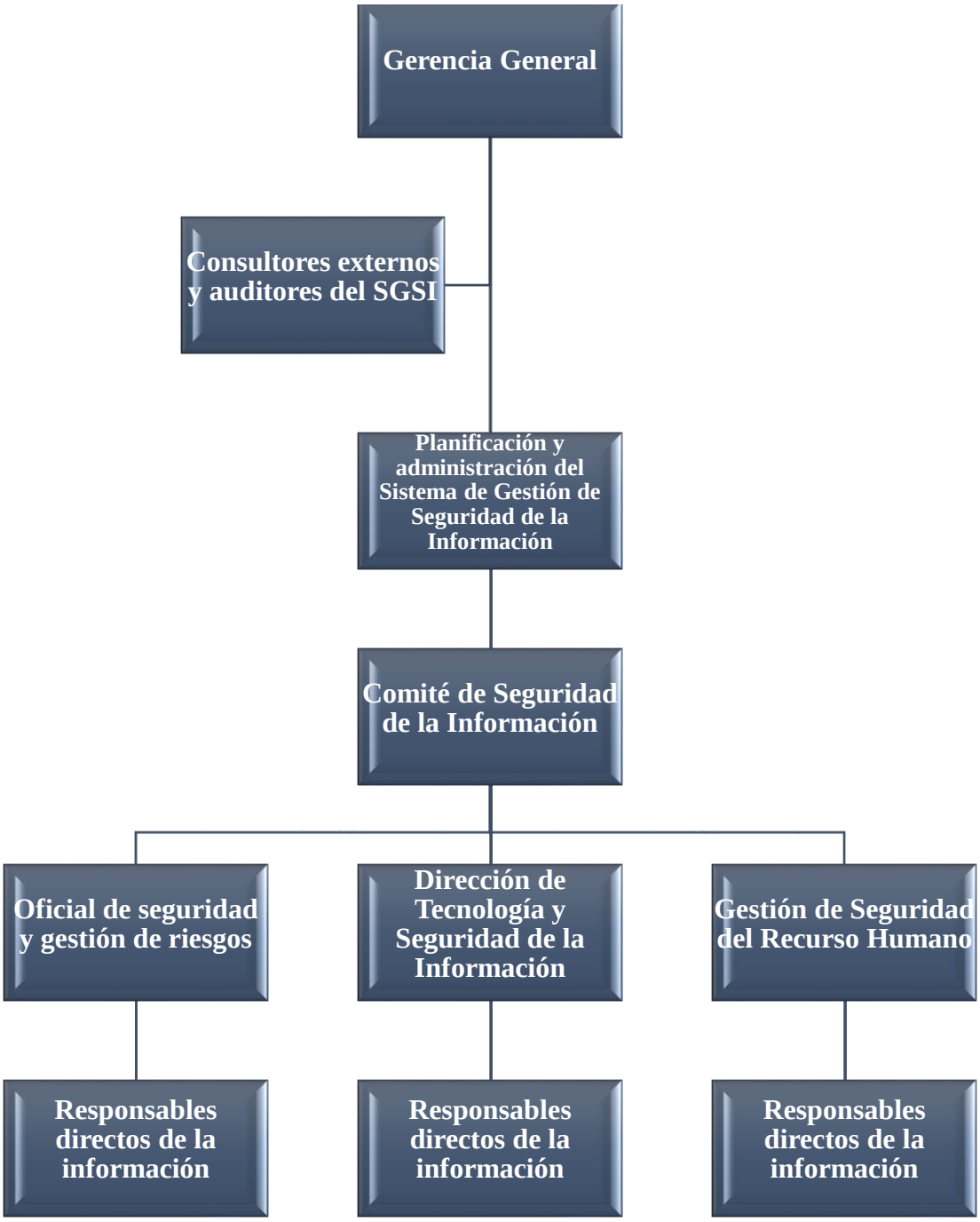
Según lo establecido en el apartado “5.3. Roles, responsabilidades y autoridades organizacionales” de la NTS ISO/IEC 27001:2013, la alta dirección tiene la obligación de asegurarse que se asignen las facultades y responsabilidades a los roles definidos para la seguridad de la información de la organización. Con base en este requerimiento, como primer punto se identificaron dentro del organigrama organizacional las áreas cuyas funciones abarcan la seguridad

de la información dentro de la entidad. Para lo cual se identificó que Administración y Finanzas es quien se encarga actualmente de la seguridad.

Se ha tomado en cuenta lo descrito en el anexo 2 de la NTS ISO/IEC 27003:2010 “Roles y responsabilidades para la seguridad de la información”, el cual representa una guía general de las principales actividades que cada participante de forma jerárquica del SGSI debería realizar para cumplir con los objetivos del sistema.

Basado en lo anterior, considerando el tamaño de IBES. S.A. de C.V. y los recursos de los cuales dispone para la implementación del SGSI, se establece el esquema organizacional del sistema de gestión de seguridad de la información en la figura propuesta N° 3.

Figura propuesta N° 3. Organigrama del SGSI.



Fuente: Fuente: *NTS ISO/IEC 27003:2010*

2.5.2. Determinación de responsabilidades y facultades a los roles asignados.

Establecida la estructura organizacional de la seguridad de la información es necesario la asignación de responsabilidades para los roles identificados.

- **Gerencia General:** el liderazgo, compromiso y la participación de la Alta Dirección, representada por la gerencia general, respecto al sistema de gestión de seguridad de la información es esencial ya que ellos son los dueños del negocio y por lo tanto deben estar conscientes de la política de seguridad. La actitud y el convencimiento de la Alta Dirección es fundamental para el éxito del SGSI y por lo tanto se muestra la importancia de predicar con el ejemplo por parte de la dirección a través de las responsabilidades siguientes:

    a) Aprobar la política de seguridad de la información.

    b) Asegurar el establecimiento de la política y de los objetivos de seguridad de la información.

    c) Garantizar la disponibilidad de recursos para el SGSI.

    d) Transmitir la importancia de una gestión de seguridad eficaz y conforme a los requerimientos del SGSI.

    e) Apoyar y dirigir a las personas involucradas para contribuir en la eficiencia y eficacia del SGSI.

    f) Fomentar una cultura de seguridad de la información en la organización.

    g) Revisar la política de seguridad de la información de forma periódica e incorporar las modificaciones si existieran y promover la mejora continua

- **Consultores externos y auditores del SGSI:** las consultorías y auditorias del SGSI permiten a las organizaciones el cumplimiento de los requerimientos normativos,

porque incluyen un conjunto de medidas para el control y mitigación de los riesgos asociados a los activos de seguridad de la información; dentro de sus responsabilidades figuran las siguientes:

Consultores externos

a) Enfocarse en la contribución de precisar en los objetivos propuestos por la organización en relación a la política de seguridad de la información.
b) Brindar apoyo necesario para que la entidad tenga eficiencia y eficacia en su en relación a la seguridad de la información.
c) Identificar necesidades de instruir alguna área donde se muestren deficiencias, para fortalecer el desempeño de los colaboradores respecto al SGSI.
d) Desarrollar alternativas y lineamientos en materia de solución de problemas e implementación de controles de seguridad y dar a conocer de cada uno de ellos.

Auditores del SGSI

a) Revisar la política de seguridad de la información y toda la documentación que posee la organización con relación al SGSI.
b) Identificar el nivel de madurez que tiene la organización en cuanto a la implementación de controles.
c) Realizar un análisis de riesgo y observaciones de todas las partes interesadas.
d) Determinar vulnerabilidades y amenazas que no fueron tratadas en evaluaciones anteriores.
e) Elaborar un informe donde se establezcan las fortalezas y debilidades detallando las no conformidades encontradas y haciendo las recomendaciones de mejora continua.

- **Planificador y administrador del SGSI:** formado por miembros con un entendimiento de los activos de la información y un amplio conocimiento de la forma de hacer uso de la información, son quienes coordinan y dirigen y controlan la ejecución del plan establecido en el SGSI y dan seguimiento de acciones correctivas y preventivas. Estará integrado por el área organizacional de Administración y Finanzas y Contabilidad. Dentro de sus responsabilidades están:

    a) Diseñar conjuntamente con las demás áreas del SGSI la política de Seguridad de la información y demás lineamientos específicos.
    b) Elaborar los objetivos de seguridad de la información con la ayuda de las demás áreas del SGSI.
    c) Crear y definir lineamientos para la conformación de grupos de respuestas frente a incidentes de seguridad.
    d) Realizar acciones correctivas y preventivas relacionadas con la seguridad de la información.
    e) Establecer el alcance del SGSI con la participación del resto de áreas del sistema.
    f) Ejecutar el plan de seguridad definido en los documentos del SGSI.
    g) Promover la realización de auditorías enfocadas a garantizar la seguridad de la información y la mejora continua.
    h) Participar en la elaboración de programas de capacitación del SGSI y promover su cumplimiento.
    i) Coordinar y participar en labores de auditoría y consultoría y manejo de información.

j) Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

k) Plantear las prioridades de la organización respecto al SGSI

- **Comité de seguridad de la información:** es el responsable del mantenimiento y mejora continua, junto con el área de planificación, del SGSI. De igual forma, están comprometidos con la ejecución e informe oportuno a la Gerencia General de las de las actividades principales para mantener los niveles de seguridad establecidos por el puesto de bolsa. Estará integrado por representantes de la gerencia general, administración y finanzas, agentes de bolsa, contabilidad y recursos humanos. Se detallan las responsabilidades del comité:

  a) Participar en la divulgación de la política de seguridad de la información.

  b) Garantizar el cumplimento de lo establecido en los documentos del SGSI.

  c) Tener participación en el análisis de riesgo de la información.

  d) Efectuar revisiones periódicas de la documentación vinculada a la operatividad del SGSI.

  e) Colaborar en las actividades de seguridad y supervisar los planes de trabajo de las unidades organizacionales y de seguridad.

  f) Reportar de manera oportuna y eficiente las vulnerabilidades e incidentes de seguridad.

  g) Participar en la implementación de controles, lineamientos y procedimientos de seguridad, según los riesgos detectados.

  h) Amparar la ejecución de medidas correctivas que sean señaladas por las auditorias.

i) Contribuir en el análisis de riesgo y ejecutar medidas necesarias para mitigar el riesgo asociado a los sistemas de información.

j) Comprometerse en que la seguridad sea parte del proceso de planificación.

- **Oficial de seguridad y gestión de riesgos:** esta persona que se encargara de informar a los proveedores, y el equipo de trabajo acerca de los cambios en las políticas de seguridad y sobre la normativa legal aplicable a la seguridad de la información. Su representante será el área legal y oficial de cumplimiento del puesto de bolsa. Además, en esta área se encontrarán a las personas responsables de la gestión de riesgos, que incluirá la evaluación y tratamientos de los mismos y estará integrada por representantes de las áreas organizacionales de administración y finanzas y recursos humanos y el área de tecnología y seguridad de la información del SGSI. A continuación se detallan las funciones y facultades de ambos responsables:

  Oficial de seguridad:

  a) Debe interpretar y conocer sobre la normativa legal vigente vinculada con la seguridad de la información bajo el contexto de las operaciones bursátiles del puesto de bolsa.

  b) Velar por el cumplimiento de la legislación aplicable a la seguridad de la información por parte del puesto de bolsa.

  c) Actualizar la normativa legal vigente dentro del SGSI del puesto de bolsa.

  d) Gestionar la implementación de las políticas de seguridad de la información junto con las demás áreas del sistema.

  e) Determinar los controles del SGSI.

f) Atender las auditorías al SGSI y facilitar información sobre las políticas y controles implementados.

Gestión de riesgos:

a) Identificar los riesgos que amenazan los activos de información
b) Establecer un programa continuo que permita monitorear las vulnerabilidades y administrar los planes de su mitigación.
c) Definir los mecanismos para la gestión de los riesgos de seguridad de la información.
d) Informar al comité de seguridad de la información aspectos relacionados con la gestión de riesgos.
e) Asegurarse que el puesto de bolsa proporcione información sobre la gestión de riesgos en la información cuando un ente regulador lo solicite.

- **Dirección de tecnología y seguridad de la información:** tendrá la función de implementar políticas de seguridad de la información y velar la debida gestión de los activos de información, con la asesoría de las otras áreas del SGSI. El encargado de esta área debe ser un especialista en el manejo de tecnologías de la información, para lo cual se sugiere contratar personal para desempeñar este cargo y auxiliares necesarios. A continuación se detallan las actividades que deben realizar:

a) Deben asegurarse que se cumplan las políticas y requerimientos de seguridad determinados para la compra, diseño, operación, gestión y mantenimiento de la plataforma tecnológica y servicios de telecomunicaciones del puesto de bolsa.
b) Participar en la creación de la política de seguridad del a información y demás lineamientos específicos.

c) Ser parte integral en el diseño de los objetivos de seguridad de la información.

d) Determinar los roles y responsabilidades de seguridad a los responsables directos a los responsables directos de la información.

e) Responsable de los procesos de control de acceso, seguridad física, seguridad lógica y seguridad de los sistemas informáticos.

f) Asignar límites a los usuarios de los sistemas.

g) Realizar una comprobación que los controles determinados cumplen con los requerimientos.

h) Proponer modificación de políticas o nuevas políticas de seguridad cuando sean necesario.

- **Gestión de seguridad del recurso humano:** es el responsable del personal del puesto de bolsa. Sera gestionada por el área organizacional de recursos humanos. A continuación se describen las siguientes actividades que debe ejecutar:

  a) Capacitar periódicamente y concientizar al personal del puesto de bolsa en relación la seguridad de la información

  b) Debe coordinarse con el área de tecnología y seguridad de la información para la asignación de roles y responsabilidades específicas.

- **Responsables directos de la información:** son los responsables de mantener la seguridad de la información en los procesos donde participan, es decir, sus puestos de trabajo. Se describen a continuación las responsabilidades de los usuarios de la información:

  a) Deben conocer la estructura organizacional del SGSI y quienes serán los participantes de este.

b) Cumplir con las políticas, controles y directrices de seguridad de la información
c) Asistir a las capacitaciones gestionadas por el área de recursos humanos relacionadas con la seguridad de la información.
d) Definir, mantener, documental, actualizar y mejorar de forma continua los procedimientos en beneficio de la seguridad de la información.
e) Informar a su responsable inmediato del SGSI respecto a problemáticas detectadas en los controles o actividades relacionadas con su trabajo y que están vinculadas a la seguridad de la información.
f) Hacer un uso adecuado de los activos de información de los cuales es responsable.
g) Tomar participación y apoyar en la identificación, valoración y tratamiento de los riesgos de seguridad.
h) Proponer mejoras los controles o políticas de seguridad del SGSI que estén vinculadas con los procesos de su trabajo.
i) Mantener la integridad, disponibilidad y confidencialidad de la información que procesan para la realización de sus actividades.
j) Trabajar en conjunto con el resto de áreas del SGSI.

2.5.3. Matriz RACI del SGSI.

La matriz RACI es una tabla que expone el grado de responsabilidad de las personas o grupos que participan en un proyecto y, simultáneamente, los roles correspondientes asignados dentro de éste. La finalidad principal de la matriz RACI es ilustrar los vínculos existentes entre el trabajo que se realizará y los miembros del equipo, departamento o área de la entidad, garantizando que los recursos adecuados estén asignados a las actividades adecuadas.

El acrónimo RACI es originario del inglés y está referenciado a las responsabilidades más comunes incluidas en la matriz:

- **Responsible** (responsable): son las personas que realizan el trabajo para lograr una tarea específica dentro del proyecto. Regularmente debe existir un único rol con esta participación de responsable, aunque otros pueden ejecutar el mismo si se delegara dicha responsabilidad a otra persona para ayudar en el trabajo requerido.
- **Accountable** ("aprobador"): es el encargado de rendir cuentas sobre la actividad, también reconocido como la autoridad final que aprueba el proceso. En otras palabras, es a quien le corresponde firmar la aprobación del trabajo que es proporcionado por el Responsable. Sólo debe haber un "Accountable" especificado para cada tarea o entrega.
- **Consulted** (consultado): son aquellos no directamente implicados en el desarrollo de las actividades, pero que se les solicita opiniones, y con quienes existe una comunicación bidireccional.
- **Informed** (informado): aquellos que se mantienen al día sobre los progresos, generalmente, cuando la tarea se termina o entrega, o quienes reciben las salidas de un proceso y con el que sólo hay una vía de comunicación unidireccional.

Comprendido lo anterior, en la tabla propuesta N° 2 se presenta la matriz RACI del SGSI del puesto de bolsa IBES, S.A. de C.V. En la columna de actividades se han descrito las responsabilidades según los párrafos de la NTS ISO/IEC 27001:2013 y la NTS ISO/IEC 27003:2010, integrando las actividades de los requerimientos y el desarrollo del SGSI junto con los roles y responsabilidades diseñados para este sistema (los roles han sido extraídos del organigrama del sistema.

Tabla propuesta N° 2. Matriz RACI de roles y responsabilidades del SGSI de IBES, S.A. de C.V

Proceso o actividad		Rol								
NTS ISO/IEC 27001:2013	**NTS ISO/IEC 27003:2010**	**Gerencia General**	**Consultores Externos y auditores del SGSI**	**Planificación y administración del SGSI**	**Comité de Seguridad**	**Oficial de Seguridad**	**Gestión de riesgos**	**Tecnología y seguridad de la información**	**Seguridad RRHH**	**Responsables directos de la información**
	5.2. Definir prioridades organizacionales para el desarrollo del SGSI	**I , C**	**C**	**R , A**						
	5.3. Definir alcance preliminar	**I**	**C**	**R , A**						
	5.4. Diseñar el proyecto del SGSI	**I , A**	**C**	**R**						
4.1. Contexto interno y externo de la organización		**I , C**		**R , A**						
4.2. Necesidades y expectativas de las partes interesadas		**I , C**		**R , A**						
4.3. Alcance del SGSI	(6.1,6.2,6.3,6.4,6.5) - Definición del alcance y límites del SGSI	**I , C, A**	**C**	**R**	**C , I**	**C , I**	**C , I**	**C , I**	**C , I**	
5.2. Política de seguridad de la información	(6.6, 9.2.3) - Política del SGSI	**I, A**	**C**	**R**	**C , I**	**C , I**	**C , I**	**C , I**	**C , I**	**I**
	5. Aprobación del SGSI	**R , A**		**I**	**I**	**I**	**I**	**I**	**I**	**I**
(5.1, 5.2) - Roles, responsabilidades y autoridades del SGSI	9.2.1 Estructura organizacional de la seguridad d la información	**I**	**C**	**I**	**I , A**		**C**	**R**	**C**	**C**
	(7.1, 7.2) Análisis y definición de requerimientos de seguridad	**I**		**I**	**I , A**	**C**	**C**	**R**	**C**	
(6.1,8.1,8.2) - Gestión de riesgos y oportunidades de los activos de información	(7.3,8.1,8.2) - Identificar los activos de información y su evaluación de riesgos	**I**	**C**	**I**	**I, A**	**C**	**R**	**C**	**C**	**C**

6.2. Objetivos de seguridad de información	9.2.2 Diseñar un marco referencial para la documentación del SGSI	**I**		**I , A**	**R**	**C , I**	**C , I**	**C , I**	**C , I**	**C , I**
	8.3. Seleccionar objetivos de control y controles	**I**	**C**	**I**	**R , A**	**C , I**	**C , I**	**C , I**	**C , I**	**C , I**
7.4. Comunicaciones internas y externas		**C , I**	**C , I**	**A**	**R**	**C , I**	**C , I**	**C , I**	**C , I**	**C, I**
7.5. Gestión de información documental	9.2.2. Diseñar marco referencial para documentar SGSI	**C , I**	**C**	**I**	**I**	**A , I**	**A , I**	**A , I**	**A , I**	**R**
(7.2, 7.3) - Concientización, capacitación y evaluación	9.4.2 Diseñar el programa de concientización y capacitación sobre seguridad de la información	**I**	**C**	**C , I**	**C , I, A**			**C**	**R**	**C**
(8.1, 7.1) - Planificación y recursos		**C , A**		**R**	**C , I**	**C , I**	**C , I**	**C , I**		
9.1 Análisis y evaluación de métricas		**I**		**A**	**R**		**C**	**C**		
9.2 Auditoria interna		**I**	**C**	**A**	**R ,C**	**C , I**	**C , I**	**C , I**	**C , I**	**C**
9.3. Revisión de la Dirección	9.4.1. Plan para revisión de la dirección	**R , A**		**C , I**	**C , I**					
10.1 Acciones correctivas		**I**		**I**	**R , A**	**C, I**	**C , I**	**C , I**	**C , I**	**C , I**
10.2. Acciones de mejora		**I**		**I**	**R , A**	**C, I**	**C , I**	**C , I**	**C , I**	**C , I**
4.4. Operación del SGSI	8.4. Autorización para operar SGSI	**R , A**		**I**	**I**	**I**	**I**	**I**	**I**	**I**
	9.5. Producir el plan final del SGSI	**A**		**R**	**C, I**	**C, I**	**C, I**	**C, I**	**C, I**	**I**

Fuente: (Llanos, 2016)

FASE 3. PLANIFICACIÓN

En esta fase se realizaron las actividades necesarias con la finalidad de garantizar que el diseño del sistema de gestión de seguridad de la información para puestos de bolsa de productos y servicios culmine los objetivos propuestos, correspondientes a la determinación de los riesgos y las medidas para mitigarlos y a la definición las políticas y limites en el contexto de la seguridad de la información que deben cumplir las partes interesadas de la entidad.

3.1. LEVANTAMIENTO DE ACTIVOS

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

Las actividades vinculadas con la clasificación de los activos de información y su valoración de riesgos, se han ejecutado según los siguientes puntos:

- **Identificación de activos.** Este proceso se ejecutó en función del alcance del SGSI, el cual solo establece el proceso de tecnología, por lo cual, solamente se seleccionaron los activos de información administrados y utilizados por las diferentes áreas de IBES, S.A de C.V., y que posteriormente fueron el insumo para el proceso de valoración de riesgos
- **Clasificación y presentación:** en la primera actividad de esta etapa se definió una clasificación de los activos en la tabla propuesta N° 3, según la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (conocido como MAGERIT), diseñada por la Dirección General de Modernización Administrativa, Procedimientos e

Impulso de la Administración Electrónica del gobierno de España. En segundo lugar, se realizó la identificación y clasificación (según tabla propuesta N° 2) de los activos de información determinados como vitales a partir del impacto que puede ocasionar su indisponibilidad o su incorrecto funcionamiento según la tabla propuesta N° 4.

- **Responsable del activo.** Adicionalmente se identificó en la tabla propuesta N° 4 el área responsable de cada uno de los activos, a partir del organigrama de IBES.

Tabla propuesta N° 3. Clasificación de los tipos de activo de información.

Tipo de activo	Descripción de la tipificación del activo
Redes de comunicación	Son los servicios de comunicación contratados a los proveedores; medios de transporte que llevan información a otros lugares
Personal	Son las personas vinculadas con el procesamiento de la información y gestión de los activos.
Datos / información	Ficheros, datos de autenticación, datos de control de acceso, copias de respaldo, registro de actividades, bases de datos
Software	Aplicaciones instaladas en las computadoras, programas, sistemas de información, sistemas operativos.
Equipo informático	Dispositivos físicos donde se almacena la información, equipo físico que procesa los datos de forma directa o indirecta.
Soporte de información	Documentación soporte de las operaciones y actividades. Puede ser física o digital
Instalaciones	Lugares donde están ubicados los activos e información de la empresa
Equipo auxiliar	Otros equipos que permiten de soporte a los sistemas de información sin tener algún vínculo con los datos.

Fuente: *(Silva, 2015)*

En la tabla propuesta N° 4 se presenta el levantamiento de activos de información de la empresa IBES, S.A. de C.V. y una breve descripción de cada uno.

Tabla propuesta N° 4. Levantamiento de activos de información.

N°	Activo	Tipo de activo	Descripción	Responsable
A1	Base de datos de recursos humanos	Datos/información	Contiene la información de datos personales de cada empleado, su rol en la entidad, el área a la que pertenece, planillas de sueldos y bonificaciones, descuentos previsionales y de seguridad social.	Recursos humanos
A2	Bases de datos clientes	Datos/información	Información tributaria del cliente, sus números de cuentas bancarias, domicilios, contactos telefónicos, correos electrónicos, datos de ordenes de negociación, declaraciones de no colusión, contratos aceptados, contratos en curso, garantías de contrato y fechas relevantes	Contabilidad
A3	Bases de datos proveedores	Datos/información	Información tributaria de los proveedores, números de cuentas bancarias, domicilios, contactos telefónicos, direcciones de correo electrónico, servicios que prestan (cuando aplica), productos que ofrecen (cuando aplica) y fechas de contratación.	Contabilidad
A4	Bases de datos impuestos	Datos/información	Donde se procesa la información relacionada con IVA, pago a cuenta, informes de obligación fiscal.	Contabilidad

A5	Bases de datos gestión de cobro	Datos/información	Base de datos donde se gestiona los cobros a clientes representados u otros puestos de bolsa, fechas de contratación, control de ordenes de entrega de productos o servicios, formas de pago, control de documentación de soporte, fechas de cobro, montos de cobro, liquidaciones de contratos	Contabilidad
A6	Base de datos de gestión de pago	Datos/información	Base de datos donde se gestiona los pagos a clientes representados u otros puestos de bolsa, fechas de contratación, control de ordenes de entrega de productos o servicios, formas de pago, control de documentación de soporte, fechas de pago, montos de pago, liquidaciones de contratos	Contabilidad
A7	Bases de datos contabilidad	Datos/información	Base de datos que procesa todas las operaciones contables de la entidad, entre ellas están: gestión de partidas de diario, libro mayor, movimientos de cuentas, balances de comprobación, estados financieros, catálogo de cuentas, cierres contables, parámetros de sistema.	Contabilidad
A8	Lector de huellas	Datos/información	Es un dispositivo de hardware cuya finalidad es detectar, escanear y leer una huella dactilar de una persona que permita identificarlo y así generar el acceso a dispositivos u oficinas. Estos lectores se encuentran desde la entrada a recepción hasta cada oficina dentro de la empresa	Administración y finanzas

A9	Datos de autenticación	Datos/información	Nombre de usuarios y contraseñas de acceso a las cuentas de usuario o administrador de las computadoras, bases de datos o aplicaciones instaladas. Cada empleado debe modificar su contraseña cada 30 días.	Todos los empleados
A10	Computadoras de escritorio	Equipos informáticos	Los equipos de cómputo asignados al personal de la empresa	Todos los empleados
A11	Cámaras de seguridad	Equipos informáticos	La video vigilancia se integra de un grabador digital, un disco duro donde se almacenan las grabaciones y las cámaras necesarias para vigilar un lugar determinado. Existen 6 cámaras instaladas en toda la empresa.	Administración y finanzas
A12	Servidor en red	Equipos informáticos	Es el ordenador que permite el acceso a los recursos compartidos entre los equipos de cómputo u otros servidores conectados en una red informática. Solo existe 1 servidor, ubicado en oficinas de Administración y Finanzas.	Administración y finanzas
A13	Computaras portátiles	Equipos informáticos	Es un equipo informático personal que puede ser transportado fácilmente. Estos son utilizados por los agentes de bolsa únicamente cuando deben salir a reuniones fuera del puesto de bolsa.	Gerencia general y agentes de bolsa
A14	Impresoras	Equipos informáticos	Periférico que permite trasladar gráficos y texto a papel en físico. Se encuentran en los lugares de trabajo de cada empleado. Existen 7 impresoras.	Todos los empleados

A15	Sistema de alarmas	Equipo auxiliar	Equipos electrónicos instalados en lugares estratégicos para detectar movimientos sospechosos mediante sensores, uso de contactos magnéticos, detectores de humo. Es gestionado por Administración y Finanzas.	Administración y finanzas
A16	Escáner	Equipos informáticos	Periférico de la computadora que permite digitalizar imágenes impresas para transferirla a un dispositivo externo.	Todos los empleados
A17	Unidades Flash	Equipos informáticos	Es un dispositivo de almacenamiento que permite guardar información haciendo uso de la memoria flash. Cada empleado posee una unidad flash.	Todos los empleados
A18	Máquina de fax	Equipos informáticos	Equipo de oficina en el cual mediante trasmisión telefónica se remite información escaneada-impresa a un tercero interesado.	Todos los empleados
A19	Oficinas	Instalaciones	Instalación física donde se realizan las operaciones de la entidad y el procesamiento de datos.	Todos los empleados
A20	Sala de servidores	Instalaciones	Espacio físico en que se encuentran colocados los servidores y sus complementos necesarios para su correcto funcionamiento.	Gerencia general y administración y finanzas
A21	Instalaciones eléctricas	Instalaciones	Conjunto de cableado y otros dispositivos para la distribución de energía eléctrica en la edificación de la entidad.	Servicios externos
A22	Gabinetes de protección	Instalaciones	Muebles con la finalidad de proteger documentación física y otros activos.	Todos los empleados
A23	Bodega de almacenamiento	Instalaciones	Sala o espacio físico para almacenar documentación física.	Administración y finanzas

A24	Recepcionista	Personal	Personal encargado a la atención a visitantes y llamadas, proporcionando información autorizada por sus superiores.	Recursos humanos
A25	Personal de contabilidad	Personal	Encargados del procesamiento de información financiera y contable de la entidad.	Recursos humanos
A26	Gerentes	Personal	Encargado de la toma de decisiones mediante el análisis de la información que obtiene de diferentes áreas de la entidad, así como; de aquella información que proviene de partes externas.	Recursos humanos
A27	Oficial de cumplimiento	Personal	Se encarga de controlar e informar a la Fiscalía General de la Republica sobre las transacciones que realiza la entidad como un medio en que da fe pública que el Puesto de Bolsa de productos y servicios no se encuentra vinculado con el lavado de dinero y delitos conexos.	Recursos humanos
A28	Agentes de bolsas	Personal	Su función es realizar las negociaciones con la BOLPROS y los clientes.	Recursos humanos
A29	Mensajero	Personal	Encargado de llevar y traer correspondencia de la entidad.	Recursos humanos
A30	Líneas telefónicas	Redes de Comunicación	Cableado físico u otro medio de transmisión de señales que conecte el aparato telefónico del usuario a la red de telecomunicaciones.	Servicios externos
A31	Red LAN	Redes de Comunicación	Conexión entre el servidos y los ordenadores y periféricos de la entidad para facilitar la transmisión de información de forma interna.	Servicios externos

A32	Red Wifi Corporativa	Redes de Comunicación	Red de conexión de los equipos móviles para acceder a los recursos de la red corporativa de la entidad.	Servicios externos
A33	Red Wifi de invitado	Redes de Comunicación	Red de conexión para invitados	Servicios externos
A34	Cableado de redes	Redes de Comunicación	Disposición de líneas por medio de las cuales fluye la información a través de la red.	Servicios externos
A35	Servidor Windows	Redes de Comunicación	Computador bajo sistema operativo Windows que provee de servicios en una red.	Servicios externos
A36	Dispositivos portátiles	Redes de Comunicación	Dispositivos electrónicos propiedad de la entidad para la extracción, difusión o almacenamiento de la información.	Servicios externos
A37	Correos electrónicos	Redes de Comunicación	Red de comunicación que permite transmitir y recibir información.	Servicios externos
A38	Sistemas operativos	Software	Software básico que facilita la interacción entre el usuario y demás programas un ordenador	Servicios externos
A39	Antivirus y firewall	Software	Software de administración de seguridad	Servicios externos
A40	Aplicaciones de trabajo	Software	Herramientas y accesorios incorporados al ordenador.	Servicios externos
A41	Documentación física clasificada	Soportes de información	Soporte físico del registro de las operaciones de la organización.	Todos los empleados
A42	Documentación digital clasificada	Soportes de información	Soporte digital de los registros de las operaciones de la organización.	Todos los empleados

A43	Copias de respaldo	Soportes de información	Medidas de seguridad y reserva de los archivos y directorios de la organización	Contabilidad y RRHH
A44	Manuales de usuarios	Soportes de información	Instructivos o guías de orientación.	Administración y finanzas
A45	Planta eléctrica	Equipamiento auxiliar	Generador de electricidad a través de combustión interna.	Servicios externos

Fuente: *(Silva, 2015) (Aguirre Cardona & Aristizabal Betancourt, 2013)*

3.2. DETERMINACIÓN DE LOS RIESGOS DE LOS ACTIVOS DE INFORMACIÓN.

3.2.1. Criticidad de los activos.

Una vez identificados los activos de información se procedió a valorar su grado de importación y criticidad para la organización, para lo cual, se valoró la afectación o perdida que le puede generar a la entidad en cuanto aspectos financieros, legales y de imagen, en caso dado que al materializarse una amenaza afecte su disponibilidad, integridad o confidencialidad. Para tal efecto, se utilizaron los siguientes criterios para realizar la respectiva valoración:

Para tener una descripción general de los criterios que se utilizaron para realizar la respectiva valoración en la tabla propuesta N° 5 “Valoración de áreas significativas para definir criticidad de los activos”, se exponen las áreas afectadas, una descripción especifica del área y los criterios que representan los daños en aspectos financieros, legales y de imagen los cuales fueron valorados en una escala cuantitativa de menor a mayor impacto.

Tabla propuesta N° 5. Valoración de áreas significativas para definir criticidad de los activos de información.

Área afectada	Descripción	Criterio de valoración	Valor a asignar
Financiero	Pérdidas económicas generadas para la empresa por la falta, deterioro o modificación del activo o la información que procesa	No son pérdidas significativas	1
		Perdidas que provocan un impacto bajo dependiendo de las características e importancia del activo o la información que gestiona	2
		Pérdidas que propician un impacto económico moderado según las características e importancia del activo o a información que gestiona	3
		Perdidas que generan un impacto importante en función de las características y relevancia del activo o la información que gestiona	4
		Perdidas de impacto significativo en economía de la entidad según las características y relevancia del activo o la información que gestiona	5
Legales	Incumplimiento de aspectos legales de la entidad y litigios que puedan ocurrir.	No existen repercusiones relacionados con asuntos legales y contractuales	1
		Las entidades reguladoras dan a conocer sus observaciones sobre alguna eventualidad y/o interés de conocer la situación por las otras partes interesadas	2
		Se pueden generar sanciones escritas por parte de las entidades reguladoras y/o reclamos de terceros	3
		Se producen sanciones económicas por parte de las entidades reguladoras e inicio de litigios con terceros.	4
		Se pueden producir sanciones de mayor impacto por parte de las entidades reguladoras, terminación de contratos por incumplimientos, suspensión de licencias, cierre de operaciones y litigios de gran significancia.	5
Imagen corporativa	Perjuicio en contra del prestigio de la entidad	Eventos conocidos únicamente de forma interna en algunas áreas de la empresa, pero no ha sido divulgado al público y no son perjudiciales.	1
		Eventos conocidos internamente en toda la entidad y por algunas partes	2

		interesadas externas que pueden afectar levemente el prestigio a la entidad	
		Conocimiento de los eventos que llama la atención a las partes interesadas internas externas, y que tienen un impacto moderado en la imagen corporativa.	3
		Conocimiento de los eventos que produce un mayor énfasis de las partes interesadas sobre el desarrollo de dichas situaciones. Tiene un impacto significativo en la imagen corporativa.	4
		Las partes interesadas internas y externas se informan a detalle sobre las eventualidades que se desarrollan en el contexto de la empresa y que generan un impacto muy grave en la imagen corporativa.	5

Fuente: *(Silva, 2015) (Suárez, 2015)*

Los parámetros para definir la criticidad del activo fueron determinados a partir de una serie de interrogantes que tienen como finalidad cuestionar el daño que genera de forma económica, legal y de prestigio que los activos de información no estén disponibles y así mismo la información procesada en los mismos no sea integra y no se garantice la seguridad en cuanto al aspecto confidencial, en la Tabla propuesta N° 6 “Criterios para la valoración de los activos de información”, se listan los criterios de valoración en relación a la disponibilidad, integridad y confidencialidad de la información y como dichas áreas que resultan afectadas en la organización.

Tabla propuesta N° 6. Criterios para valorar criticidad de los activos de información.

Criterio	Área afectada	Pregunta
Disponibilidad	**Financiero**	Si el activo o la información procesada por este no se encuentra disponible ¿puede generar pérdidas económicas a la entidad?
	Legal	Si el activo o la información procesada por este no se encuentra disponible ¿puede ocasionar sanciones legales o litigios por parte de terceros para la entidad?
	Imagen corporativa	Si el activo o la información procesada por este no se encuentra disponible ¿pueden dañar la imagen corporativa de la entidad?
Integridad	**Financiero**	Si el activo o la información procesada por este se encuentre alterada ¿puede generar pérdidas económicas a la entidad?
	Legal	Si el activo o la información procesada por este se encuentre alterada ¿puede ocasionar sanciones legales o litigios por parte de terceros para la entidad?
	Imagen corporativa	Si el activo o la información procesada por este se encuentre alterada ¿pueden dañar la imagen corporativa de la entidad?
Confidencialidad	**Financiero**	La divulgación o revelación no autorizada de la información del puesto de bolsa de productos o servicios ¿puede generar pérdidas económicas a la entidad?
	Legal	La divulgación o revelación no autorizada de la información del puesto de bolsa de productos o servicios ¿puede ocasionar sanciones legales o litigios por parte de terceros para la entidad?
	Imagen corporativa	La divulgación o revelación no autorizada de la información del puesto de bolsa de productos o servicios ¿pueden dañar la imagen corporativa de la entidad?

Fuente: *(Silva, 2015)*

Para la determinación de los niveles de criticidad de los activos de información, se utilizó una metodología cuantitativa en relación a la gestión de los activos de información, en la tabla propuesta N° 7 “Escala de criticidad de los activos de información”, se muestran los niveles de criticidad en una escala cuantitativa y cualitativa de alto, medio, bajo o si no aplica en un dado caso la gestión de los activos de información no comprometen la disponibilidad, integridad y confidencialidad de la información.

Tabla propuesta N° 7. Escala de criticidad de los activos de información.

Criterio de evaluación	Valor crítico del activo	Escala de criticidad
La gestión del activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información de la empresa.	menor o igual a 5 y mayor a 4	**Alto**
La gestión del activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información.	menor o igual a 4 y mayor a 2	**Medio**
La gestión del activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información.	menor o igual a 2 y mayor a 0	**Bajo**
La gestión del activo no compromete la integridad, confidencialidad y disponibilidad de la de la información que procesa la entidad.	Igual a 0	**No aplica**

Fuente: *(Silva, 2015)*

De acuerdo con la metodología planteada con anterioridad la tabla propuesta N° 8 “Matriz de valoración de criticidad de los activos de información” representa los niveles de criticidad a los cuales se encuentran expuestos los activos de información y mediante una ponderación cuantitativa se identificaron los niveles de criticidad del activo y se determinó que tan importante es gestionarlos ya que comprometen la disponibilidad, integridad y confidencialidad de la información.

Tabla propuesta N° 8. Matriz de valoración criticidad de los activos de información.

Código de activo	Valoración nivel de criticidad del activo													Nivel de criticidad
	Confidencialidad			Integridad			Disponibilidad							
	Financiero	Legal	Imagen corporativa	Financiero	Legal	Imagen corporativa	Financiero	Legal	Imagen corporativa	Confidencialidad	Integridad	Disponibilidad	Valor total	
A1	3	1	5	5	3	5	5	3	5	3.0	4.3	4.3	3.9	MEDIO
A2	5	4	5	5	3	5	5	2	5	4.7	4.3	4.0	4.3	ALTO
A3	5	1	5	4	1	4	5	1	4	3.7	3.0	3.3	3.3	MEDIO
A4	5	5	4	5	5	5	5	4	5	4.7	5.0	4.7	4.8	ALTO
A5	5	1	3	5	1	3	5	1	3	3.0	3.0	3.0	3.0	MEDIO
A6	5	3	5	5	4	5	5	4	4	4.3	4.7	4.3	4.4	ALTO
A7	5	2	4	5	5	5	5	5	5	3.7	5.0	5.0	4.6	ALTO
A8	2	0	3	1	0	2	2	0	2	1.7	1.0	1.3	1.3	BAJO
A9	3	0	1	3	0	1	3	0	1	1.3	1.3	1.3	1.3	BAJO
A10	5	0	3	5	0	1	5	0	1	2.7	2.0	2.0	2.2	MEDIO
A11	3	1	3	1	1	2	3	1	3	2.3	1.3	2.3	2.0	BAJO
A12	5	2	5	5	2	5	5	3	5	4.0	4.0	4.3	4.1	ALTO
A13	5	0	3	5	0	3	5	0	3	2.7	2.7	2.7	2.7	MEDIO
A14	1	0	0	1	0	0	1	0	0	0.3	0.3	0.3	0.3	BAJO
A15	3	0	2	3	0	2	3	0	2	1.7	1.7	1.7	1.7	BAJO
A16	1	0	0	1	0	0	1	0	0	0.3	0.3	0.3	0.3	BAJO
A17	3	0	2	3	0	2	3	0	2	1.7	1.7	1.7	1.7	BAJO
A18	3	3	2	3	2	2	3	2	2	2.7	2.3	2.3	2.4	MEDIO
A19	4	2	3	1	0	0	3	4	2	3.0	0.3	3.0	2.1	MEDIO
A20	4	1	3	5	2	3	4	2	4	2.7	3.3	3.3	3.1	MEDIO
A21	2	1	1	1	1	1	5	3	4	1.3	1.0	4.0	2.1	MEDIO
A22	1	0	1	0	0	0	1	0	0	0.7	0.0	0.3	0.3	BAJO
A23	4	4	3	1	0	1	4	3	3	3.7	0.7	3.3	2.6	Medio
A24	5	5	5	4	5	4	3	3	3	5.0	4.3	3.0	4.1	ALTO
A25	5	5	5	5	5	5	5	5	4	5.0	5.0	4.7	4.9	ALTO
A26	5	5	5	4	5	4	5	4	4	5.0	4.3	4.3	4.6	ALTO
A27	4	5	3	5	5	4	3	4	4	4.0	4.7	3.7	4.1	ALTO
A28	5	5	5	4	5	5	4	4	4	5.0	4.7	4.0	4.6	ALTO
A29	5	5	4	4	4	4	4	4	4	4.7	4.0	4.0	4.2	ALTO

A30	4	2	3	3	0	3	3	2	3	3.0	2.0	2.7	2.6	**MEDIO**
A31	5	4	3	4	4	3	5	5	4	4.0	3.7	4.7	4.1	**ALTO**
A32	4	1	2	4	1	2	4	1	2	4.0	1.0	2.0	2.33	MEDIO
A33	2	0	2	1	0	2	1	0	2	1.3	0.0	2.0	1.1	BAJO
A34	3	1	3	3	1	2	4	0	2	3.3	0.7	2.3	2.1	MEDIO
A35	5	3	4	5	4	4	5	4	4	5.0	3.7	4.0	4.2	ALTO
A36	4	2	2	4	2	1	2	2	1	3.3	2.0	1.3	2.2	MEDIO
A37	4	3	2	5	3	4	5	3	2	4.7	3.0	2.7	3.4	MEDIO
A38	5	1	1	4	1	1	5	1	1	4.7	1.0	1.0	2.2	MEDIO
A39	5	1	4	4	3	3	5	3	4	4.7	2.3	3.7	3.6	MEDIO
A40	2	0	1	3	0	1	3	0	1	2.7	0.0	1.0	1.2	BAJO
A41	5	4	4	5	5	4	5	4	4	5.0	4.3	4.0	4.4	ALTO
A42	5	4	4	5	5	4	5	4	4	5.0	4.3	4.0	4.4	ALTO
A43	4	2	1	4	2	1	4	2	1	4.0	2.0	1.0	2.3	MEDIO
A44	1	0	1	1	0	1	1	0	1	1.0	0.0	1.0	0.7	BAJO
A45	1	0	1	1	0	1	2	0	2	1.3	0.0	1.3	0.9	BAJO

Fuente: *(Silva, 2015)*

3.2.2. Identificación de amenazas y vulnerabilidades.

Los activos de información están sujetos a muchos tipos de amenazas, las amenazas como tal tienen el potencial para causar un incidente de seguridad no deseado, el cual puede generar daños a los activos y por consiguiente a la organización como tal. El daño puede ocurrir por un ataque directo o indirecto a la información organizacional, la amenaza puede originarse de fuentes accidentales o de forma deliberada, pero para que una amenaza pueda originar daño tiene que valerse de la existencia de vulnerabilidades.

Las vulnerabilidades son debilidades asociadas con los activos organizacionales, de las cuales se valen los activos para generar incidentes no deseados, pero que terminan ocasionando pérdidas, daños o deterioro en los activos de información.

Con base a lo anterior, y para facilitar el proceso de identificación de amenazas y vulnerabilidades la Tabla propuesta N° 9 "Determinación de amenazas y vulnerabilidades", muestra un listo de amenazas donde se identifica el tipo de amenaza como tal, una descripción específica y la asociación de las vulnerabilidades existentes que en términos generales pueden a afectar a cualquier tipo de organización

Tabla propuesta N° 9. Determinación de amenazas y vulnerabilidades.

Tipo de Amenaza	Amenaza	Descripción amenaza	Vulnerabilidad asociada
Desastres naturales	Fenómenos meteorológicos	Cambios de la naturaleza que suceden por si solos y que puede influir en la vida humana y por consiguiente en la pérdida de la la información. (Lluvia, vientos, tormentas eléctricas, huracanes y tornados).	Áreas físicas en mal estado, falta de protección contra incendios e inundaciones.
	Fenómenos de origen volcánico	Liberación de gases y lava provocando un invierno volcánico.	Falta de protección contra incendios y contaminación.
	Inundaciones o daños por agua	Volumen de agua extremada que provoca bloqueo de drenajes, caída de árboles y tendido eléctrico	Falta de protección contra inundaciones e incendios por origen eléctrico
	Terremotos	Liberación de tenciones acumuladas en el interior de la tierra que provocan daños en la infraestructura, incendios, deslizamiento, licuación del suelo, creciente de ríos y quebradas, pérdidas humanas y desperfectos en el tendido eléctrico	Áreas físicas en mal estado o problemas de origen estructural donde se encuentra el activo.
	Incendios forestales	Fuego no controlado que puede causar daños en la infraestructura y los edificios.	Falta de protección contra incendios

	T-sunamis	Serie de olas originado por el desplazamiento de una masa de agua provocando inundaciones, daños en infraestructura y pérdidas humanas.	Falta de protección contra inundaciones, Áreas físicas en mal estado.
Desastres de origen industrial	Explosión de gas	Liberación súbita de gas a alta presión en el ambiente generando incendios, daños en los tendidos eléctricos y en la infraestructura.	Deterioro en las tuberías de gas
	Suspensión de servicios de comunicación	Afectación de la disponibilidad de redes y servicios.	Líneas de comunicación no protegidas, uniones de cables, deficientes conexiones.
	Corte del suministro eléctrico	Afectación en la disponibilidad del servicio de energía eléctrica	Estructura inadecuada del tendido eléctrico, uniones de cables y falta de recursos por parte de la organización
	Condiciones inadecuadas de temperatura o humedad	Condiciones climáticas no aptas.	Funcionamiento inadecuado del aire acondicionado. Ventilación insuficiente
	Degradación de los soportes de almacenamiento físico y lógico	Fragilidad de los soportes que pueden conducir a la perdida de información	Falta de mantenimiento.
Errores y fallos no intencionados	Errores de los usuarios	Incidentes no intencionados ocasionados por los distintos usuarios de la información o aquellos que son participes en su procesamiento poniendo en riesgo la confidencialidad, disponibilidad de e integridad de la información.	Ausencia de controles para el acceso limitado a los usuarios, verificación de la información y su almacenamiento.
	Errores del administrador	Cometidos en torno a la gestión de las tecnologías de la información de la entidad.	No se capacita al personal de la entidad.

	Errores de monitorización (log)	Fallas cometidas en la monitorización de los servidores.	Falta de controles para monitorizar los servidores de la entidad.
	Errores de configuración	Desacierto en la configuración de los activos que integran el sistema de información de la entidad.	Carencia de procedimientos adecuados para monitorizar la configuración de los programas y aplicativos de la entidad.
	Deficiencias de la organización	Cualquier área de la organización que no alcance sus objetivos o los logre de manera parcial.	Falta de una estructura organizativa en la cual se distribuyan las responsabilidades de una forma adecuada.
	Errores de [re-]encaminamiento	Fallos en los circuitos que comprenden como algunos participantes al menos dos dispositivos de abonado de un sistema de comunicaciones, siendo capaces dichos dispositivos de abonado de establecer una conexión conmutada por circuitos y una conexión conmutada por paquetes mediante elementos de red del sistema de comunicaciones, comprendiendo el procedimiento establecer.	No existen controles sobre el uso de cuentas de correo electrónico ni de acceso a la red, Falta de controles sobre el uso de redes sociales, chat, foros.
	Fuga de información	Incidente en el que se coloca en poder de un tercero la información confidencial de la entidad.	Ausencia de controles para el personal respecto al acceso que estos tienen en internet.
	Alteración accidental de la información	Modificación no intencional a la información de la entidad.	Ausencia de políticas para la verificación y almacenamiento de la información.

	Destrucción de la información	Eliminación de documentación física y digital de forma no intencional por los usuarios.	Carencia de controles criptográficos de la información digital, así como de respaldos automáticos; en tanto a la información física no se establecen políticas, así como su difusión en los usuarios para la desechar la documentación física de la entidad.
	Errores de mantenimiento / actualización de programas (software)	Inconsistencias ocasionadas durante el mantenimiento y las actualizaciones que se realizan a los programas o aplicativos informáticos de la entidad.	Carencia de controles para el mantenimiento y soporte preventivo o periódico de los programas y aplicativos que integran el sistema de información.
	Errores de mantenimiento / actualización de equipos (hardware)	Inconsistencias ocasionadas durante el mantenimiento y las actualizaciones que se realizan a los activos físicos de ofimática, así como también a sus periféricos.	Falta de controles para el mantenimiento y soporte preventivo o periódico de los dispositivos que integran el sistema de información.
	Caída del sistema informático por agotamiento de recursos	Condición en la cual una aplicación informática, ya sea un programa o parte o la totalidad del sistema operativo deja de funcionar de la forma esperada y dejan de responder a otras partes del sistema.	Ausencia de controles que permitan medir la capacidad de los recursos físicos y lógicos de la entidad.
	Pérdida de equipos	Extravío de periféricos del sistema informático.	Ausencia de controles para el acceso a personal no autorizado a las

			instalaciones de la entidad.
	Indisponibilidad del personal	Ausencia total o parcial de los empleados de la entidad para un proceso o actividad específica.	No se capacita ni concientiza a los empleados.
Actos deliberados	Fuga o divulgación de información por parte del personal	Son acciones que pueden realizar los empleados para extraer información y transmitirla a personas no autorizadas	No existencia de una política de confidencialidad o contratos confidencialidad
	Accesos no autorizados a las oficinas	Entrada de personas no autorizadas a las instalaciones del a empresa, en horas laborales o no.	No utilización de sistemas biométricos para acceso, inexistencia de cámaras de seguridad o defectuosidad de estas y el acceso no controlado de visitantes
	Suplantación de la identidad del usuario	Comúnmente conocido como "Phishing", valiéndose de fallos humanos, engañan a los usuarios de internet, con páginas falsas cuyo objetivo es extraer datos de autenticación de acceso.	Contraseñas no seguras, no auditoría de cuentas de usuario, no existencia de Logs de eventos de seguridad, inadecuada asignación de roles y permisos.
	Abuso de privilegios de acceso	Utilizar esos privilegios para asumir la propiedad de cualquier archivo, modificar registros y eventos o realizar algún acto indebido para dañar o beneficiarse de forma deliberada	Medidas de control inadecuadas sobre los administradores de TI o responsables de esta área.
	Robo	Acción de extraer equipo de TI, accesorios, software, datos confidenciales, documentación física o digital	Falta de cámaras de seguridad, no vigilancia, deficiencia en sistema de alarma sistema de alarmas (si se posee), no hay puertas de acceso restringido y con sistema biométrico de autenticación
	Difusión de software dañino	Ingresar programas perjudiciales para el hardware o el correcto funcionamiento del sistema	No existe antivirus instalado, los usuarios no aplican

		operativo y las aplicaciones instaladas en este.	las medidas de seguridad establecidas.
	Instalación de software no autorizado	Proceso de instalar programas o aplicaciones que no han sido autorizadas por los responsables de las gestiones de TI en la empresa. Esto puede dañar el funcionamiento del sistema operativo algún software ya instalado.	Antivirus no instalado, inadecuada asignación de roles y permisos.
	Vandalismo	Destrucción o daño de equipo informático, información física o digital, al personal o cualquier otro activo de información, provocado por personas internas o externas a la entidad.	No existen cámaras de seguridad, vigilancia, seguridad perimetral.
	Acceso no autorizado a cuentas de usuario en las computadoras	Ingreso a los perfiles de Windows sin autorización del usuario propietario de la cuenta o responsable de la gestión de TI.	Guardar contraseñas de autenticación escritas en algún papel donde cualquiera puede verlo, proporcionar la contraseña a terceros.
	Interceptación de información en tránsito (correos, archivos, llamadas telefónicas o transmisiones de datos)	Es la captura de información no autorizada que está trasmitiéndose a su receptor, y que puede o no llegar a este. Se considera perteneciente a los delitos tipificados como de espionaje, es muy común debido a que puede ser realizado por cualquier persona, con independencia de sus características personales, es decir, sin requerir cualificación especial.	No aplicación de políticas de seguridad, inadecuada asignación de roles y permisos
	Modificación deliberada de la información	Acto de modificar los datos de archivos, documentos, bases de datos, sistema operativo, o software, sin autorización del responsable.	No asignación adecuada de roles y permisos.
	Copias no autorizadas de datos	Realización de copias de información. Ya sea física o digital sin el permiso correspondiente.	No asignación adecuada de roles y permisos.
	Conexión no autorizada de dispositivos en la red corporativa	Cuando se conectan a la red otros dispositivos que no sean de la empresa y que no han sido autorizados.	Controles de seguridad no aplicados, inadecuada asignación de roles y permisos

	Manipulación inadecuada o no autorizada de los equipos informáticos	Utilización de los equipos con fines que no sean en beneficio de la entidad.	Políticas no aplicadas, inadecuada gestión y asignación de roles y permisos, inadecuado forma de cifrar datos
	Robo de activos de información	Sustracción intencionada y no autorizada de los recursos tecnológicos y documentos	No adecuada gestión de la seguridad, inadecuada o ausencia de seguridad perimetral, políticas no aplicadas, inadecuada asignación de roles y permisos.
	Virus de computadora	Es un software malicioso que tiene como finalidad alterar el correcto funcionamiento de las computadoras, sin que el usuario sea consciente.	No hay un antivirus instalado den las computadoras, o si existe uno, esta desactualizado, o desactivado.
	Ingeniería social	Es una práctica que permite manipular a las personas con la finalidad de obtener información confidencial sobre procesos, personas, sistemas informáticos, debilidades organizacionales entre otros, cuyo objetivo sería obtener un beneficio o provocar un ataque que dañe significativamente a la entidad	Controles de seguridad no aplicados, inadecuada asignación de roles y permisos.
	Ataques de hacking no ético	Ataques contra la seguridad de los sistemas informáticos y el software instalado para conocer las vulnerabilidades de seguridad en TI, y con el objetivo de obtener algún beneficio y dañar a la entidad.	No hay un antivirus instalado den las computadoras, o si existe uno, esta desactualizado, o desactivado. Firewall no activado o inexistente
	Sabotaje	Manipulación de datos para provocar daños a propósito en la integridad, confidencialidad y disponibilidad de la información	No adecuada gestión de la seguridad, inadecuada o ausencia de seguridad perimetral, políticas no aplicadas, inadecuada asignación de roles y permisos.

Fuente: (Silva, 2015) (Barrantes Porras & Hugo Herrera, 2012) (Cepeda, 2016)

3.2.3. Riesgos de los activos de información.

Una vez que determinadas las amenazas y vulnerabilidades a las cuales se expone los activos de información, se procedió a identificar los riesgos asociados a dichos activos, por tal razón la Tabla propuesta N° 10 “Riesgos vinculados a los activos de información detalla un listado de riesgo a los cuales se expone los activos de información y que de forma general pueden afectar a cualquier tipo organización así mismo los principios de seguridad de la información en relación a la disponibilidad, integridad y confidencialidad de la información.

Tabla propuesta N° 10. Riesgos vinculados a los activos de información.

CODIGO DE RIESGO	RIESGO	ACTIVOS AFECTADOS	Objetivos de seguridad afectados		
			D	I	C
R1	Desastres naturales	Desde A10 hasta A41	X		
R2	Accesos no autorizados a oficinas, sistemas de información y equipos	A10 hasta A20, A41		X	X
R3	Ataques de hacking no ético (interno y externo)	A1 hasta A9, A31 hasta A33, A35, A38 hasta A40, A42 y A43	X	X	X
R4	Uso de privilegios de forma inadecuada	A1 hasta A9, A38 y A39, A42 y A43		X	X
R5	Interceptar sin autorización la información enviada o recibida	A30 hasta A33, A35 hasta A37, A41 y A42		X	X
R6	Robo, extravío o sabotaje de la información que es propiedad de la entidad.	A1 hasta A9, A12, A24 hasta A29, A35, A37, A38, A41 hasta A43.	X	X	X
R7	Indisponibilidad de los servicios proporcionados por fallas generadas por los sistemas informáticos o eléctricos.	A2 hasta A7, A12, A24 hasta A29, A35, A37 y A38.	X	X	
R8	Cambios o alteración de privilegios sin la respectiva autorización por parte del administrador	A1 A9, A11 y A12, A15, A24 hasta A33, A35 hasta A40.		X	X
R9	Acciones no intencionales por parte del administrador	A1 hasta A7, A11 y A12, A15, A30 hasta A33, A35 hasta A38 y A43.		X	

R10	Uso inadecuado o divulgación no autorizada de información de autenticación	A1 hasta A9, A24 hasta A29, A35, A37 y A38.		X	X
R11	Modificación de la información sin autorización pertinente	A1 al A7, A9, A24 al A30, A42 y A43	X	X	
R12	Extracción no autorizada de equipos	A13, A17, A24 al A30 y A37	X	X	
R13	Manipulación de los sistemas informáticos para propiciar daños o fraudes	A1 al A7, A9, A12, A24 al A36, A38 al A41 y A44	X	X	
R14	Instalación de software no autorizado en los equipos informáticos de la entidad	A1 al A7, A9, A12, A24 al A36, A38 al A41 y A44	X	X	X
R15	Suplantación de identidad de los usuarios y administradores	A1 al A10, A13, A14, A16 al A18 y A24 al A33,		X	X

Fuente: *(Aguila Portillo, Cruz Reyes, & Hernández Villacorta, 2009) (Franco, 2015)*

3.3. ANÁLISIS Y EVALUACIÓN DE RIESGOS

Para la evaluación de riesgos es necesario tomar en cuenta los siguientes puntos:

- El proceso de evaluación de amenazas y vulnerabilidades, para estimar el efecto producido en caso de pérdidas y establecer el grado de aceptación y aplicabilidad de las operaciones del negocio.
- Identificar los activos y las facilidades que pueden ser afectadas por las amenazas y vulnerabilidades.
- Análisis de los activos del sistema y las vulnerabilidades para establecer un estimado de pérdida esperada en caso de que ocurra ciertos eventos y la probabilidad estimada cuando ocurra. El propósito de una evaluación del riesgo es determinar si las contramedidas son adecuadas para reducir la probabilidad de la pérdida o impacto de la pérdida dentro del nivel aceptable.

3.3.1. Escalas de valoración de riesgo.

Por medio del análisis de riesgos se definió la probabilidad de ocurrencia de los riesgos y el impacto de los mismos, con el objetivo de obtener el nivel de riesgo inherente, el cual, facilita establecer el nivel de riesgo propio de la actividad sin necesidad de medidas y controles de seguridad que actualmente existen en la entidad para mitigar los riesgos.

Para determinar la probabilidad de ocurrencia de una amenaza sobre cada uno de los activos, se utilizaron los criterios de valoración descritos en la tabla propuesta N° 11.

Tabla propuesta N° 11. Escala de probabilidad de ocurrencia.

Valor Asignado	Valor Cualitativo
1	Inusual
2	Baja (dudosa)
3	Media (probable)
4	Alta (posible)
5	Muy Alta

Para determinar el impacto de los riesgos sobre la integridad, confidencialidad y disponibilidad sobre los activos de información se utilizaron los criterios de valoración cualitativo y cuantitativo de la tabla propuesta N° 12.

Tabla propuesta N° 12. Escala de valoración de impacto cuantitativo y cualitativo.

Impacto	Impacto cuantitavo (porcentaje sobre utilidad del ejercicio)	Impacto cualitativo (uno o más factores)	Valor
Muy bajo	Se obtendrá como resultado pequeñas pérdidas no significativas, menores o igual al 0.25%.	La seguridad de la información de la entidad no se afecta.	1
		La imagen corporativa de la entidad no se ve afectada ante las partes interesadas.	
		Genera insignificantes reprocesos en la entidad.	
		Puede recuperarse la información con rapidez y la misma calidad.	
Bajo	Se obtendrá como resultado pequeñas pérdidas poco significativas, mayores al 0.25% y menor o igual al 5%.	La seguridad de la información de la entidad no se afecta.	2
		La imagen corporativa de la entidad se ve levemente afectada ante las partes interesadas.	
		Genera reprocesos menores a la entidad.	
		Puede recuperarse la información en un tiempo moderado más no con la misma calidad.	
Medio	Se obtendrá como resultado pérdidas relevantes, mayores al 5% y menor o igual al 20%.	La seguridad de la información de la entidad se afecta en un grado menor o leve.	3
		La imagen corporativa de la entidad se ve medianamente afectada ante las partes interesadas.	
		Genera reprocesos moderados a la entidad.	
		Puede recuperarse la información más no con la misma calidad.	
Alto	Se obtendrá como resultado pérdidas muy importantes; mayores al 20% y menor o igual al 50%.	La seguridad de la información de la entidad se afecta en un grado mayor.	4
		La imagen corporativa de la entidad se ve altamente afectada ante las partes interesadas.	
		Genera reprocesos mayores a la entidad.	
		La información se recupera con dificultad y sin la misma calidad.	
Muy alto	Se obtendrá como resultado pérdidas críticas, mayores al 50%.	La seguridad de la información de la entidad se afecta seriamente.	5
		La imagen corporativa de la entidad se afectada gravemente ante las partes interesadas.	
		Genera un alto nivel de reprocesos para la entidad.	
		La información se recupera con dificultad y a un alto costo.	
		Se ve afectado el negocio en marcha.	

Fuente: *(Silva, 2015)*

Para determinar el nivel de riesgo de los activos, se muestra en la tabla propuesta N° 13 el nivel de riesgo según el valor obtenido del producto entre la probabilidad de ocurrencia y el impacto,

provenientes de la tabla propuesta N° 11 y N° 12, respectivamente. El resultado del producto de estos, se debe buscar en la columna "valor del nivel de riesgo" para definir el nivel de riesgo y la gestión del mismo.

Tabla propuesta N° 13. Escala de valoración de nivel de riesgos.

Nivel de riesgo	Valor del nivel de riesgo	Gestión del riesgo
Riesgo Grave	Nivel de riesgo menor o igual a 25 y mayor o igual a 15	Requiere de atención máxima y es necesario ejecutar acciones inmediatas que consigan mitigar, compartir, transferir o eludir el riesgo.
Riesgo Alto	Nivel de riesgo menor a 15 y mayor o igual a 10	Se necesita atención urgente y ejecutar medidas para mitigar el nivel de riesgo
Riesgo Moderado	Nivel de riesgo menor a 10 y mayor o igual a 5	Se requiere de medidas rápidas e idóneas que permitan disminuir el riesgo a bajo o mínimo
Riesgo Bajo	Nivel de riesgo menor a 5 y mayor o igual a 2	El riesgo se puede mitigar con actividades propias y mediante acciones preventivas para disminuir el riesgo
Riesgo Mínimo	Nivel de riesgo menor a 2 y mayor o igual a 0	El riesgo es aceptable con independencia de si se toman otras medidas de control diferentes a las determinadas. También pueden ser riesgos eliminables.

Fuente: (Silva, 2015)

3.3.2. Determinación de nivel de riesgo.

En este apartado se describe el resultado del proceso de valoración del riesgo inherente de las amenazas asociadas a los activos de información de IBES, S.A. de C.V. Primero se define el nivel de riesgo cualitativo, el cual se expone en la tabla propuesta N° 14 partiendo del impacto que este puede ocasionar a los objetivos del a seguridad de la información: Disponibilidad (D), Integridad (I) y Confidencialidad (C). Además de la probabilidad de ocurrencia del mismo.

Se utiliza la columna 3 de la tabla propuesta N° 12 (impacto cualitativo), para lo cual en cada riesgo se pondrá el valor de impacto en letras a cada componente de la seguridad que se vea vulnerado. Luego se define la probabilidad de ocurrencia en letras y al final se estimará una valoración de riesgo por cada área, y posteriormente un nivel de riesgo cualitativo total.

Tabla propuesta N° 14. Valoración cualitativa de riesgo inherente de activos de información.

Código Riesgo	Valoración de impacto			Probabilidad de ocurrencia	Estimación de Riesgo			Nivel de Riesgo
	D	I	C		D	I	C	
R1	Muy Alto			Inusual	Moderado			Moderado
R2		Alto	Medio	Alta		Grave	Alto	Grave
R3	Alto	Alto	Muy Alto	Inusual	Bajo	Bajo	Moderado	Bajo
R4		Alto	Alto	Media	Alto	Alto		Alto
R5	Medio	Medio	Alto	Inusual	Bajo	Bajo	Bajo	Bajo
R6	Alto		Muy Alto	Alta	Grave		Grave	Grave
R7	Medio			Baja	Moderado			Moderado
R8		Alto	Muy Alto	Media		Alto	Grave	Alto
R9	Alto	Medio		Alta	Grave	Alto		Alto
R10			Medio	Media			Moderado	Moderado
R11	Muy Alto	Muy Alto		Alta	Grave	Grave		Grave
R12	Medio	Medio		Media	Moderado	Moderado		Moderado
R13	Muy Alto	Muy Alto		Alta	Grave	Grave		Grave
R14	Medio	Medio	Medio	Baja	Moderado	Moderado	Moderado	Moderado
R15		Media	Bajo	Media	Moderado	Moderado		Moderado

Fuente: *(Silva, 2015)*

En la tabla propuesta N° 15 se determinó el nivel de riesgo cuantitativo (inherente) utilizando las mismas tablas que en el proceso anterior (determinación de riesgo cualitativo), con la diferencia que la probabilidad de ocurrencia y el impacto son valores numéricos enteros.

Tabla propuesta N° 15. Valoración cuantitativa de riesgo inherente de activos de información.

Código Riesgo	Probabilidad de ocurrencia	Impacto	Ponderación del riesgo	Nivel de Riesgo
R1	1	5	5	MODERADO
R2	4	4	16	GRAVE
R3	1	4	4	BAJO
R4	4	3	12	ALTO
R5	1	3	3	BAJO
R6	4	5	20	GRAVE
R7	2	3	6	MODERADO
R8	3	4	12	ALTO
R9	4	3	12	ALTO
R10	3	3	9	MODERADO
R11	5	4	20	GRAVE
R12	2	3	6	MODERADO
R13	3	5	15	GRAVE
R14	2	3	6	MODERADO
R15	2	3	6	MODERADO

Fuente: *(Silva, 2015)*

3.3.3. Mapa de calor.

En concordancia y alineado con los niveles de riesgo, el mapa de calor es una herramienta que permite la representación gráfica de los riesgos ya que estos son ubicados por zonas de acuerdo a la probabilidad e impacto. Es importante mencionar que dentro del mapa calor cada zona de ubicación corresponde a un tipo de riesgo en específico. Con base a lo anterior, la Figura propuesta N° 4 “Guía de mapa de calor”, representa la descripción general de las zonas que se tuvieron en cuenta para valorar los riegos inherentes y poder ubicarlos dentro del mapa.

Figura propuesta N° 2. Guía de mapa de calor.

Zona de Riesgo Medio 5 puntos Reducir el riesgo a niveles más bajos	Zona de Riesgo Alto 10 puntos Acciones urgentes para mitigar riesgo	Zona de Riesgo Grave 15 puntos Atención máxima y acciones inmediatas	Zona de Riesgo Grave 20 puntos Atención máxima y acciones inmediatas	Zona de Riesgo Grave 25 puntos Atención máxima y acciones inmediatas
Zona de Riesgo Bajo 4 puntos Acciones preventivas para mitigar riesgo	Zona de Riesgo Medio 8 puntos Reducir el riesgo a niveles más bajos	Zona de Riesgo Alto 12 puntos Acciones urgentes para mitigar riesgo	Zona de Riesgo Grave 16 puntos Atención máxima y acciones inmediatas	Zona de Riesgo Grave 20 puntos Atención máxima y acciones inmediatas
Zona de Riesgo Bajo 3 puntos Acciones preventivas para mitigar riesgo	Zona de Riesgo Medio 6 puntos Reducir el riesgo a niveles más bajos	Zona de Riesgo Medio 9 puntos Reducir el riesgo a niveles más bajos	Zona de Riesgo Alto 12 puntos Acciones urgentes para mitigar riesgo	Zona de Riesgo Grave 15 puntos Atención máxima y acciones inmediatas
Zona de Riesgo Mínimo 2 puntos Aceptación del riesgo	Zona de Riesgo Bajo 4 puntos Acciones preventivas para mitigar riesgo	Zona de Riesgo Medio 6 puntos Reducir el riesgo a niveles más bajos	Zona de Riesgo Medio 8 puntos Reducir el riesgo a niveles más bajos	Zona de Riesgo Alto 10 puntos Acciones urgentes para mitigar riesgo
Zona de Riesgo Mínimo 1 punto Aceptación del riesgo	Zona de Riesgo Mínimo 2 puntos Aceptación del riesgo	Zona de Riesgo Bajo 3 puntos Acciones preventivas para mitigar riesgo	Zona de Riesgo Bajo 4 puntos Acciones preventivas para mitigar riesgo	Zona de Riesgo Medio 5 puntos Reducir el riesgo a niveles más bajos

Fuente: *(Silva, 2015)*

Una vez realizada la valorización de probabilidad e impacto de cada uno de los riesgos determinados, se procedió a efectuar una multiplicación entre estas variables para conocer el valor del riesgo. Por lo tanto, la figura N° 2 Ubicación del riesgo inherente en mapa de calor representa la relación entre probabilidad e impacto teniendo como resultado la determinación del riesgo y consecuentemente la ubicación en las zonas de riesgo determinadas.

Figura propuesta N° 3. Ubicación de riesgos inherentes determinados en mapa de calor.

		R13	R6	
		R4, R8, R9	R2	R11
	R7, R12, R14, R15	R10		
		R3	R5	R1

3.4. PLAN DE GESTIÓN DE RIESGOS

Una vez realizado la evaluación del riesgo a la cual se encuentran expuestos los activos de información de IBES, S.A. de C.V. y con el objetivo de gestionarlo se han determinado los planes de tratamiento del riesgo orientados a garantizar las características de disponibilidad, integridad y confidencialidad de la información, la decisión de gestionar el riesgo es basado en dos aspectos fundamentales:

- El impacto generado si el riesgo se materializa
- Con que frecuencia este puede suceder.

Estos indicadores brindan el panorama ideal sobre el daño o la perdida que se podría generar si el riesgo se materializa y si no se establezca acciones para su mitigación.

3.4.1. Opciones de tratamiento de riesgo.

Ante lo expuesto con anterioridad, se presenta 4 estrategias básicas para la gestión del riesgo en la tabla propuesta N° 16, que sirven como orientación ante las acciones a seguir por parte de la administración antes y después de que el riesgo se materialice.

Tabla propuesta N° 16. Criterios para el tratamiento del riesgo.

Opción	Acción
Evitar el riesgo	Implementación de medidas enfocada a impedir que el riesgo se materialice.
Reducir el riesgo	Establecimiento de medidas que disminuyan la probabilidad de ocurrencia del riesgo y el impacto generado.
Transferir el riesgo	Ante la ocurrencia del riesgo y con la finalidad de disminuir el daño o la pérdida, responsabilizar a tercer mediante el traslado del riesgo como ejemplo compañías de seguros.
Asumir el riesgo	Materializado el riesgo y ante el no establecimiento de medidas para su mitigación se debe aceptar el riesgo.

Fuente: *(Plaza, 2015) (Aguila Portillo, Cruz Reyes, & Hernández Villacorta, 2009)*

Expuestas las estrategias de gestión de riesgo es necesario identificar y evaluar las opciones para tratamiento del riesgo, la selección de dichas opciones de control debe hacerse tomando en cuenta los criterios para el tratamiento del riesgo, así como también los requerimientos legales, regulatorios y contractuales, el propósito de este contexto es definir cuál debe ser la actuación más apropiada por parte de la Alta Dirección frente a la gestión que debe dar a los riesgo identificados con base a los criterios para el tratamiento del riesgo la tabla propuesta N° 17, la cual muestra las opciones que se establecieron para cada uno de los riesgos identificados.

Tabla propuesta N° 17. Determinación de opción de tratamiento a riesgos de los activos de información.

Código de Riesgo	Riesgo	Riesgo	Opción de Tratamiento
R1	Desastres naturales	MODERADO	Reducir el riesgo
R2	Accesos no autorizados a oficinas, sistemas de información y equipos	GRAVE	Evitar el riesgo
R3	Ataques de hacking no ético (interno y externo)	BAJO	Reducir el riesgo
R4	Uso de privilegios de forma inadecuada	ALTO	Reducir el riesgo
R5	Interceptar sin autorización la información enviada o recibida	BAJO	Reducir el riesgo
R6	Robo, extravió o sabotaje de la información que es propiedad de la entidad.	GRAVE	Evitar el riesgo
R7	Indisponibilidad de los servicios proporcionados por fallas generadas por los sistemas informáticos o eléctricos.	MODERADO	Reducir el riesgo
R8	Cambios o alteración de privilegios sin la respectiva autorización por parte del administrador	ALTO	Evitar el riesgo
R9	Acciones no intencionales por parte del administrador	ALTO	Reducir el riesgo
R10	Uso inadecuado o divulgación no autorizada de información de autenticación	MODERADO	Evitar el riesgo
R11	Modificación de la información sin autorización pertinente	GRAVE	Evitar el riesgo
R12	Extracción no autorizada de equipos	MODERADO	Reducir el riesgo
R13	Manipulación de los sistemas informáticos para propiciar daños o fraudes	GRAVE	Evitar el riesgo
R14	Instalación de software no autorizado en los equipos informáticos de la entidad	MODERADO	Reducir el riesgo
R15	Suplantación de identidad de los usuarios y administradores	MODERADO	Reducir el riesgo

3.4.2. Determinación de la gestión de riesgo.

Luego de realizar el proceso de identificación de opciones de tratamiento del riesgo, se deben seleccionar los objetivos de control y controles que se aplicaran a estas opciones de gestión del riesgo. La selección de controles debe llevarse a cabo considerando los criterios determinados para la aceptación del riesgo, así como los requerimientos legales, reguladores y contractuales.

De acuerdo con la NTS ISO/IEC 27001:2013, en la cláusula 6.1.3. Tratamiento del riesgo de seguridad de la información, la selección de los objetivos de control y los controles deben ser comparados con los establecidos en el Anexo A de dicha norma, para asegurarse no haber obviado algún control necesario.

La finalidad de este apartado es definir la acción y controles tomados del Anexo A, para darle un tratamiento adecuado a cada uno de los riesgos identificados, considerando la información expuesta en la tabla propuesta N° 17, donde se definió la opción de tratamiento a cada riesgo. A continuación, en la tabla propuesta N° 18 se muestra el plan de tratamiento para los activos y sus respectivos riesgos identificados., además designando al responsable de vigilar el cumplimiento de estos controles (tomado de las áreas del esquema organizacional del SGSI de IBES).

Tabla propuesta N° 18. Plan de gestión de riesgo.

Riesgos	Activos	Opción de tratamiento de riesgo	Actividades a realizar	Controles	Responsable
Desastres naturales	Desde A10 hasta A41	Transferir el riesgo	Contratar un seguro contra algún suceso de la naturaleza Ejecutar controles de protección de los activos	✓ A.6.1.3. Contacto con autoridades. ✓ A.11.1.1. Perímetro de seguridad física. ✓ A.11.1.3. Seguridad de oficinas, habitaciones e instalaciones. ✓ A.11.1.4. Protección contra amenazas externas. ✓ A.11.1.5. Trabajo en áreas seguras. ✓ A.11.2.1. Ubicación y protección del equipo. ✓ A.11.2.3. Seguridad de cableado. ✓ A.11.2.6. Seguridad del equipo y activos fuera de las instalaciones.	Comité de seguridad
Accesos no autorizados a oficinas, sistemas de información y equipos	A10 hasta A20, A41	Evitar el riesgo	Hacer una revisión periódica del estado de los usuarios, sus rolles y privilegios en el sistema de control de acceso a oficinas, bases de datos, aplicaciones y sistemas operativos. Ejecutar con frecuencia campañas de seguridad, capacitación y concientización	✓ A.6.1.1. Roles y responsabilidades de la seguridad de la información. ✓ A.6.1.2. Segregación de funciones. ✓ A.7.1.1. Selección de personal. ✓ A.7.1.2. Términos y condiciones de empleo. ✓ A.7.2.2. Capacitación, educación y concientización sobre la seguridad de la información. ✓ A.8.1.2. Propiedad de los activos. ✓ A.9.1. Requerimiento del negocio para el control de acceso. ✓ A.9.2. Gestión del acceso de usuarios. ✓ A.9.3. Responsabilidades del usuario.	Dirección de Tecnología y Seguridad de la Información

			Ejecutar pruebas de Hacking Ético de forma periódica que permita determinar el nivel de protección de la infraestructura de TI. Revisar frecuentemente las bitácoras de entrada a las áreas de seguridad y los Logs de eventos de seguridad	✓ A.9.4. Control de acceso a sistemas y aplicaciones. ✓ A.11.1.1. Perímetro de seguridad física. ✓ A.11.1.2. Controles de entrada físicos. ✓ A.11.1.3. Seguridad de oficinas, ✓ habitaciones e instalaciones. ✓ A.11.1.4. Protección contra amenazas externas y ambientales. ✓ A.11.1.6. Áreas de carga y descarga. ✓ A.11.2.1. Ubicación y protección de equipo. ✓ A.11.2.8. Equipo desatendido de usuario. ✓ A.11.2.9. Política de escritorio y pantalla limpia. ✓ A.12.4.2. Protección de la bitácora de información. ✓ A.12.4.3. Bitácoras del administrador y operador.	
Ataques de hacking no ético (interno y externo)	A1 hasta A9, A31 hasta A33, A35, A38 hasta A40, A42 y A43	Reducir el riesgo	Ejecutar pruebas de Hacking Ético de forma periódica que permita determinar el nivel de protección de la infraestructura de TI. Instalación, revisión y actualización (periódica) de un antivirus, antimalware y firewall corporativo	✓ A.6.1.1. Roles y responsabilidades de seguridad de la información. ✓ A.6.1.2. Segregación de funciones. ✓ A.7.1.1. Selección de personal. ✓ A.7.1.2. Términos y condiciones de empleo. ✓ A.7.2.2. Capacitación, educación y concientización sobre la seguridad de la información. ✓ A.7.2.3. Proceso disciplinario. ✓ A.10.1. Controles criptográficos. ✓ A.12.2.1. Controles contra software malicioso. ✓ A.12.6. Gestión de la vulnerabilidad técnica. ✓ A.12.7. Consideraciones en la auditoria de sistemas de información.	Dirección de Tecnología y Seguridad de la Información

				✓ A.13.1. Gestión de seguridad de red. ✓ A.14.1.2. Aseguramiento de servicios de aplicación en redes públicas.	
Uso de privilegios de forma inadecuada	A1 hasta A9, A38 y A39, A42 y A43	Reducir el riesgo	Revisar frecuentemente las bitácoras de entrada a las áreas de seguridad y los Logs de eventos de seguridad Hacer una revisión periódica del estado de los usuarios, sus roles y privilegios en el sistema de control de acceso a oficinas, bases de datos, aplicaciones y sistemas operativos. Borrar (si es necesario) o bloquear cuentas de super usuario. Cuando sea el caso de bloquear la cuenta, la contraseña de esta debe ser gestionada por el oficial de seguridad.	✓ A.6.1.1. Roles y responsabilidades de la seguridad de la información. ✓ A.6.1.2. Segregación de funciones. ✓ A.6.1.3. Contacto con autoridades. ✓ A.7.1. Antes del empleo. ✓ A.7.2. Durante el empleo. ✓ A.9.2.2. Provisión de accesos de usuarios. ✓ A.9.2.3. Gestión de privilegios de derechos de acceso. ✓ A.9.2.4. Gestión de la información de autenticación secreta de los usuarios. ✓ A.9.3. Responsabilidades del usuario. ✓ A.9.4. Control de acceso a sistemas y aplicaciones. ✓ A.12.4. Registro y monitoreo.	Gestión de riesgos

			Todos los cambios significativos deben ser revisados y pre-aprobados por los encargados de cada área y luego informarlo al comité de seguridad para su aprobación final.		
Interceptar sin autorización la información enviada o recibida	A30 hasta A33, A35 hasta A37, A41 y A42	Reducir el riesgo	Implementar medidas que aseguren el cifrado de información intercambiada con terceros mediante correo electrónico Gestión documental de archivos físicos Escucha telefónicas únicamente para fines de identificar interceptores de información	✓ A.6.1.2. Segregación de funciones. ✓ A.6.1.4. Contacto con grupos de especial interés. ✓ A.6.2. Dispositivos móviles y trabajo remoto. ✓ A.7.1.1. Selección de personal. ✓ A.7.2.1. Responsabilidades de la dirección. ✓ A.7.2.2. Capacitación, educación y concientización sobre la seguridad de la información. ✓ A.7.2.3. Proceso disciplinario. ✓ A.7.3. Terminación y cambio de empleo. ✓ A.8.1.3. Uso aceptable de los activos. ✓ A.8.1.4. Devolución de los activos. ✓ A.13.1. Gestión de seguridad de red. ✓ A.13.2. Transferencia de información.	Gestión de riesgos
Robo, extravío o sabotaje de la información que es propiedad de la entidad.	A1 hasta A9, A12, A24 hasta A29, A35, A37, A38, A41 hasta A43.	Evitar el riesgo	Revisar con frecuencia el estado de los usuarios, sus roles y privilegios de los sistemas. Implementar medidas de cifrado de los discos duros de	✓ A.6.1.1. Roles y responsabilidades de la seguridad de la información. ✓ A.6.1.2. Segregación de funciones. ✓ A.6.2. Dispositivos móviles y trabajo remoto. ✓ A.7.1. Controles antes del empleo. ✓ A.7.2. Controles durante el empleo. ✓ A.8.1. Responsabilidad sobre los activos	Gestión de Seguridad de Recursos Humanos

			dispositivos móviles y portátiles. Clasificación de la información según su confidencialidad. Asegurar la aplicación del bloqueo de dispositivos externos en los equipos de cómputo de la empresa Verificar continuamente los Logs de eventos de seguridad	✓ A.8.2. Clasificación de la información. ✓ A.8.3. Gestión de medios (dispositivos donde se guarda información). ✓ A.9.1. Requerimientos del negocio para el control de acceso. ✓ A.9.2. Gestión de acceso de usuarios. ✓ A.9.3. Responsabilidades del usuario. ✓ A.9.4. Control de acceso a sistemas y aplicaciones. ✓ A.10.1. Controles criptográficos. ✓ A.11.1.1. Perímetro de seguridad física. ✓ A.11.1.2. Controles de entrada físicos. ✓ A.11.1.4. Protección contra amenazas externas y ambientales. ✓ A.11.2.8 Equipo desatendido de usuario. ✓ A.11.2.9. Política de escritorio y pantalla limpia. ✓ A.12.4.1. Registro de eventos. ✓ A.12.4.2 Protección de la bitácora de información. ✓ A.12.4.3. Bitácoras del administrador y operador.	
Indisponibilidad de los servicios proporcionados por fallas generadas por los sistemas informáticos o eléctricos.	A2 hasta A7, A12, A24 hasta A29, A35, A37 y A38.	Reducir el riesgo	Todos los cambios significativos deben ser revisados y pre-aprobados por los encargados de cada área y luego informarlo al comité de seguridad para su aprobación final.	✓ A.6.1.3 Contacto con autoridades. ✓ A.6.1.4 Contacto con grupos de especial interés. ✓ A.8.1.1 Inventario de activos. ✓ A.8.1.2 Propiedad de los activos. ✓ A.8.1.3 Uso aceptable de los activos. ✓ A.11.2.2. Herramientas de soporte. ✓ A.11.2.3 Seguridad en el cableado. ✓ A.11.2.4 Mantenimiento de equipo.	Dirección de Tecnología y Seguridad de la Información

			Garantizar que los contratos con los proveedores de TI suscriban acuerdos de niveles de servicios Asegurar la realización de pruebas de contingencia de TI	✓ A.12.6. Gestión de vulnerabilidades ✓ Técnicas. ✓ A 12.7.1. Controles de auditoria de los sistemas de información.	
Cambios o alteración de privilegios sin la respectiva autorización por parte del administrador	A1 A9, A11 y A12, A15, A24 hasta A33, A35 hasta A40.	Evitar el riesgo	Hacer una revisión periódica del estado de los usuarios, sus roles y privilegios en el sistema de control de acceso, bases de datos, aplicaciones y sistemas operativos. Se debe garantizar que se esté implementando la política de contraseña segura	✓ A.6.1.1 Roles y responsabilidades de la seguridad de la información. ✓ A.6.1.2 Segregación de funciones. ✓ A.7.2.1 Responsabilidades de la Dirección. ✓ A.7.2.2 Capacitación, educación y concientización sobre la seguridad de la información. ✓ A.7.2.3 Proceso disciplinario. ✓ A.8.1.3 Uso aceptable de los activos. ✓ A.9.1 Requerimiento del negocio para el control de acceso. ✓ A.9.2 Gestión del acceso de usuarios ✓ A.9.3.1. Uso de información de autenticación secreta. ✓ A.9.4. Control de acceso a sistemas y aplicaciones.	Dirección de Tecnología y Seguridad de la Información
Acciones no intencionales por parte del administrador	A1 hasta A7, A11 y A12, A15, A30 hasta A33, A35 hasta A38 y A43.	Reducir el riesgo	Asegurar el entrenamiento y capacitación adecuada del personal en cuanto a seguridad y manejo de TI Verificar continuamente los	✓ A.6.1.1 Roles y responsabilidades de la seguridad de la información. ✓ A.6.1.2 Segregación de funciones. ✓ A.7.1.1. Selección del personal. ✓ A.7.1.2 Términos y condiciones de empleo. ✓ A.7.2.1 Responsabilidades de la Dirección.	Gestión de Seguridad de Recursos Humanos

			Logs de eventos de seguridad Todos los cambios significativos deben ser revisados y pre-aprobados por los encargados de cada área y luego informarlo al comité de seguridad para su aprobación final.	✓ A.7.2.2 Capacitación, educación y concientización sobre la seguridad de la información. ✓ A.7.2.3 Proceso disciplinario. ✓ A.8.3.1 Gestiones de los medios removible. ✓ A.8.3.2 Eliminación de medios. ✓ A.8.3.3 Transferencia de medios físicos.	
Uso inadecuado o divulgación no autorizada de información de autenticación	A1 hasta A9, A24 hasta A29, A35, A37 y A38.	Evitar el riesgo	Asegurar la implementación bloqueo automático de pantalla por inactividad y de la política de contraseña segura. Ejecutar con frecuencia campañas de seguridad, capacitación y concientización	✓ A.9.1.1 Política de control de acceso. ✓ A.9.1.2 Acceso a redes y servicios de red. ✓ A.9.2.1 Registro y anulación de usuarios. ✓ A.9.2.2 Provisiones de acceso de usuarios. ✓ A.9.2.3 Gestión de privilegios de derecho de acceso. ✓ A.9.2.4 Gestión de información de autenticación secreta de los usuarios. ✓ A.9.3.1 Uso de información de autenticación secreta.	Gestión de riesgos
Modificación de la información sin autorización pertinente	A1 al A7, A9, A24 al A30, A42 y A43	Evitar el riesgo	Todos los cambios significativos deben ser revisados y pre-aprobados por los encargados de cada área y luego informarlo al comité de seguridad para su aprobación final.	✓ A.8.3.1 Gestiones de los medios removible. ✓ A.8.3.2 Eliminación de medios. ✓ A.8.3.3 Transferencia de medios físicos. ✓ A.9.1.1 Política de control de acceso. ✓ A.9.1.2 Acceso a redes y servicios de red. ✓ A.9.2.1 Registro y anulación de usuarios. ✓ A.9.2.2 Provisiones de acceso de usuarios. ✓ A.9.2.3 Gestión de privilegios de derecho de acceso.	Oficial de seguridad y gestión de riesgos

			Verificar continuamente los Logs de eventos de seguridad Hacer una revisión periódica del estado de los usuarios, sus roles y privilegios en el sistema de control de acceso a oficinas, bases de datos, aplicaciones y sistemas operativos.	✓ A.9.2.4 Gestión de la información de autenticación secreta de los usuarios. ✓ A.9.2.5 Revisión de los derechos de acceso. ✓ A.9.2.6. Remover o ajustar los derechos de acceso. ✓ A.10.1.1 Política sobre el uso de controles criptográficos. ✓ A.10.1.2 Gestión de llaves. ✓ A.12.3.1 Copia de seguridad de la información.	
Extracción no autorizada de equipos	A13, A17, A24 al A30 y A37	Reducir el riesgo	Implementar video vigilancia (en caso no existiera), mejorar la visualización de puntos ciegos en las oficinas o bodegas Ejecutar con frecuencia campañas de seguridad, capacitación y concientización	✓ A.7.2.1 Responsabilidad de la Dirección. ✓ A.7.2.2 Capacitación, educación y concientización sobre la seguridad de la información. ✓ A.7. 2.3 Proceso disciplinario. ✓ A.8.1.1 Inventario de activos. ✓ A.8.1.2 Propiedad de los activos. ✓ A.11.2.1 Ubicación y protección del equipo. ✓ A.11.2.5 Retiro de Activos. ✓ A.11.2.6 Seguridad del equipo y de activos fuera de las instalaciones.	Dirección de Tecnología y Seguridad de la Información
Manipulación de los sistemas informáticos para propiciar daños o fraudes	A1 al A7, A9, A12, A24 al A36, A38 al A41 y A44	Evitar el riesgo	Garantizar una adecuada segregación de responsabilidades Verificar continuamente los Logs de eventos de seguridad	✓ 6.1.2 Segregación de funciones. ✓ A. 6.2.1 Política de dispositivos móviles. ✓ A.7.2.3 Proceso disciplinario. ✓ A. 9.4.1 Restricción de acceso a la información. ✓ A.9.4.2 Procedimientos seguros de inicios de sesión.	Dirección de Tecnología y Seguridad de la Información "

			Hacer una revisión periódica del estado de los usuarios, sus roles y privilegios en el sistema de control de acceso a oficinas, bases de datos, aplicaciones y sistemas operativos.	✓ A.9.4.3 Sistema de gestión de contraseñas. ✓ A.9.4. 4. Uso de programas utilitarios privilegiados. ✓ A.9.4.5 Control de acceso al código fuente. ✓ A.11.2.1 Ubicación y protección del equipo.	
Instalación de software no autorizado en los equipos informáticos de la entidad	A1 al A7, A9, A12, A24 al A36, A38 al A41 y A44	Reducir el riesgo	Garantizar la implementación debida de la política que restringe la instalación de software por usuarios no autorizados.	✓ A.7.2.2 Capacitación, educación y concientización sobre la seguridad de la información. ✓ A.7.2.3 Proceso disciplinario. ✓ A.9.2.1 Registro y anulación de usuarios. ✓ A.9.2.2 Provisiones de acceso de usuarios. ✓ A.9.2.3 Gestión de privilegios de derecho de acceso, Proceso disciplinario. ✓ A. 9.4.1 Restricción de acceso a la información. ✓ A.9.4.2 Procedimientos seguros de inicios de sesión. ✓ A.9.4.3 Sistema de gestión de contraseñas, ✓ A.12.2.1 Controles contra Software maliciosos. ✓ A.12.5.1 Instalación de software en sistemas operacionales.	Dirección de Tecnología y Seguridad de la Información
Suplantación de identidad de los usuarios y administradores	A1 al A10, A13, A14, A16 al A18 y A24 al A33,	Reducir el riesgo	Verificar continuamente los Logs de eventos de seguridad	✓ A.5.1.1 Política de la seguridad de la información. ✓ A.7.2.1 Responsabilidad de la Dirección.	Dirección de Tecnología y Seguridad de la Información

			Asegurar la implementación bloqueo automático de pantalla por inactividad y de la política de contraseña segura. Hacer una revisión periódica del estado de los usuarios, sus roles y privilegios en el sistema de control de acceso a oficinas, bases de datos, aplicaciones y sistemas operativos. Ejecutar con frecuencia campañas de seguridad, capacitación y concientización	✓ A.7.2.2 Capacitación, educación y concientización sobre la seguridad de la información. ✓ A.7. 2.3 Proceso disciplinario. ✓ A.9.2.1 Registro y anulación de usuarios. ✓ A.9.2.2 Provisiones de acceso de usuarios. ✓ A.9.2.3 Gestión de privilegios de derecho de acceso. ✓ A.9.2.4 Gestión de la información de autenticación secreta de los usuarios. ✓ A.9.2.5 Revisión de los derechos de acceso. ✓ A.9.2.6. Remover o ajustar los derechos de acceso. ✓ A.10.1.1 Política sobre el uso de controles criptográficos.	

Fuente: *(Silva, 2015) (Aguila Portillo, Cruz Reyes, & Hernández Villacorta, 2009) (Franco, 2015) (Figueroa, Flores, & Samayoa, 2013)*

3.4.3. Declaración de aplicabilidad.

La declaración de aplicabilidad es un documento que enlista los controles contenidos en el Anexo A de la NTS ISO/IEC 27001:2013; dicho anexo se utiliza como referencia para la implementación de medidas de seguridad necesarias para resguardar la confidencialidad, integridad y disponibilidad de la información. Dicho documento es firmado por la máxima autoridad encargada de la responsabilidad del sistema de gestión de seguridad de la información; que para el puesto de bolsa de productos y servicios es el Gerente General de la entidad.

La finalidad de este documento es mantener un registro y control de todas aquellas medidas que son aplicadas por la entidad para palear las amenazas y riesgos que pueden perjudicar su información.

A continuación, se simula la aprobación de la delación de aplicabilidad para IBES, S.A. de C.V.

Declaración de Aplicabilidad de Intermediarios Bursátiles Salvadoreños, S.A. de C.V.

Se emite la presente declaración de aplicabilidad de controles para el Sistema de Gestión de Seguridad de la Información en función de Intermediarios Bursátiles de El Salvador, S.A. de C.V., como responsable de implementar, operar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información, para determinar los resultados de la identificación y valoración de Riesgos de Seguridad de la Información, y la formulación de actividades de tratamiento de riesgos que cada líder operativo de proceso estimó conveniente para mitigarlos y operar de forma segura y conforme los requisitos de los servicios ofrecidos por la entidad.

Los controles aplicables para la operación del Sistema de Gestión de Seguridad de la Información son los numerales que se relacionan a continuación en el "Detalle de la Declaración de Aplicabilidad" tomando como referencia el Anexo "A" de la NTS ISO/IEC 27001:2013.

Controles Anexo A de NTS ISO/IEC 27001:2013	Objetivo de control	Descripción	Son aplicados	Justificación
A.5 Política de seguridad de la información				
A.5.1 Gestión de la dirección para la seguridad de la información Objetivo: Proporcionar directrices y apoyo para la seguridad de la información en concordancia con los requerimientos del negocio, leyes y regulaciones pertinentes.				
A.5.1.1	Políticas para la seguridad de la información	Control Un conjunto de políticas de seguridad de la información debe ser definido y aprobado por la Dirección, publicarlo y comunicarlo a todos los empleados y entidades externas pertinentes.	Sí	La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes
A.5.1.2	Revisión de las políticas para la seguridad de la información	Control Las políticas para la seguridad de la información debe revisarse a períodos planificados o siempre que se produzcan cambios significativos, para asegurar que se mantenga su continuidad, idoneidad, adecuación y efectividad.	Sí	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
A.6 Organización de la seguridad de la información				
A.6.1 Organización interna Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización				
A.6.1.1	Roles y responsabilidades de la seguridad de la información	Control Todas las responsabilidades de la seguridad de la información deben estar definidas y asignadas.	Sí	La entidad ha definido roles y responsabilidades.
A.6.1.2	Segregación de funciones	Control Las funciones conflictivas y las áreas de responsabilidad deben ser segregadas para reducir las oportunidades de modificaciones o uso no autorizado o mal intencionado de los activos de la organización.	Sí	Si, la entidad segrega las funciones entre rangos jerárquicos tal como lo establece el diagrama organizacional.
A.6.1.3	Contacto con autoridades	Control Deben mantenerse los contactos	Sí	Se cuenta con mecanismos de comunicación con las autoridades de la SSF y BOLPROS.

		adecuados con las autoridades pertinentes.		
A.6.1.4	Contacto con grupos de especial interés	Control Se deben mantener contactos apropiados con los grupos de especial interés u otros foros y asociaciones profesionales especializadas en seguridad.	Sí	Si, se tiene una cartera de asesores profesionales con los cuales existe comunicación constante ante eventualidades de los clientes.
A.6.1.5	Seguridad de la información en la gestión de proyectos.	Control La seguridad de la información debe ser tratada en la gestión de proyectos, independientemente del tipo de proyecto.	Sí	La Gestión de proyectos incluye dentro de sus actividades los controles asociados a los procesos afectados.
A.6.2 Dispositivos móviles y trabajo remoto				
Objetivo: Asegurar la seguridad del trabajo remoto y el uso de dispositivos móviles.				
A.6.2.1	Política de dispositivos móviles	Control Una política y medidas de soporte de seguridad deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Sí	Dentro de la organización se cuenta con políticas para el manejo de la información de manera remota, lo cual incluye a los dispositivos móviles y a quienes los utilizan para modificarla.
A.6.2.2	Trabajo remoto	Control Una política y medidas de soporte de seguridad deben ser implementadas para proteger la información accedida, procesada o almacenada en sitios de trabajo remoto.	Sí	En la organización existen roles definidos para modificar la información.
A.7 Seguridad de los recursos humanos				
A.7.1 Antes del empleo Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y sean idóneos para los roles para los cuales se les considera.				
A.7.1.1	Selección de personal	Control Los controles de verificación de los antecedentes de todos los candidatos para el empleo deben llevarse a cabo en concordancia con las leyes, regulaciones y normas de ética pertinentes y, deben ser proporcionales al requerimiento del negocio, la	Sí	EL área de RRHH cuenta con políticas para la selección de personal calificado para el manejo de la información.

		clasificación de la información a ser accedida y los riesgos percibidos.		
A.7.1.2	Términos y condiciones de empleo	Control Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las responsabilidades de la organización para la seguridad de la información.	Sí	Los contratos cuentan con una cláusula de confidencialidad.
A.7.2 Durante el empleo Objetivo: Asegurar que todos los empleados y contratistas estén conscientes de cumplir con sus responsabilidades de la seguridad de la información.				
A.7.2.1	Responsabilidades de la Dirección	Control La Dirección debe requerir que los empleados y contratistas apliquen la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	Sí	EL cumplimiento de los controles establecidos está dentro de las actividades obligatorias para los empleados y los contratistas que deseen trabajar con la organización.
A.7.2.2	Capacitación, educación y concientización sobre la seguridad de la información	Control Todos los empleados de la organización y, cuando sea pertinente, los contratistas, deben recibir una apropiada concientización, capacitación y actualización periódica de las políticas y procedimientos organizacionales, que sean relevantes a su función laboral.	Sí	Se cuenta con un plan de capacitaciones para concientizar a los empleados y terceros que tengan contratos laborales con la organización.
A.7.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal y comunicado de forma que se tomen acciones en contra de empleados que han cometido una violación en la seguridad de la información.	Sí	Todos los empleados que sean reincidentes en el incumplimiento de las normas de seguridad de la información establecidas son amonestados con acciones de personal.

A.7.3 Terminación y cambio del empleo Objetivo: Proteger los intereses de la organización como parte de un proceso de terminación o cambio de empleo.				
A.7.3.1	Responsabilidades de terminación o cambio de empleo	Control Deben ser definidas las responsabilidades y funciones de la seguridad de la información que permanezcan validas después de una terminación o cambio de empleo, comunicadas y remarcadas al empleado o contratista.	Sí	El contrato de los empleados y terceros que tienen relaciones laborales con la organización tiene una clausula en la que su responsabilidad de confidencialidad se extiende fuera del periodo de contratación.
A.8 Gestión de activos				
A.8.1 Responsabilidad sobre los activos Objetivo: Identificar los activos organizacionales y definir las apropiadas responsabilidades de protección.				
A.8.1.1	Inventario de activos	Control Activos asociados con información e instalaciones de procesamiento de la información deben ser identificados y un inventario de estos activos debe ser levantado y mantenido.	Sí	La responsabilidad recae sobre el departamento de contabilidad.
A.8.1.2	Propiedad de los activos	Control Los activos dentro del inventario deben ser asignados.	Sí	Cada activo fijo tiene asignado un responsable dentro de la organización.
A.8.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información, los activos asociados y las instalaciones para procesamiento de la información.	Sí	Cada colaborador de la organización recibe durante el periodo de inducción las instrucciones necesarias para el correcto uso de los activos dentro del área de trabajo.
A.8.1.4	Devolución de los activos	Control Todos los empleados y usuarios externos deben devolver todos los activos de la organización que se encuentran en su posesión una vez dada la terminación de su empleo, contrato o acuerdo.	Sí	El departamento de contabilidad se encarga de llevar el inventario de activos fijos, entradas y salidas de los mismos, así como su gestión.
A.8.2 Clasificación de la información Objetivo: Asegurar que la información reciba un nivel apropiado de protección en concordancia con su importancia para la organización				

A.8.2.1	Clasificación de la información	Control La información debe ser clasificada en términos de su valor, requerimientos legales, sensibilidad y criticidad a modificaciones o divulgación no autorizada.	Sí	La gerencia general de encarga de evaluar el valor de la información y asignar a la misma el nivel de sensibilidad y controles asociados.
A.8.2.2	Etiquetado de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar la información en concordancia con el esquema de clasificación de información adoptado por la organización.	No	A pesar que la información es clasificada esta no recibe una etiqueta o manera de identificarse de forma correcta.
A.8.2.3	Manejo de activos	Control Se debe desarrollar e implementar procedimientos para manejo de activos en concordancia con el esquema de clasificación de información adoptado por la organización.	No	El departamento de contabilidad no cuenta con una manera de identificar de manera simple el nivel de sensibilidad que la gerencia a la información.
A.8.3 Manejo de medios Objetivo: Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de información almacenada en medios.				
A.8.3.1	Gestión de los medios removibles	Control Se deben implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.	No	Al no tener de manera clara los niveles de sensibilidad de la información asignados por la gerencia no puede crearse un procedimiento para gestionar medios removibles.
A.8.3.2	Eliminación de medios	Control Se deben eliminar los medios de manera segura cuando ya no son requeridos utilizando procedimientos formales.	Sí	Cada medio es evaluado constantemente según su naturaleza para considerar su utilidad dentro de la organización
A.8.3.3	Transferencia de medios físicos	Control Medios que contengan información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante su transporte.	Sí	Todos los medios de la organización se encuentran protegidos con claves de acceso.
A.9 Control de acceso				

A.9.1 Requerimiento del negocio para el control de acceso Objetivo: Limitar el acceso a la información y a instalaciones de procesamiento de la información.				
A.9.1.1	Política del control de acceso	Control Se debe establecer, documentar y revisar una política de control de acceso basada en los requerimientos de seguridad de la información y del negocio.	Sí	Utilizan una política de control de acceso basada en los requerimientos del SGSI.
A.9.1.2	Acceso a redes y servicios de red	Control Se debe proveer a los usuarios únicamente con acceso a la red y servicios de red que hayan sido específicamente autorizados.	Sí	Existe accesos limitados a la red y sus servicios.
A.9.2 Gestión del acceso de usuarios Objetivo: Asegurar el acceso autorizado a los usuarios y prevenir el acceso no autorizado a los sistemas y servicios.				
A.9.2.1	Registro y anulación de usuarios	Control Para habilitar la asignación de derechos de acceso se debe implementar un procedimiento formal para la creación y anulación de usuarios.	Sí	Existe un monitoreo constante a la asignación de usuarios al personal de la entidad.
A.9.2.2	Provisión de accesos de usuarios	Control Se debe implementar un proceso formal de provisión de accesos de usuario para asignar o revocar derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.	Sí	
A.9.2.3	Gestión de privilegios de derechos de acceso	Control Se debe restringir y controlar la asignación y uso de los privilegios de derechos de acceso.	Sí	El departamento de RRHH junto a la Gerencia General, son quienes gestionan los derechos y privilegios de accesos del personal de la entidad.
A.9.2.4	Gestión de la información de autenticación secreta de los usuarios	Control Se debe controlar a través de un proceso formal de gestión la asignación de información de autenticación secreta.	Sí	El departamento de RRHH realiza una gestión periódica de los derechos de acceso de los empleados.
A.9.2.5	Revisión de los derechos de acceso	Control Los dueños de los activos deben	Sí	El departamento de contabilidad realiza una gestión y levantamiento de inventarios periódico de los propietarios y responsables de los activos.

		revisar periódicamente los derechos de acceso de los usuarios.		
A.9.2.6	Remover o ajustar los derechos de acceso	Control Se deben remover los derechos de acceso de todos los empleados y usuarios externos a la información e instalaciones de procesamiento de la información una vez dada la terminación de su empleo, contrato o acuerdo, o ser ajustados cuando se dé un cambio.	Sí	El departamento de RRHH se encarga de remover o ajustar los derechos de acceso de los empleados en la entidad.
A.9.3 Responsabilidades del usuario Objetivo: Hacer responsables a los usuarios por salvaguardar su información de autenticación.				
A.9.3.1	Uso de información de autenticación secreta	Control Se debe requerir a los usuarios seguir las prácticas de la organización en el uso de la información de autenticación secreta.	No	No se identificaron controles implementados relacionados al uso de información de autenticación secreta.
A.9.4 Control de acceso a sistemas y aplicaciones Objetivo: Prevenir el acceso no autorizado a sistemas y aplicaciones.				
A.9.4.1	Restricción del acceso a la información	Control Se debe restringir el acceso a la información y a funcionalidades de los sistemas de aplicación en concordancia con la política de control de acceso.	Sí	Existen controles físicos y lógicos implementados para la restricción del acceso a la información.
A.9.4.2	Procedimientos seguros de inicio de sesión	Control Cuando sea requerido por la política de control de acceso, se deben controlar por un procedimiento seguro de inicio de sesión el acceso a los sistemas y aplicaciones.	Sí	Durante el proceso de inducción cada jefe inmediato se encarga de adiestrar a cada uno de los empleados respecto a los procedimientos adecuados para un correcto y seguro inicio de sesión en los sistemas.
A.9.4.3	Sistema de gestión de la contraseña	Control Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	Sí	Cada usuario es responsable de la gestión de sus contraseñas y de asegurar la calidad de las mismas; tal y como se les indica durante el proceso de inducción.
A.9.4.4	Uso de programas utilitarios privilegiados	Control Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en	Sí	Cada empleado cuenta con acceso a programas que resultan necesarios para el desempeño de sus labores.

		capacidad de sobrescribir los controles de aplicaciones y sistema.		
A.9.4.5	Control de acceso al código fuente de los programas	Control Se debe restringir el acceso al código fuente de los programas.	No	No se identificó la aplicación de controles relacionados al acceso del código fuente de los programas.
A.10 Criptografía				
A.10.1 Controles criptográficos Objetivo: Asegurar el apropiado y efectivo uso de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.				
A.10.1.1	Política sobre el uso de controles criptográficos	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No	No implementan controles criptográficos.
A.10.1.2	Gestión de llaves	Control Se debe desarrollar e implementar una política sobre el uso, protección y duración de las llaves criptográficas durante todo el ciclo de vida.	No	
A. 11 Seguridad física y ambiental				
A.11.1 Áreas seguras Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones de procesamiento de la información y a la información de la organización.				
A.11.1.1	Perímetro de seguridad física	Control Se deben definir y utilizar perímetros de seguridad para proteger áreas que contienen información, ya sea sensitiva o crítica, e instalaciones de procesamiento de la información.	Sí	Cuentan con personal de vigilancia y un sistema de video vigilancia.
A.11.1.2	Controles de entrada físicos	Control Las áreas seguras deben estar protegidas por controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.	Sí	
A.11.1.3	Seguridad de oficinas, habitaciones e instalaciones	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones e instalaciones.	Sí	Cuentan con puertas de acceso biométrico para instalaciones que son de uso exclusivo para el personal.

A.11.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Sí	En la entidad se cuenta con planes contingencias ante desastres naturales, ataque maliciosos y accidentes de tipo industrial.
A.11.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar procedimientos para trabajar en áreas seguras.	Sí	Las instalaciones físicas cumplen con medidas de seguridad.
A.11.1.6	Áreas de carga y descarga	Control Se deben controlar los puntos de acceso como las áreas de carga y descarga y otros puntos donde personas no autorizadas puedan ingresar a las instalaciones, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.	Sí	Cuentan con personal de vigilancia y un sistema de video vigilancia.
A.11.2 Equipo Objetivo: Prevenir la pérdida, daño, robo o exposición de los activos y la interrupción de las operaciones de la organización.				
A.11.2.1	Ubicación y protección del equipo	Control El equipo debe estar ubicado y protegido para reducir los riesgos de amenazas y peligros ambientales, y de las oportunidades de accesos no autorizados.	Sí	Los departamentos de Contabilidad y RRHH, se encargan de controlar a la adecuada ubicación y protección de los equipos.
A.11.2.2	Herramientas de soporte	Control El equipo debe ser protegido contra fallas de energía y otras interrupciones causadas por fallas en las herramientas de soporte.	Sí	La entidad contrata a un tercero que se encarga de verificar la protección y soporte contra fallas de energía eléctrico y otras interrupciones causadas por errores cometidos en las herramientas de soporte.
A.11.2.3	Seguridad en el cableado	Control El cableado de la energía y las telecomunicaciones que transportan datos o soportan servicios de información, deben ser protegidos de intercepción, interferencia o daño.	Sí	El cableado de las instalaciones es constantemente monitoreado para ser protegidos contra intercepción, interferencia o daños.
A.11.2.4	Mantenimiento de equipo	Control El equipo debe recibir un correcto mantenimiento para asegurar su	Sí	Los equipos que posee la entidad reciben un constante mantenimiento de acuerdo a la naturaleza de cada uno de ellos.

		continuidad, disponibilidad e integridad.		
A.11.2.5	Retiro de activos	Control El equipo, información o software no debe ser extraído de las instalaciones sin previa autorización.	Sí	La entidad implementa controles para evitar la extracción de estos sin autorización previa.
A.11.2.6	Seguridad del equipo y activos fuera de las instalaciones	Control Al trabajar con equipos y activos fuera de las instalaciones de la organización, se deben aplicar medidas de seguridad considerando los riesgos que esto implica.	No	En la entidad no se identificaron medidas para procurar la seguridad de los activos que son utilizados fuera de las instalaciones.
A.11.2.7	Seguridad en la reutilización o eliminación de equipos	Control Todos los elementos del equipo que contengan medios de almacenamiento deberán ser verificados para asegurar que los datos sensibles y el software con licencia hayan sido eliminados o sobrescrito con seguridad antes de su reutilización o eliminación.	Sí	El departamento de contabilidad se encarga de controlar mediante políticas la reutilización o eliminación de los equipos.
A.11.2.8	Equipo desatendido de usuario	Control Los usuarios deben asegurarse que el equipo desatendido tiene protección apropiada.	No	No se detectaron controles que aseguraran los equipos desatendidos por los usuarios.
A.11.2.9	Política de escritorio y pantalla limpia	Control Se debe adoptar una política de escritorio limpio para documentos y medios de almacenamiento removibles y una política de pantalla limpia en las instalaciones de procesamiento de la información.	No	No se encontraron controles aplicados en la entidad que procuraran un escritorio o pantalla limpia.
A.12 Seguridad de las operaciones				
A.12.1 Procedimientos y responsabilidades operacionales Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de la información.				
A.12.1.1	Procedimientos de operación documentados	Control Los procedimientos de operación deben documentarse y estar disponibles a todos los usuarios que lo necesiten.	No	La entidad no posee procedimientos de operación documentados.

A.12.1.2	Gestión de cambios	Control Cambios en la organización, procesos de negocios, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.	Sí	El Gerente General es el encargado del control de los cambios de procesos del negocio respecto al procesamiento de la información.
A.12.1.3	Gestión de la capacidad	Control El uso de los recursos debe ser monitoreado, optimizado y se deben realizar proyecciones de la capacidad futura necesaria para asegurar el desempeño requerido por el sistema.	Sí	El uso de los recursos es constantemente monitoreado por los gerentes dentro de cada uno de sus departamentos.
A.12.1.4	Separación de los ambientes de desarrollo y prueba	Control Los ambientes de desarrollo, prueba y producción, deben estar separados para reducir los riesgos de acceso no autorizado o cambios en el ambiente en producción.	No	En la entidad no se identificaron controles de separación de ambientes de desarrollo y prueba.
A.12.2 Protección contra software malicioso Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra software malicioso.				
A.12.2.1	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse contra software malicioso, combinándolos con una apropiada concientización del usuario.	Sí	La entidad cuenta con antivirus en sus ordenadores y controles para los usuarios de los equipos informáticos para evitar la difusión de software malicioso.
A.12.3 Copias de seguridad Objetivo: Protección contra pérdida de datos.				
A.12.3.1	Copia de seguridad de la información	Control Se debe hacer copias de seguridad de la información, software e imágenes del sistema y probarlas periódicamente de acuerdo a la política de respaldo.	Sí	La entidad realiza respaldos manuales cada semana.
A.12.4 Registro y monitoreo Objetivo: Registrar eventos y generar evidencia.				
A.12.4.1	Registro de eventos	Control Se deben producir, mantener y revisar periódicamente registros de los eventos de las actividades del usuario,	No	La entidad no posee bitácoras de registros de eventos.

		excepciones, fallas y eventos de seguridad de la información.		
A.12.4.2	Protección de la bitácora de información	Control Las instalaciones de registro y la bitácora de la información deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	No	
A.12.4.3	Bitácoras del administrador y operador	Control Se deben llevar bitácoras de las actividades del administrador y operador del sistema y éstas deben ser protegidas y revisadas regularmente.	No	
A.12.4.4	Sincronización de reloj	Control Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una única fuente de tiempo de referencia.	Sí	Los relojes de la entidad se encuentran sincronizados.
A.12.5 Control de software operacional Objetivo: Asegurar la integridad de los sistemas operacionales				
A.12.5.1	Instalación de software en sistemas operacionales	Control Se deben implementar procedimientos para controlar la instalación de software en sistemas operacionales.	Sí	Solo el personal autorizado realiza las instalaciones de software en la entidad.
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: Prevenir la explotación de las vulnerabilidades técnicas.				
A.12.6.1	Gestión de vulnerabilidades técnicas	Control Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información usados, evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para abordar el riesgo asociado.	Sí	La entidad realiza una gestión de las vulnerabilidades técnicas de los sistemas de información mediante la toma de medidas apropiadas para abordar el riesgo asociado a cada activo enlistado por la entidad.
A.12.6.2	Restricción en la instalación de software	Control Se deben establecer e implementar	Sí	Solo el personal autorizado realiza las instalaciones de software en la entidad.

		reglas que rijan la instalación de software por parte de los usuarios.		
A.12.7 Consideraciones en la auditoria de sistemas de información Objetivo: Minimizar el impacto de las actividades de auditoria en los sistemas en producción				
A 12.7.1	Controles de auditoria de los sistemas de información	Control Los requerimientos y actividades de auditoria que involucran los sistemas en producción deben ser cuidadosamente planificados y acordados para minimizar las interrupciones a los procesos de negocio.	No	La entidad no realiza auditorías al sistema de gestión de seguridad de la información.
A.13 Seguridad de las comunicaciones				
A.13.1 Gestión de seguridad de red Objetivo: Asegurar la protección de la información en redes y su soporte a las instalaciones de procesamiento de la información.				
A.13.1.1	Controles de red	Control Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.	Sí	Se ha instalado el cableado adecuadamente y se contrata servicio externo para solventar problemas y dar mantenimiento
A.13.1.2	Seguridad de los servicios de red	Control Mecanismos de seguridad, niveles de servicio y requisitos de la gestión de todos los servicios de red, deben ser identificados e incluidos en cualquier acuerdo de servicios de red, ya sea si estos servicios son provistos por la misma organización o se subcontratan.	No	No se prevén mecanismos de seguridad para los servicios de red, propios ni con los proveedores.
A.13.1.3	Segmentación de redes	Control Se deben segmentar en redes los grupos de servicios de información, usuarios y sistemas de información.	No	Todos trabajan en la misma red corporativa
A.13.2 Transferencia de información Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A.13.2.1	Procedimientos y políticas de transferencia de información	Control Se deben establecer políticas, procedimientos y controles formales para proteger la transferencia de	No	No se han definido políticas ni controles sobre esta situación

		información a través de todos los tipos de recursos de comunicación.		
A.13.2.2	Acuerdos de transferencia de información	Control Los acuerdos deben abordar la seguridad de la transferencia de información del negocio entre la organización y entidades externas.	No	No se ha acordado la seguridad de la información transferida con las partes interesadas
A.13.2.3	Mensajes electrónicos	Control Se debe proteger adecuadamente la información contenida en los mensajes electrónicos.	No	No existen controles para la protección de los correos
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Control Se deben identificar, revisar periódicamente y documentar los requerimientos para acuerdos de confidencialidad o no divulgación, reflejando las necesidades de la organización para la protección de la información.	No	No se han establecido acuerdos de confidencialidad con sus partes interesadas
A.14 Adquisición, desarrollo y mantenimiento de sistemas				
A.14.1 Requisitos de seguridad de los sistemas de información. Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información a través de todo su ciclo de vida. Esto también incluye los requerimientos para sistemas de información que proveen servicios sobre redes públicas.				
A.14.1.1	Análisis y especificación de requerimientos de seguridad de la información	Control Los requerimientos relacionados a seguridad de la información deben ser incluidos en los requerimientos para nuevos sistemas de información, o mejoras a sistemas de información existentes.	Sí	Administración y finanzas es el responsable de verificar los requerimientos de seguridad en la compra, modificación y mantenimiento de los sistemas, se realiza mediante check list de verificación
A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	Control La información involucrada en servicios de aplicación sobre redes públicas debe ser protegida de actividades fraudulentas, disputas de contrato y divulgación no autorizada y modificación.	No	No existen redes públicas en la organización

A.14.1.3	Protección de transacciones de servicios de aplicación	Control La información involucrada en transacciones en servicios de aplicación debe ser protegida para prevenir transacciones incompletas, mal enrutamiento, alteración, divulgación, duplicación o replicación no autorizada de mensajes.	No	No se considera la protección de las transacciones ya que cualquier puede modificar la información de los sistemas
A.14.2 Seguridad en los procesos de desarrollo y soporte Objetivo: Asegurar que la seguridad de la información sea diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
A.14.2.1	Política de desarrollo seguro	Control Se debe establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.	No	No ha definido política relacionado con este control
A.14.2.2	Procedimientos de control de cambios en sistemas	Control Los cambios a los sistemas dentro del ciclo de vida de desarrollo, deben ser controlados a través del uso de procedimientos formales de control de cambios.	No	No existen procedimientos de control en los cambios a los sistemas
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma operativa	Control Cuando se cambien las plataformas operativas, se debe revisar y probar las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.	No	No se realiza revisiones técnicas
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control Se debe desalentar las modificaciones a los paquetes de software, limitándolas a cambios necesarios y todos los cambios deben ser estrictamente controlados.	Sí	Se han definido roles y privilegios, para evitar modificación en el software.
A.14.2.5	Principios de ingeniería de sistemas seguros	Control Se deben establecer, documentar, mantener y aplicar principios para ingeniería de sistemas seguros en cualquier iniciativa de implementación de sistemas de información.	No	No se aplican principios de ingeniería

A.14.2.6	Ambiente de desarrollo seguro	Control Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguro, para iniciativas de desarrollo e integración de sistemas que cubran todo el ciclo de vida de desarrollo.	No	La entidad no tiene especialistas en desarrollo de software. Además, no es de su interés desarrollar software interno.
A.14.2.7	Desarrollo subcontratado	Control La organización debe supervisar y monitorear las actividades del desarrollo subcontratado de sistemas.	No	No se realizan supervisiones ni monitoreos
A.14.2.8	Pruebas de seguridad del sistema.	Control Las pruebas de la funcionalidad de seguridad del sistema, deben llevarse a cabo durante su desarrollo.	Sí	Se realizan pruebas de funcionalidad, sin embargo, no se documentan ni se lleva un control sobre ellas
A.14.2.9	Pruebas de aceptación del sistema.	Control Se deben establecer programas de pruebas de aceptación y los criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.	No	No se aplican pruebas de aceptación ni criterios para los nuevos sistemas
A.14.3 Datos de prueba Objetivo: Asegurar la protección de los datos usados para pruebas.				
A.14.3.1	Protección de los datos de prueba.	Control Datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.	No	No se protege ni controla la información utilizada como prueba
A.15 Relaciones con los proveedores				
A.15.1 Seguridad de la información en las relaciones con los proveedores. Objetivo: Asegurar la protección de los activos de la organización que son accesibles por los proveedores.				
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores.	Control Se debe de acordar con el proveedor y documentar los requerimientos de	No	No se ha definido política ni requerimientos de seguridad con los proveedores

		seguridad de la información, para la mitigación de los riesgos asociados con el acceso de los proveedores a los activos de la organización.		
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Control Se deben establecer y acordar todos los requerimientos de seguridad de la información pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer componentes de infraestructura de TI para la información de la organización.	Sí	Son acuerdos únicamente verbales con los proveedores, nunca se documenta esta situación
A.15.1.3	Tecnología de información y comunicación en la cadena de suministro.	Control Los acuerdos con proveedores deben incluir los requerimientos para abordar los riesgos de seguridad de información asociados con los servicios de tecnología de comunicaciones e información y la cadena de suministro de productos.	No	No se definen acuerdos ni verbales ni escritos
A.15.2 Gestión del servicio de entrega del proveedor. Objetivo: Mantener un nivel acordado de seguridad de la información y el servicio de entrega alineados con los acuerdos del proveedor.				
A.15.2.1	Monitoreo y revisión de los servicios del proveedor.	Control La organización debe monitorear, revisar y auditar periódicamente el servicio de entrega del proveedor.	Sí	Se realiza el monitoreo, pero no se audita. Además, no se documentan las revisiones a los sistemas
A.15.2.2	Gestión de cambios en los servicios del proveedor.	Control Se deben gestionar los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, teniendo en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y la re-evaluación de los riesgos.	No	No se gestionan los cambios, debido a que se lleva controles sobre ellos y también porque no existen políticas de seguridad de la información

La presente declaración de aplicabilidad será revisada juntamente con los resultados de cada nuevo proceso de valoración de riesgos y/o ante cambios significativos de los elementos de las tecnologías informáticas y/o de personal. Esta información, será material de comparación en los procesos de revisión por la dirección del sistema de gestión de seguridad de la información, en los periodos convenidos para su actualización.

Se firma la presente Declaración de Aplicabilidad,

Berardi Macchiato
Gerente General
Intermediarios Bursátiles de El Salvador, S.A. de C.V.

CONCLUSIONES

Una organización con una estructura de relación jerárquica o de subordinación, requiere de una metodología que le permita gestionar la seguridad de la información con criterios alineados a su estrategia empresarial, al ser la información el recurso más importante para todo tipo de organizaciones y efecto para los Puestos de Bolsa de Productos y Servicios de El Salvador que en función de sus operaciones manejan ciertos volúmenes de información propia o de terceros, por lo que es necesario garantizar su disponibilidad, confidencialidad e integridad.

El presente trabajo tuvo como objetivo el diseño de un SGSI con la finalidad de garantizar la integridad, confidencialidad y disponibilidad de la información tanto física como digital de las sociedades dedicadas a la intermediación de productos y servicios denominados puestos de bolsas que hayan sido autorizadas por la Bolsa de Producto y Servicios de El Salvador; en vista de que este tipo de sociedades carecen de una gestión adecuada de seguridad de la información y gestión de riesgo se puede concluir lo siguiente:

- Los puestos de bolsa en su mayoría desconocen de la existencia de los sistemas de gestión de seguridad de la información esto permite que, a pesar de la implementación de ciertos tipos de controles, la información no cuente con el nivel de seguridad adecuada y por lo tanto se encuentre expuesta a cierto tipo de amenazas producto de las vulnerabilidades existentes.

- La ausencia de controles enfocados a proteger y resguardar la información que es intercambiada con los usuarios puede tener consecuencias negativas para la entidad en aspectos financieros, legales, contractuales y de imagen frente a las partes interesadas.

- La carencia de una metodología de seguridad para los puestos de bolsas puede ser superada con la implementación del sistema de gestión de seguridad de la información propuesto en el Capítulo IV de este documento tendiendo como base la Norma Técnica Salvadoreña ISO/IEC 27001:2013. Sistema de gestión de seguridad de la información.

- Conscientes del nivel de cumplimiento requerido por la NTS ISO/IEC 27001:2013 la implementación del SGSI implica que los puestos de bolsa deben realizar un considerable esfuerzo ante la falta de ciertos controles de seguridad y de esa forma garantizar el cumplimiento de lo requerido por la norma.

- Es necesaria la participación absoluta de la alta dirección de los puestos de bolsas para garantizar la aprobación, implementación y actualización del SGSI y del cumplimento de los requerimientos establecidos en la NTS ISO/IEC 27001:2013.

- Basados en la experiencia se ha demostrado que la Norma Técnica Salvadoreña NTS ISO/IEC 27001:2013. Sistema de gestión de seguridad de la información es un alusivo adaptable a todo tipo de entidades interesadas en el diseño e implementación de un SGSI, no importando, tamaño, naturaleza o giro del negocio.

- La realización de la investigación y sus resultados representan una valiosa aportación para los puestos de bolsas ya que pretende fortalecer ciertas debilidades relacionadas a la gestión de seguridad de la información y al mismo tiempo es un proceso innovador que impulsa la imagen corporativa de este tipo de entidades ante sus partes interesadas.

RECOMENDACIONES

Según las conclusiones establecidas, se han determinado las siguientes recomendaciones para la profesión de contaduría pública y los puestos de bolsa de productos y servicios:

- Que las universidades salvadoreñas, fortalezcan y desarrollen adecuadamente la preparación académica de sus profesionales que estudian la carrera de Contaduría Pública, respecto al diseño e implementación de los SGSI y la normativa técnica relacionada, mediante modificaciones a sus mallas curriculares o capacitaciones en seminarios especializados, con la finalidad de expandir los campos de acción de los profesionales de la contabilidad y permitan estar a la vanguardia de las necesidades tecnológicas de las empresas salvadoreñas.
- Que la gerencia de cada uno de los puestos de bolsa de productos y servicios puedan gestionar el diseño e implementación un SGSI integral a mediano plazo (de 2 a 4 años), según sus necesidades y homogenizarlas con los requerimientos de seguridad que solicite la Bolsa de Productos y Servicios de El Salvador, con el objetivo de consolidar y promover un mercado bursátil más seguro y dinámico para las operaciones que los usuarios realizan en este mecanismo.
- Que la gerencia de los puestos de bolsa capacite y/o concientice sobre temas de seguridad de la información y normativa aplicables a esta, a sus partes interesadas (las cuales deben definir sus necesidades de seguridad con respecto a los puestos de bolsa), con la finalidad que logren un adecuado diseño e implementación de un SGSI.
- Que los responsables de la gestión de riesgos organizacionales en los puestos de bolsa, prioricen el área de seguridad de la información, con el objetivo que se le brinde la importancia necesaria en el plan de tratamiento de los riesgos corporativos.

BIBLIOGRAFIA

Aguila Portillo, M. J., Cruz Reyes, K. U., & Hernández Villacorta, J. C. (Noviembre de 2009). Propuesta de un Sistema de Gestión del manejo y Seguridad de la Información bajo las normas internacionales ISO 27000 paral a Comisión Ejecutiva Hidroeléctrica del Río Lempa, CEL. *Para optar al título de: Ingeniero Industrial*. San Salvador, El Salvador: Universidad de El Salvador, Facultad de Ingeniería y Arquitectura.

Aguirre Cardona , J. D., & Aristizabal Betancourt, C. (2013). Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial la Ofrenda. *Proyecto de grado*. Colombia: Universidad Tecnológica de Pereira.

Álvaro Rodríguez de Roa, R. R. (06 de 2006). *Asociación Española para la Calidad.* Obtenido de https://www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128

Areitio, J. (2008). Seguridad de la Información-Redes, Informatica y Sistemas de Información. En J. Areitio, *Seguridad de la Información-Redes, Informatica y Sistemas de Información* (pág. 495). Madrid: Paraninfo.

Asamblea Legislativa de El Salvador. (20 de Abril de 2012). Ley de Bolsas de Productos y Servicios. San Salvador, El Salvador.

Barrantes Porras, C. E., & Hugo Herrera, J. R. (2012). Diseño e implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos. *Diseño e implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos*. Lima, Perú: Universidad de San Martín de Porres.

BCR. (30 de 06 de 2015). *BCR*. Obtenido de http://www.bcr.gob.sv/bcrsite/uploaded/content/category/847807313.pdf

Bolsa de Productos de El Salvador. (s.f de s.f de 2015). *Bolpros.com*. Obtenido de Estadísticas Acumuladas: https://bolpros.com/estadisticas-acumuladas/

Centro Europeo de Empresas e Innovación. (2010). *ceeicec.com.* Obtenido de Sistema de Gestión de Seguridad de la Infomración, ISO 27001: http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf

Cepeda, I. L. (2016). Análisis para la implementación de un Sitema de Gestión de la Seguridad de la Información según la norma ISO 27001 en la empresa SERVIDOC,

S.A. *Proyecto de trabajo de grado*. Cali, Colombia: Universidad Nacional Abierta y a Distancia.

Díaz, L. (10 de noviembre de 2014). *BOLPROS, una historia de innovación*. Obtenido de BOLPROS, bolsade productos y servicios de El Salvador: https://bolpros.com/bolpros-una-historia-de-innovacion-2/

Ernst & Young. (2014). *EY Construyendoi un mejor entorno de negocios.* Obtenido de http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf

ESET Latinoamérica. (2016). *We Live Security.* Obtenido de ESET Security Report Latinoamérica 2016: https://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf

Figueroa, A., Flores, K., & Samayoa, S. (03 de 2013). Modelo de gesión de seguridad de la información para la fundación Salvador del mundo de El Salvador, con referencia al estandar iternacional ISO/IEC 27001:2005. San Salvador, El Salvador.

Franco, D. E. (2015). Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001. *Previa a la obtención del Título de: Licenciado en Sistemas de Información*. Guayaquil, Ecuador: Escuela Superior Politécnica del Litoral.

Guillen, Y., Rivas, E., & Pérez, M. (Julio de 2011). Implicaciones tributairas y contables de las transacciones que se realizan a través de la Bolsa de Productos y Servicios en El Salvador. *Trabajo de investigación para optar al grado de Licenciatura en Contaduría Pública*. San Salvador, El Salvador: Universidad de El Salvador, Facultad de Ciencias Económicas, Escuela de Contaduría Pública.

Henríquez de Guzmán, L. d., Herrera Rivera, G. Y., & Lemus Campos, F. d. (Septiembre de 2016). Modelo de Sistema de Gestión de la Seguridad de la Información para profesionales de la Contaduría Pública que ejercen la auditoría externa en El Salvador. *Para optar al grado de: Licenciatura en Contaduría Pública*. San Salvador, El Salvador: Universidad de El Salvador, Facultad de Ciencias Económicas.

Henriquez, L., Herrera, G., & Lemus, F. (Septiembre de 2016). Modelo de Sistema de Gestión de la Seguridad de la Información para profesionales de la contaduría pública que ejercen la auditoría externa en El Salvador. *Trabajo de investigación para optar al grado de Licenciatura en Contaduría Pública*. San Salvador, El Salvador: Universidad de El Salvador, Facultad de Ciencias Económicas, Escuela de Contaduría Pública.

Instituto Nacional de Ciberseguridad. (11 de 03 de 2015). *Incibe*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

Instituto Nacional de Ciberseguridad-España. (s/f). *https://www.incibe.es/*. Obtenido de Imlantación de un SGSI en una empresa: https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISACA. (2012). *Cobit 5 para la Seguridad de la Información.* Illinois: ISACA.

ISACA. (4 de Septiembre de 2014). *isaca.org.* Obtenido de Implementación efectiva de un SGSI ISO 27001: https://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

ISO 27000. ES. (s.f.). *ISO 27000.ES.* Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO Tools Excellence Perú. (Marzo de 2015). *isotools.pe*. Obtenido de ISO 27001: Estructura y pasos fundamentales para la adaptación a la norma: http://www.isotools.pe/iso-27001-estructura-y-pasos-fundamentales-adaptacion-norma/

ISO/IEC. (15 de 10 de 2005). ISO/IEC 27001:2005. *Sistema de Gestión de Seguridad de la Información- Requerimientos*.

ISO/IEC. (1 de Julio de 2007). Norma ISO 27002:2005. *Código para la práctica de la gestión de la seguridad de la información*.

ISO/IEC 27001:2013. (2013). NTS ISO/IEC 27001:2013.

ISO/IEC 27002. (2013). Código para la práctica de la gestión de la seguridad de la Información. *Tecnologías de la Información*.

Linares, V. (15 de 05 de 2017). *El Mundo*. Obtenido de http://elmundo.sv/buscan-normar-la-seguridad-de-la-informacion-en-el-sistema-financiero

Lizarazo M., L. J. (s.f.). *Bolsa de Productos Agropecuarios El Mercado de Físicos.*

Llanos, D. E. (Agosto de 2016). Establecimiento, implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. *Tesis para optar por el Título de Ingeniero Informático.* Lima, Perú: Pontificia Universidad Católica de Perú.

Mega, I. G. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. *Tesis de Maestría en Ingeniería en Computación*. Montevideo, Uruguay: Universidad de la República.

Mejía, C. (2017). *Bolpros.com*. Obtenido de ¿Quiénes somos | Bolpros: https://bolpros.com/la-bolsa/

Organización Internacional de Estandarizacion y Comisión Electrotécnica Internacional. (1 de Julio de 2007). Norma ISO 27002:2005. *Código para la práctica de la gestión de la seguridad de la información*.

Organización Salvadoreña de Normalización. (s/f). *osn.gob.sv*. Obtenido de Historia OSN: http://www.osn.gob.sv/index.php?option=com_content&view=article&id=49&Itemid=176

Plaza, X. A. (Marzo de 2015). Análisis y diseño de un Sistema de Gestión de la Seguridad de la Información basado en el criterio de la norma NTE INEN-ISO/IEC 27001:2011, de un modelo de negocio aplicado en la comercialización y distribución de productos químicos. *Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS* . Guayaquil, Ecuador: Universidad Politécnica Salesiana Sede Guayaquil.

Sampieri, R. H. (2014). *Metodología de la Investigación 6° edición.* México DF: McGraw Hill Education.

Seis, J. A. (Abril de 2015). Diseño de un Sistema de Gestión de Seguridad de la Información para instituciones militares. *Tesis previa a la obtención del título de Magister en Gestión de las Comunicaciones y Tecnologías de la Información*. Quito, Ecuador: Escuela Politécnica Nacional.

Silva, C. A. (2015). Diseño de un Sistema de Gestión de Seguridad de la Informació para una entidad financiera de Segundo Piso. *Trabajo de grado*. Colombia: Institución Universitaria Politécnico Grancolombiano.

Suárez, A. E. (2015). Diseño e implementación de un SGSI para el área de informática de la curaduría urbana Segunda Pasto bajo la norma ISO/IEC 27001. *Proyecto de Grado para optar al título de:: Especialista en Seguridad Informática*. San Juan de Pasto, Colombia: Universidad Nacional Abierta y Distancia (UNAD).

ANEXOS

Anexo N°1.

Encuesta realizada a los puestos de bolsa.

Universidad de El Salvador
Facultad de Ciencias Económicas
Escuela de Contaduría Pública
Encuesta

Dirigido a: Gerentes responsables de la administración de los puestos de bolsa de productos y servicios de El Salvador.

Tema de Investigación: "SISTEMA DE GESTIÓN DE SEGURIDAD PARA LOS PUESTOS DE BOLSA DE PRODUCTOS Y SERVICIOS QUE GARANTICE LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN"

Objetivo: Recopilar información necesaria referente a la forma en cómo los puestos de bolsa de productos y servicios de El Salvador gestionan la integridad, confidencialidad y disponibilidad de la información física y digital que procesan.

Indicaciones: Marcar con una "X" la opción que considere conveniente según corresponda a cada pregunta.

1) En la entidad ¿Se tienen accesos limitados a la información de acuerdo a las funciones de cada uno de los empleados?

   SI ☐ NO ☐

Objetivo: conocer la existencia del riesgo de que la información sea modificada por personal no autorizado.

2) ¿Cuál es el medio que más utilizan para solicitar o transferir información perteneciente a los clientes? (Puede señalar más de una opción)

   a) Correo electrónico ☐
   b) Dispositivo extraíble posteriormente enviado por correspondencia ☐
   c) Dispositivo extraíble entregado personalmente ☐
   d) Envío de documentos físicos mediante correspondencia ☐
   e) Entrega personal de documentos físicos ☐

Objetivo: comprender si existen controles adecuados respecto a la distribución de información para que esta no llegue a terceros no autorizados.

3) ¿Qué tipo de actividades son realizadas para concientizar al personal en cuanto a la importancia de la seguridad de la información? (Puede señalar más de una opción)

a) Capacitaciones ☐
b) Especialización en seminarios ☐
c) Entrenamiento o inducción ☐
d) Ninguna de las anteriores ☐

Objetivo: comprender si la gestión de la seguridad de la información resulta relevante para la entidad y el compromiso que es asignado al personal respecto a esta.

4) Sí un tercero o personal no autorizado intenta acceder a la información que se posee de forma física ¿Que métodos emplea para evitarlo?

a) Cuenta con video vigilancia ☐
b) Sistemas de accesos biométrica ☐
c) Sistema de alarmas ☐
d) Personal de vigilancia ☐
e) Controles de acceso a visitantes ☐

Objetivo: verificar la existencia de respuesta al riesgo ante el acceso a la información física por parte de personas no autorizado.

5) ¿Realizan mantenimiento continuo a los sistemas informáticos de la entidad con la finalidad de cuidar la información que en estos se procesa?

SI ☐ NO ☐

Objetivo: Conocer si la entidad garantiza la disponibilidad e integridad de la información procesada en los sistemas mediante un mantenimiento continuo.

6) ¿Realiza respaldos de las bases de datos del sistema de forma manual o automática?

Manual ☐ Automática ☐ No realiza respaldos ☐

Objetivo: conocer la disponibilidad de la información ante el siniestro de la perdida de esta.

7) ¿Cuáles son los medios y/o lugares de almacenamiento para el resguardo de la información digital propia y de terceros? (Puede señalar más de una opción)

a) Disco duro externo ☐
b) Alojamiento Web ☐

c) Servidores en Red ☐

d) Correo electrónico ☐

Objetivo: Conocer los medios de almacenamiento y respaldo que utilizan los puestos de bolsa para garantizar el acceso oportuno y fiable de la información.

8) ¿Qué controles aplican en el puesto de bolsa para mantener la integridad de la información? (Puede señalar más de una opción)

a) Modificación solo mediante personal autorizado ☐

b) Criptografía de datos ☐

c) Registro de actividades y eventos ☐

d) Controlar el acceso físico a los equipos y componentes de la red ☐

e) Firma digital ☐

f) Control para resguardo de los dispositivos de almacenamiento ☐

g) Actualizaciones del sistema operativo ☐

h) Antivirus y Firewall ☐

i) Restricción de accesos a programas y archivos ☐

j) Restricción de ubicación y horario ☐

k) No aplican ☐

Objetivo: Analizar las fortalezas de las medidas de seguridad que implementan la organización para garantizar la integridad de la información frente a los riesgos potenciales.

9) ¿Cuál es la forma en que la organización informa a los usuarios sobre restricciones de uso de información confidencial? (Puede señalar más de una opción)

a) Política de confidencialidad de la información ☐

b) Contratos de confidencialidad ☐

c) Segregación de funciones ☐

d) Disponibilidad de manuales de información relevante ☐

e) No existe un medio de información ☐

Objetivo: Identificar la existencia de un compromiso de la alta dirección en relación a la confidencialidad y protección de la información.

10) ¿Cuáles son los métodos utilizados para la protección de la documentación física? (Puede señalar más de una opción)

a) Almacenamiento con sistemas biométricos. ☐

b) Clasificación de la información en base a la confidencialidad y susceptibilidad de la mismo ☐

c) Autorización de acceso para el personal para el uso y manejo de la información. ☐

d) Verificación de controles para las requisiciones de la información. ☐

e) No utilizan un método ☐

Objetivo: Comprender si las medidas de seguridad que utiliza la organización son adecuadas para garantizar la integridad, disponibilidad y confidencialidad de la información propia y de terceros.

11) ¿Qué tipo de controles son implementados en la entidad para que la información esté disponible en el momento oportuno? (Puede señalar más de una opción)

a) Respaldos de la información de la información digital en un alojamiento web. ☐

b) Autorización de personal clave. ☐

c) Mantenimiento y mejoras de hardware y software que se utiliza ☐

d) Verificación continua de los servidores. ☐

e) Monitoreo constante de bodegas de almacenamiento de información física ☐

f) No implementan controles. ☐

Objetivo: Definir si los controles de seguridad son idóneos frente a las necesidades de resguardo de la información para garantizar su disponibilidad.

12) Cuando ha sucedido la pérdida de información (física o digital) en la organización, ¿Cuáles fueron los factores que la originaron: (Puede señalar más de una opción)

a) Ocasionado por software malicioso ☐

b) Fallas de los equipos informáticos ☐
c) Fallas del software instalado en los equipos informáticos ☐
d) Por robo o hurto ☐
e) Fenómenos de la naturaleza (terremotos, inundaciones, incendios) ☐
f) Por errores humanos ☐

Objetivo: Identificar los factores de riesgo a los que está expuesta la organización en relación a la seguridad de la información.

13) ¿Cuál sería el plan de acción para recuperar la información perdida a causa de un siniestro? (Puede señalar más de una opción):
a) Recuperación mediante correos electrónicos ☐
b) Respaldos de dispositivos otros dispositivos (terminales, discos duros externos) ☐
c) Respaldos en alojamiento web ☐
d) Se le solicita al cliente de nuevo ☐
e) Mediante un servidor externo ☐
f) Se regenera de la documentación física (en caso la pérdida fuera digital) ☐

Objetivo: Conocer si la alta dirección está comprometida en la gestión de mitigación del riesgo de la pérdida de información cuando este se materializa.

14) ¿Conoce acerca de los Sistemas de Gestión de Seguridad de la Información?

SI ☐ NO ☐

Objetivo: Comprender el nivel de madurez de la entidad respecto a los modelos de gestión de la seguridad de la información.

15) ¿Tiene conocimiento sobre la norma ISO/IEC 27001?

SI ☐ NO ☐

Objetivo: Determinar el nivel de competencia de la entidad en relación al conocimiento de estándares internacionales de normalización.

16) Si se diseñara un Sistema de Gestión de Seguridad de la Información personalizado para los puestos de bolsa de productos y servicios ¿le sería atractivo implementarlo para mejorar la integridad, confidencialidad y disponibilidad de la información que se procesa en la organización?

SI ☐ NO ☐

Objetivo: Medir el interés de la alta gerencia respecto al mejoramiento en seguridad de la información de la organización.

Anexo N° 2.

Análisis y procesamiento de los datos.

Pregunta 1

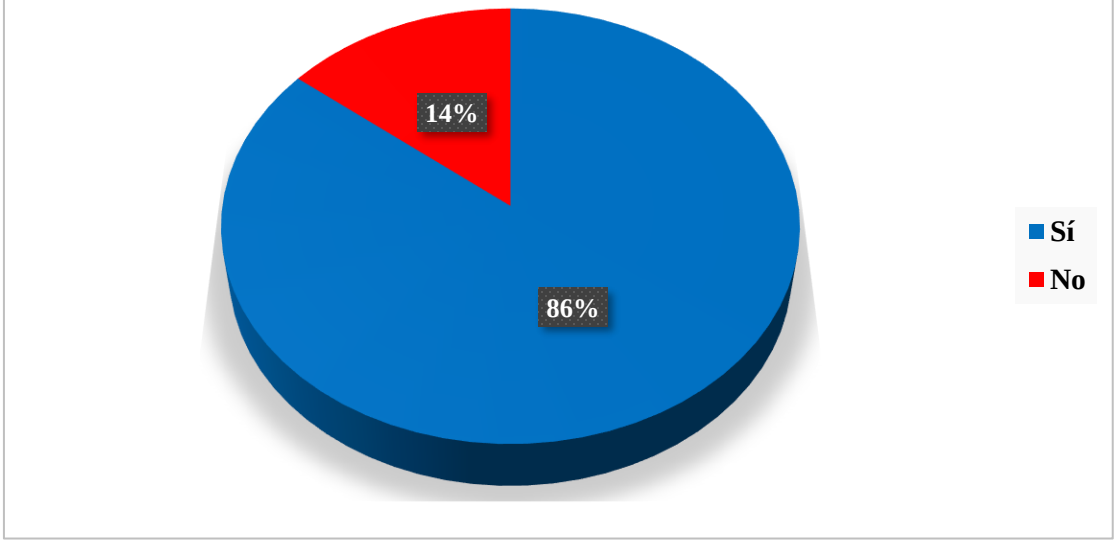
En la entidad ¿Se tienen accesos limitados a la información de acuerdo a las funciones de cada uno de los empleados?

Objetivo: conocer la existencia del riesgo de que la información sea modificada por personal no autorizado.

Tabla de resultados No. 1. Accesos limitados a la información, según la función de cada empleado.

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Sí	6	86%
No	1	14%
TOTAL	7	**100%**

Gráfico N° 1. Accesos limitados a la información segun al función del empleado



Análisis e interpretación de resultados:

En el 86% de los puestos de bolsa de productos y servicios de El Salvador se considera que las funciones que desempeña cada uno de sus empleados cuenta con accesos limitados,

con la finalidad de evitar que información relevante y confidencial no sea accesible a personal no adecuado. Sin embargo, un 14% afirma que la función dentro de sus entidades no se encuentra correctamente limitadas sus funciones con la finalidad de resguardar la confidencialidad de la información.

Pregunta 2

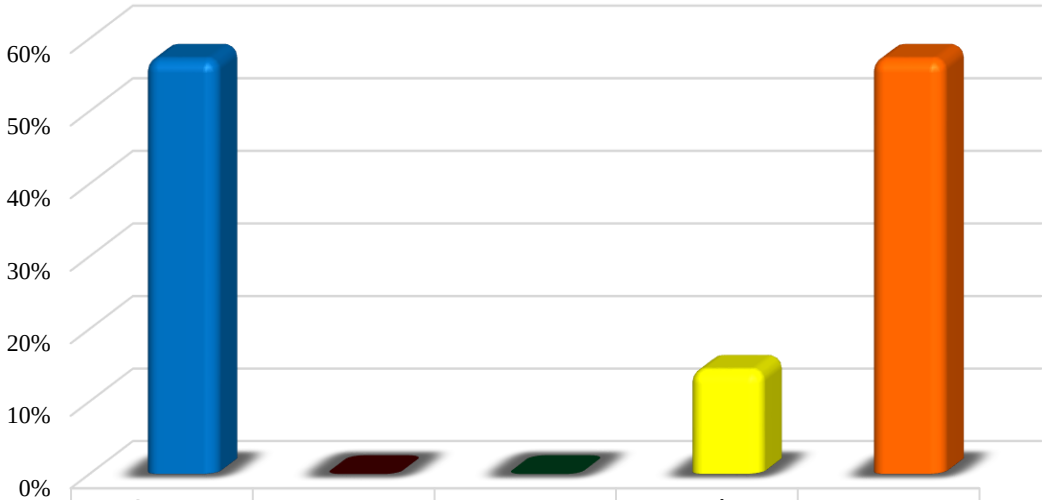
¿Cuál es el medio que más utilizan para solicitar o transferir información perteneciente a los clientes? (Puede señalar más de una opción)

Objetivo: comprender si existen controles adecuados respecto a la distribución de información para que esta no llegue a terceros no autorizados.

Tabla de resultados N°2. Medios para solicitar y transferir información de los clientes.

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Correo electrónico	4	57%
Dispositivo extraíble posteriormente enviado por correspondencia	0	0%
Dispositivo extraíble entregado personalmente	0	0%
Envío documentos físicos mediante correspondencia	1	14%
Entrega personal de documentos físicos	4	57%

Gráfico N° 2. Medios para solicitar y transferir información de los clientes



	Correo electronico	Dispositivo extraible posteriormente enviado por correspondencia	Dispositivo extraible entregado personalmente	Envío documentos fisicos mediante correspondencia	Entrega personal de documentos físicos
FRECUENCIA RELATIVA	57%	0%	0%	14%	57%

Análisis e interpretación de resultados:

Los puestos de bolsa de productos y servicios de El Salvador un 57% se inclina por el uso del correo electrónico para solicitar o transferir información de los clientes, en un porcentaje igual también hacen uso de la entrega personal de documentos físicos, demostrando que por lo menos la mitad de la población encuestada prefiere un trato directo con los clientes, ya sea físico o virtual y dejan el envío y entrega de documentos físicos mediante correspondencia con una utilización del 14%, siendo el trato indirecto con el cliente el menos preferido.

Pregunta 3

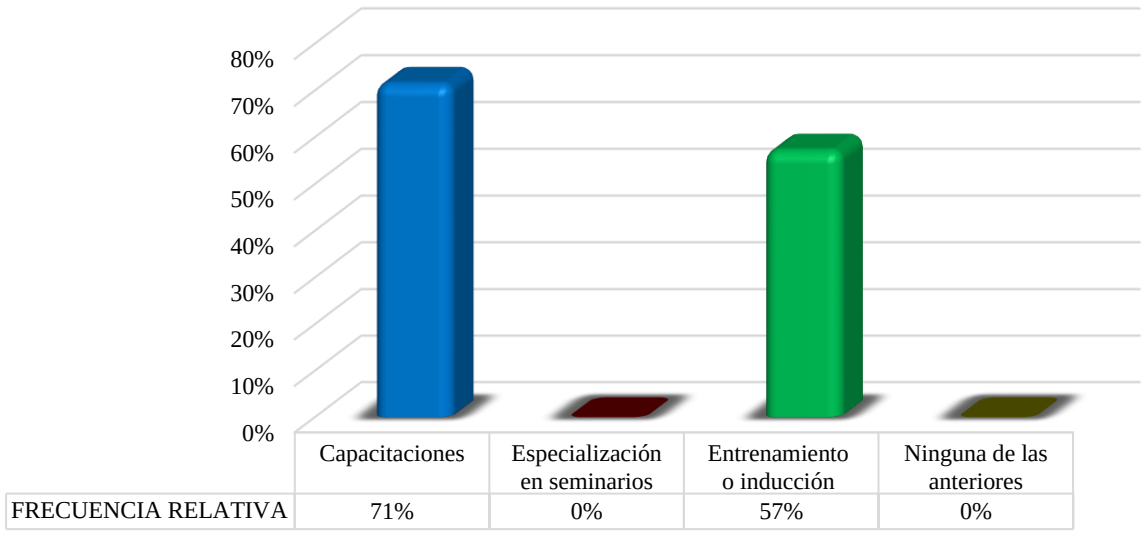
¿Qué tipo de actividades son realizadas para concientizar al personal en cuanto a la importancia de la seguridad de la información? (Puede señalar más de una opción)

Objetivo: comprender si la gestión de la seguridad de la información resulta relevante para la entidad y el compromiso que es asignado al personal respecto a esta.

Tabla de resultados N° 3. Actividades para concientizar al personal sobre la seguridad de la información.

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Capacitaciones	5	71%
Especialización en seminarios	0	0%
Entrenamiento o inducción	4	57%
Ninguna de las anteriores	0	0%

Gráfico N° 3. Actividades para conscientizar al personal sobre seguridad de la información



Análisis e interpretación de resultados:

Los resultados demuestran que el método preferido por los puestos de bolsa de productos y servicios para concientizar al personal en cuento a la importancia de la seguridad de la información son las capacitaciones, con una participación de 71% y que el siguiente método

utilizado es el entrenamiento o inducción, dejando a las especializaciones o seminarios con un 0%, demostrando que el tema no se pasa por alto en ninguna institución del rubro y que prefieren que su personal tenga un conocimiento por lo menos moderado en este

Pregunta 4

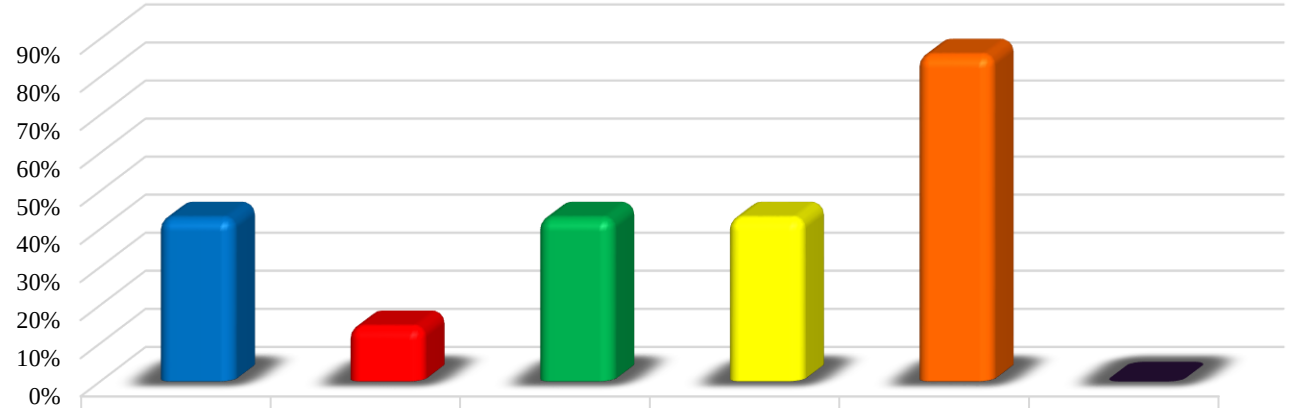
Sí un tercero o personal no autorizado intenta acceder a la información que se posee de forma física ¿Que métodos emplea para evitarlo?

Objetivo: verificar la existencia de respuesta al riesgo ante el acceso a la información física por parte de personas no autorizado.

Tabla de resultados N° 4. Medidas de seguridad contra no autorizados a la información.

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Cuenta con video vigilancia	3	43%
Sistemas de accesos biométrica	1	14%
Sistema de alarmas	3	43%
Personal de vigilancia	3	43%
Controles de acceso a visitantes	6	86%
Ninguna de las anteriores	0	0%

Gráfico N° 4 . Medidas de seguridad contra accesos no autorizados a la información



	Cuenta con video vigilancia	Sistemas de accesos biométrica	Sistema de alarmas	Personal de vigilancia	Controles de acceso a visitantes	Ninguna de las anteriores
FRECUENCIA RELATIVA	43%	14%	43%	43%	86%	0%

Análisis e interpretación de resultados:

Los resultados demuestran que todos los puestos de bolsa de productos y servicios cuentan con medidas de seguridad contra el acceso no autorizado a la información física, siendo el más utilizado el control de acceso a los visitantes con un 86%, optando un 43% de la muestra por el uso la video vigilancia, el sistema de alarmas y el personal de vigilancia, el sistema de acceso biométrico queda relegado con un 14%, esto evidencia que los métodos disuasivos son preferidos a los represivos.

Pregunta 5

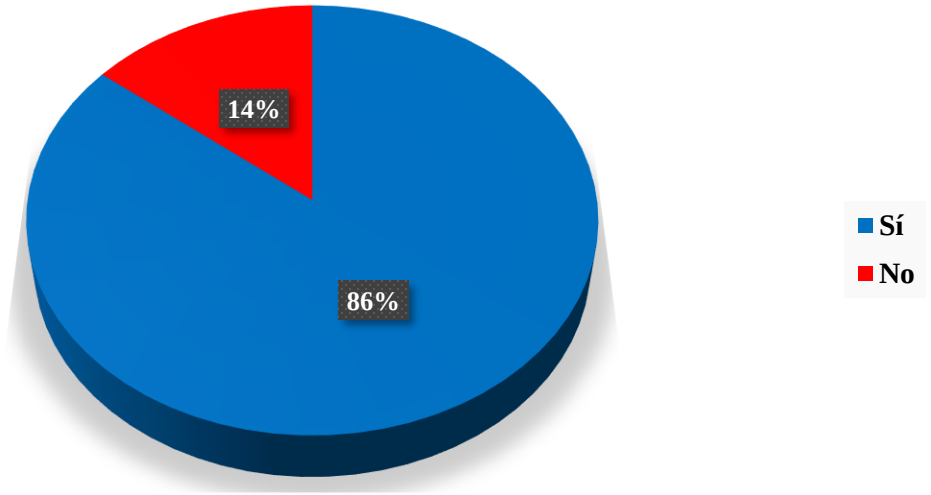
¿Realizan mantenimiento continuo a los sistemas informáticos de la entidad con la finalidad de cuidar la información que en estos se procesa?

Objetivo: Conocer si la entidad garantiza la disponibilidad e integridad de la información procesada en los sistemas mediante un mantenimiento continuo.

Tabla de resultados N° 5. Realización de mantenimiento a sistemas informáticos

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Sí	6	86%
No	1	14%
TOTAL	**7**	**100%**

Gráfico N° 5. Realizacion de mantenimiento a sistemas informáticos



Análisis e interpretación de resultados:

Seis de cada siete puestos de bolsa de productos y servicios brinda mantenimiento a los sistemas informáticos con la finalidad de asegurar la disponibilidad de la información; es decir que el 86% realiza mantenimientos al sistema y una minoría del 14% representado por un solo puesto de bolsa no realiza dicha actividad.

Pregunta 6

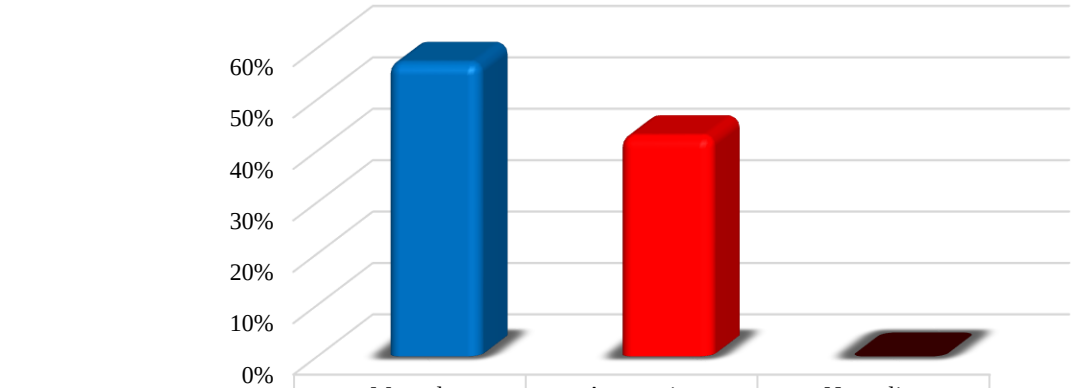
¿Realiza respaldos de las bases de datos del sistema de forma manual o automática?

Objetivo: conocer la disponibilidad de la información ante el siniestro de la perdida de esta.

Tabla N° 6. Realización de respaldos de bases de datos

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Manual	4	57%
Automática	3	43%
No realiza respaldos	0	0%
TOTAL	**7**	**100%**

Gráfico N° 6. Realización de respaldos de bases de datos



	Manual	Automatica	No realiza respaldos
FRECUENCIA RELATIVA	57%	43%	0%

Análisis e interpretación de resultados:

Los puestos de bolsa de productos y servicios realizan respaldos de sus bases de datos con la finalidad de conservar la disponibilidad de su información. Sin embargo, se consultó sí lo realizan de forma manual o automática; resultando que un 57% de los puestos de bolsa de productos y servicios lo realizan de forma manual y un 43% de forma automática.

Pregunta 7

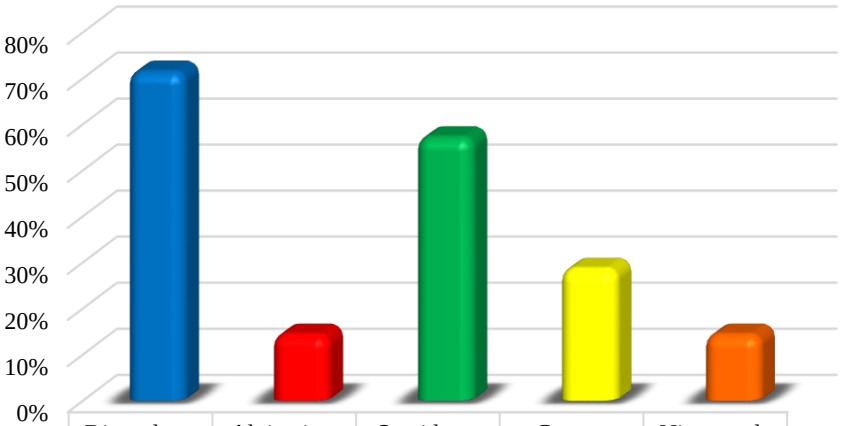
¿Cuáles son los medios y/o lugares de almacenamiento para el resguardo de la información digital propia y de terceros? (Puede señalar más de una opción)

Objetivo: Conocer los medios de almacenamiento y respaldo que utilizan los puestos de bolsa para garantizar el acceso oportuno y fiable de la información.

Tabla de resultados N° 7. Medios de almacenamiento para resguardo de información digital

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Disco duro externo	5	71%
Alojamiento Web	1	14%
Servidores en Red	4	57%
Correo electrónico	2	29%
Ninguna de las anteriores	1	14%

Gráfico N° 7. Medios de almacenamiento para resguardo de información digital



	Disco duro externo	Alojamiento Web	Servidores en Red	Correo electrónico	Ninguna de las anteriores
FRECUENCIA RELATIVA	71%	14%	57%	29%	14%

Análisis e interpretación de resultados:

Los puestos de bolsas de productos y servicios utilizan distintos medios para almacenar su información digital; el más utilizado es el disco duro externo con un 71% de la población encuestada, en un segundo lugar con un 57% se almacena en servidores en red, un 29% utiliza correo electrónico y en porcentajes iguales el alojamiento web y ninguna de las opciones anteriormente citadas con un 14%.

Pregunta 8

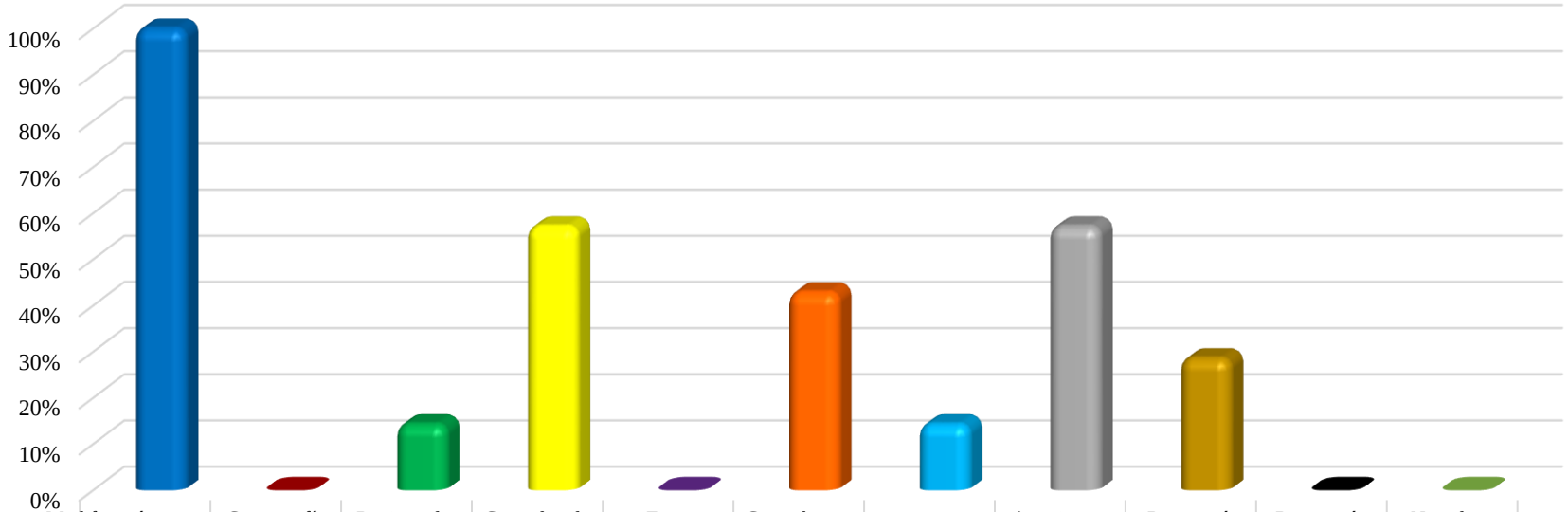
¿Qué controles aplican en el puesto de bolsa para mantener la integridad de la información? (Puede señalar más de una opción)

Objetivo: Analizar las fortalezas de las medidas de seguridad que implementan la organización para garantizar la integridad de la información frente a los riesgos potenciales.

Tabla de resultados N° 8. Controles implementados para mantener la integridad de la información

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Modificación solo mediante personal autorizado	7	100%
Criptografía de datos	0	0%
Registro de actividades y eventos	1	14%
Controlar el acceso físico a los equipos y componentes de la red	4	57%
Firma digital	0	0%
Control para resguardo de los dispositivos de almacenamiento	3	43%
Actualizaciones del sistema operativo	1	14%
Antivirus y Firewall	4	57%
Restricción de accesos a programas y archivos	2	29%
Restricción de ubicación y horario	0	0%
No aplican	0	0%

Gráfico N° 8. Controles aplicados para mantener la integridad de la informacion



	Modificación solo mediante personal autorizado	Criptografía de datos	Registro de actividades y eventos	Controlar el acceso físico a los equipos y componentes de la red	Firma digital	Control para resguardo de los dispositivos de almacenamiento	Actualizaciones del sistema operativo	Antivirus y Firewall	Restricción de accesos a programas y archivos	Restricción de ubicación y horario	No aplican
FRECUENCIA RELATIVA	100%	0%	14%	57%	0%	43%	14%	57%	29%	0%	0%

Análisis e interpretación de resultados:

De acuerdo a la información obtenida por los gerentes del puesto de bolsas de productos y servicios en relación a la implementación de controles para mantener la integridad de la información el 100% manifestó que esta solo puede ser modificada mediante personal autorizado, aunque la criptografía de datos, ni la firma digital sea practicada por los puesto bolsas, un 14% realiza registro de actividades y eventos. Finalmente se concluye que en todos los puestos de bolsa de productos y servicios tiene como medida de seguridad la implementación de algún tipo de control para garantizar la integridad de la información.

Pregunta 9

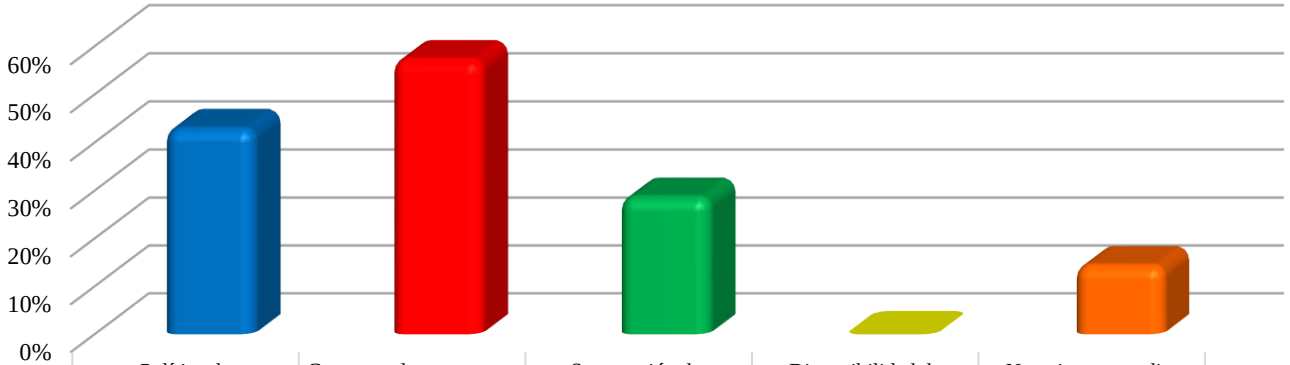
¿Cuál es la forma en que la organización informa a los usuarios sobre restricciones de uso de información confidencial? (Puede señalar más de una opción)

Objetivo: Identificar la existencia de un compromiso de la alta dirección en relación a la confidencialidad y protección de la información.

Tabla de resultados N° 9. Formas de restringir el uso de la información confidencial

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Política de confidencialidad de la información	3	43%
Contratos de confidencialidad	4	57%
Segregación de funciones	2	29%
Disponibilidad de manuales de información relevante	0	0%
No existe un medio de información	1	14%

Gráfico N° 9. Formas de restringir el uso de informacion confidencial



	Política de confidencialidad de la información	Contratos de confidencialidad	Segregación de funciones	Disponibilidad de manuales de información relevante	No existe un medio de información
FRECUENCIA RELATIVA	43%	57%	29%	0%	14%

Análisis e interpretación de resultados:

Conforme a los resultados obtenidos se determinó la manera de informar por parte de los puestos de bolsa de productos y servicios a sus usuarios sobre el uso de información confidencial, el 57% lo hace por medio de contratos de confidencialidad, pero desafortunadamente un 14% no dispone de una estrategia de divulgación. En conclusión, los puestos de bolsa tienen diferentes maneras de informar a sus usuarios sobre la utilización de información confidencial, aunque no dispongan de un manual de información relevante la mayoría de ellos cuenta con una medida de seguridad que garantice la confidencialidad de la información.

Pregunta 10

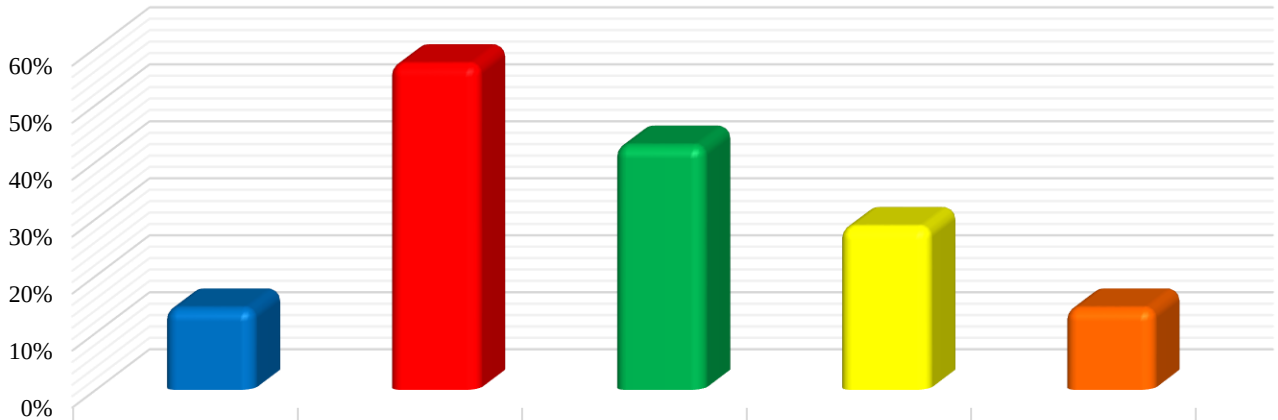
¿Cuáles son los métodos utilizados para la protección de la documentación física? (Puede señalar más de una opción)

Objetivo: Comprender si las medidas de seguridad que utiliza la organización son adecuadas para garantizar la integridad, disponibilidad y confidencialidad de la información propia y de terceros.

Tabla de resultados N° 10. Métodos de protección para la información física.

RESPUESTA	FRECUENCIA OBSOLUTA	FRECUENCIA RELATIVA
Almacenamiento con sistemas biométricos	1	14%
Clasificación de la información en base a la confidencialidad y susceptibilidad de la mismo	4	57%
Autorización de acceso para el personal para el uso y manejo de la información	3	43%
Verificación de controles para las requisiciones de la información	2	29%
No utilizan un método	1	14%

Gráfico N° 10. Metodos de proteccion para la documentacion física



	Almacenamiento con sistemas biométricos	Clasificación de la información en base a la confidencialidad y susceptibilidad de la mismo	Autorización de acceso para el personal para el uso y manejo de la información	Verificación de controles para las requisiciones de la información	No utilizan un método
FRECUENCIA RELATIVA	14%	57%	43%	29%	14%

Análisis e interpretación de resultados:

Con el objetivo de conocer los controles implementados en los puestos de bolsa de productos y servicios para asegurar la protección de la información física, con base a los resultados obtenidos se determinó que el 57% clasifica la información de acuerdo al grado de confidencialidad y susceptibilidad de la misma y un 14% cuenta con almacenamiento con sistemas biométricos. En conclusión, se puede mencionar que a pesar de que algunos puestos de bolsas no dispongan de un mecanismo en específico para asegurar la disponibilidad de la información, la mayoría de puestos cuenta con controles y asignación de responsabilidades para asegurar que la información esté protegida y disponible en el momento oportuno.

Pregunta 11

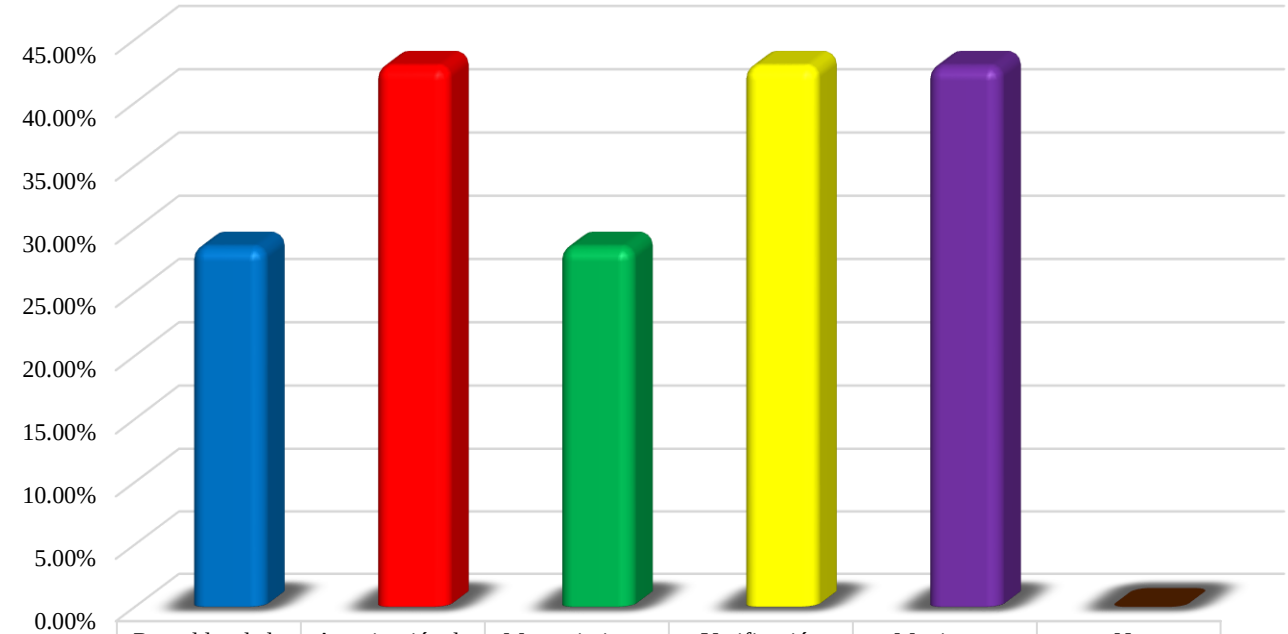
¿Qué tipo de controles son implementados en la entidad para que la información esté disponible en el momento oportuno? (Puede señalar más de una opción)

Objetivo: Definir si los controles de seguridad son idóneos frente a las necesidades de resguardo de la información para garantizar su disponibilidad.

Tabla de resultados N° 11. Controles para garantizar la disponibilidad de la información

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
a) Respaldos de la información digital en un alojamiento web.	2	28.57%
b) Autorización de personal clave.	3	42.86%
c) Mantenimiento y mejoras de hardware y software que se utiliza	2	28.57%
d) Verificación continua de los servidores.	3	42.86%
e) Monitoreo constante de bodegas de almacenamiento de información física	3	42.86%
f) No implementan controles.	0	0.00%

Gráfico N° 11. Tipo de controles implementados



	Respaldos de la información de la información digital en un alojamiento web	Autorización de personal clave	Mantenimiento y mejoras de hardware y software que se utiliza	Verificación continua de los servidores	Monitoreo constante de bodegas de almacenamiento de información física	No implementan controles
Porcentaje	28.57%	42.86%	28.57%	42.86%	42.86%	0%

Análisis e interpretación de resultados:

De acuerdo a los resultados obtenidos y con la finalidad de conocer cuáles son los controles implementados por los puestos de bolsa de productos y servicios para garantizar la disponibilidad de la información se determinó que el 42.86% de los puestos de bolsa de productos y servicios asegura la disponibilidad de la información a través de la Autorización de personal clave, verificación continua de los servidores y monitoreo constante de bodegas de almacenamiento de información física, mientras que un 28.57% lo hace por medio de respaldos de la información digital en un alojamiento web y mantenimiento y mejoras de hardware y software. En conclusión, se puede mencionar que en su mayoría los puestos de bolsa no disponen de una metodología de control general que les garantice de forma absoluta la disponibilidad de la información ya que no todos implementan controles de forma completa esto indica incluso que algunos puestos de bolsa no dispongas de una adecuada

infraestructura de almacenamiento porque carecen de mantenimiento y un constante monitoreo de la información almacenada.

Pregunta 12

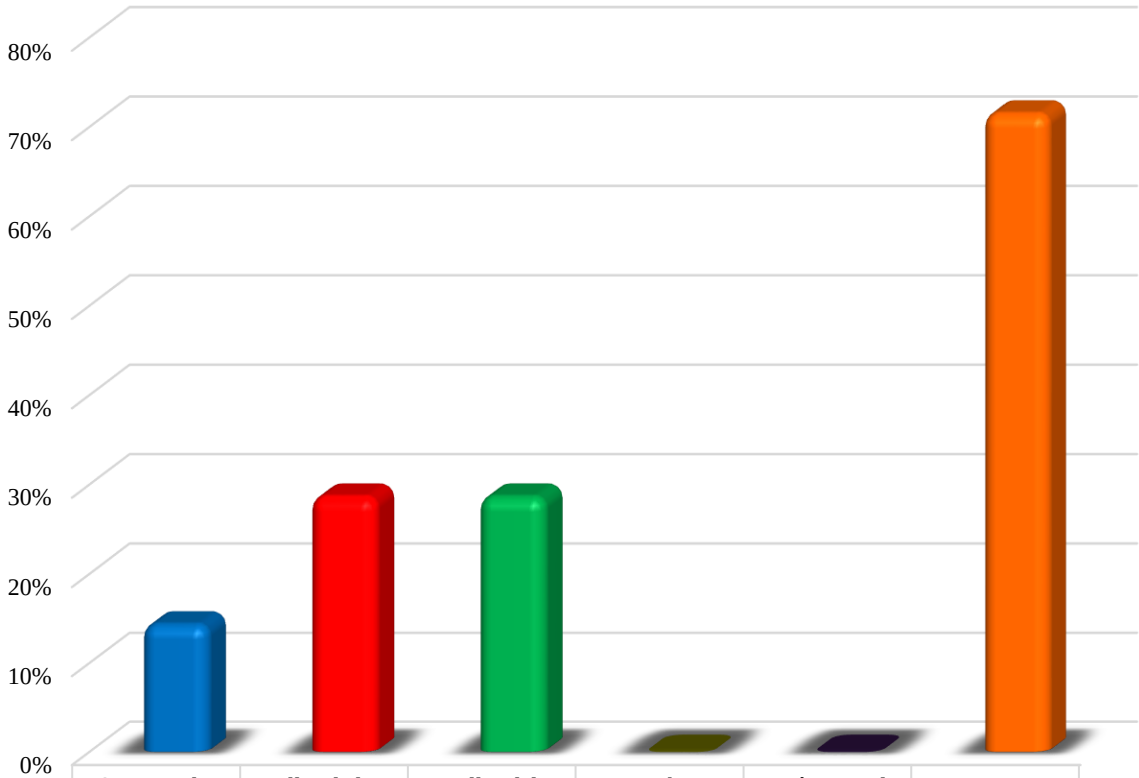
Cuando ha sucedido la pérdida de información (física o digital) en la organización, ¿Cuáles fueron los factores que la originaron: (Puede señalar más de una opción)

Objetivo: Identificar los factores de riesgo a los que está expuesta la organización en relación a la seguridad de la información.

Tabla de resultados N° 12. Eventos de seguridad que generan pérdida de información.

RESPUESTA	FRECUENCIA OBSOLUTA	FRECUENCIA RELATIVA
Ocasionado por software malicioso	1	14%
Fallas de los equipos informáticos	2	29%
Fallas del software instalado en los equipos informáticos	2	29%
Por robo o hurto	0	0%
Fenómenos de la naturaleza (terremotos, inundaciones, incendios)	0	0%
Por errores humanos	5	71%

Gráfico N° 12. Enventos de seguridad que originan pérdida de información



	Ocasionado por software malicioso	Fallas de los equipos informáticos	Fallas del software instalado en los equipos informáticos	Por robo o hurto	Fenómenos de la naturaleza (terremotos, inundaciones, incendios)	Por errores humanos
FRECUENCIA RELATIVA	14%	29%	29%	0%	0%	71%

Análisis e interpretación de resultados:

Al identificar las causas que dan origen a la pérdida de información en los puestos de bolsas de productos y servicios y según los resultados obtenidos, el 71% responde haber sufrido este tipo daños a causa del error humano y el 14% por medio software maliciosos. En conclusión, la vulnerabilidad a la cual se expone la información de ser objeto de pérdida o extravió responde en mayor porcentaje al uso o manejo por partes de los usuarios al no existir medidas de protección por parte del personal e incluso de los responsables de gestionar y suministrar la información.

Pregunta 13

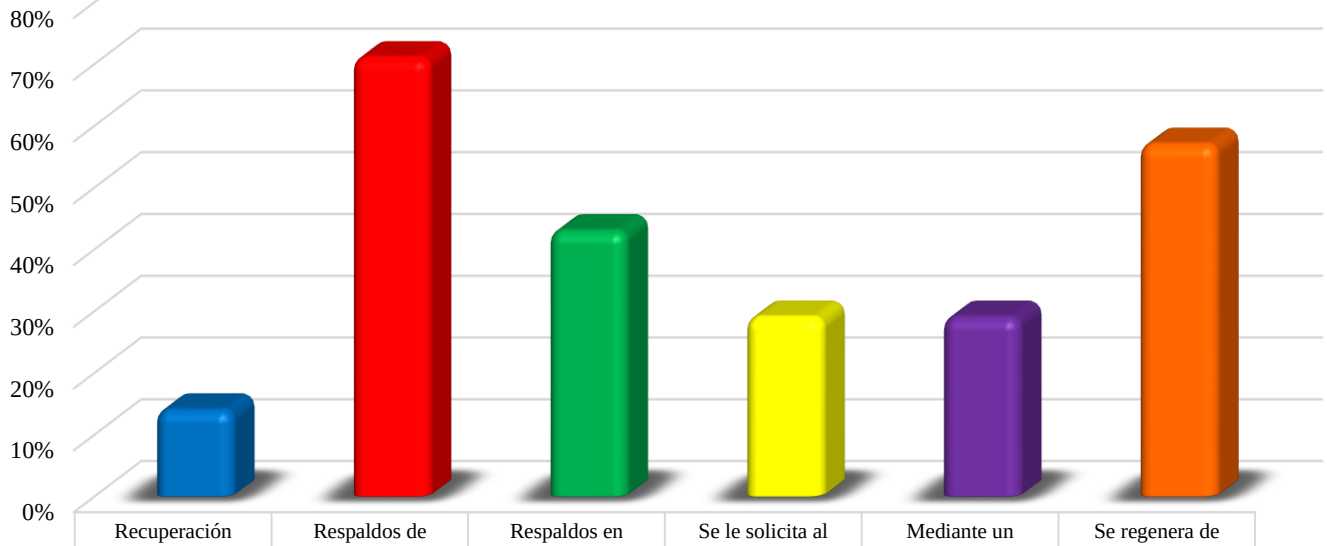
¿Cuál sería el plan de acción para recuperar la información perdida a causa de un siniestro? (Puede señalar más de una opción):

Objetivo: Conocer si la alta dirección está comprometida en la gestión de mitigación del riesgo de la pérdida de información cuando este se materializa.

Tabla de resultados N° 13. Acciones para recuperación de la información.

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Recuperación mediante correos electrónicos	1	14%
Respaldos de dispositivos otros dispositivos (terminales, discos duros externos)	5	71%
Respaldos en alojamiento web	3	43%
Se le solicita al cliente de nuevo	2	29%
Mediante un servidor externo	2	29%
Se regenera de la documentación física (en caso la pérdida fuera digital)	4	57%

Gráfico N° 13. Acciones para recuperación de la información



	Recuperación mediante correos electrónicos	Respaldos de dispositivos otros dispositivos (terminales, discos duros externos)	Respaldos en alojamiento web	Se le solicita al cliente de nuevo	Mediante un servidor externo	Se regenera de la documentación física (en caso la pérdida fuera digital)
FRECUENCIA RELATIVA	14%	71%	43%	29%	29%	57%

Análisis e interpretación de resultados:

Según los datos reflejados en la encuesta, para recuperar la información por un siniestro ocurrido, el 71 % de los puestos de bolsa dispone de respaldos guardados en discos duros externos o algún otro equipo de cómputo, el 43% regenera los datos a partir de los respaldos en los alojamientos web (nube) que posee y el 57% restauran la información a partir de la documentación física archivada. Esto nos lleva concluir que la mayoría de puestos en primera instancia depende de la tecnología para la reconstrucción de la información, puesto que recupera a través de dispositivos de almacenamiento digital y alojamiento web, y su segunda alternativa es restitución mediante archivos físicos, lo cual puede significar un proceso lento de recuperación; además al no disponer de muchas alternativas se vulnera la integridad y disponibilidad de la información.

Pregunta 14

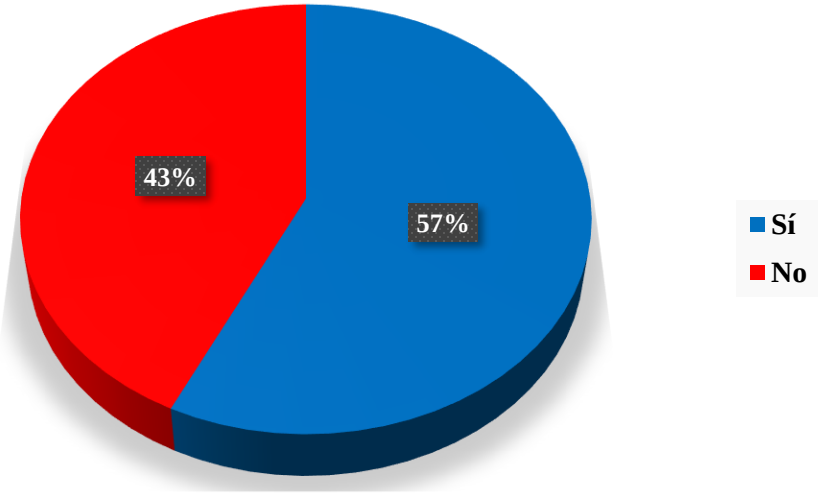
¿Conoce acerca de los Sistemas de Gestión de Seguridad de la Información?

Objetivo: Comprender el nivel de madurez de la entidad respecto a los modelos de gestión de la seguridad de la información.

Tabla de resultados N° 14. Conocimiento sobre el SGSI.

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Sí	4	57%
No	3	43%
TOTAL	**7**	**100%**

Gráfico N° 14. Conocimiento sobre el SGSI.



Análisis e interpretación de resultados:

Los resultados de esta pregunta exponen que el 57% de los puestos de bolsa conoce sobre la existencia de los SGSI y el 43% respondió no conocer sobre la temática. Lo anterior lleva a concluir que la mayoría de los puestos e bolsa son conscientes sobre las necedades de seguridad de la información que tiene una empresa, debido a que tienen una idea sobre los SGSI, pero que no implementan las medidas de seguridad por falta de recursos, desinformación o no es su prioridad proteger sus activos de información.

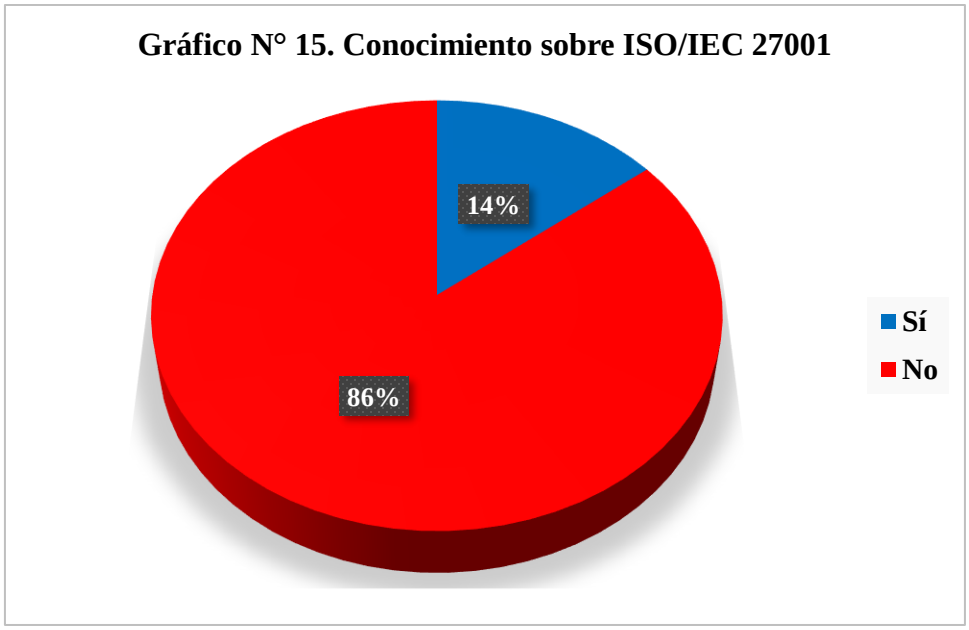
Pregunta 15

¿Tiene conocimiento sobre la norma ISO/IEC 27001?

Objetivo: Determinar el nivel de competencia de la entidad en relación al conocimiento de estándares internacionales de normalización.

Tabla de resultados N° 15. Conocimiento sobre ISO/IEC 27001.

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Sí	1	14%
No	6	86%
TOTAL	**7**	**100%**



Análisis e interpretación de resultados:

Los resultados de la encuesta revelan que la administración del 14% de los puestos de bolsa conoce acerca de la NTS ISO/IEC 27001 y el 86% no sabe sobre su existencia. Esto nos indica que casi la totalidad de estas entidades no implementan una estandarización en sus medidas de seguridad por desconocimiento de normativas que les permitirían mejorar la gestión de la seguridad de la información. Por lo cual, también es necesario capacitar a la entidad.

Pregunta 16

Si se diseñara un Sistema de Gestión de Seguridad de la Información personalizado para los puestos de bolsa de productos y servicios ¿le sería atractivo implementarlo para mejorar

la integridad, confidencialidad y disponibilidad de la información que se procesa en la organización?

Objetivo: Medir el interés de la alta gerencia respecto al mejoramiento en seguridad de la información de la organización.

Tabla de resultados N° 16. Interés de un SGSI personalizado para puestos de bolsa

RESPUESTA	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Sí	6	86%
No	1	14%
TOTAL	**7**	**100%**

Análisis e interpretación de resultados: Finalmente, los resultados de esta pregunta ponen de manifiesto la necesidad de los puestos de bolsa por la implementación de un sistema de gestión de seguridad de la información, ya que el 86% de ellos valida el diseño personalizado a sus operaciones de este modelo de gestión de seguridad, ante un 14% que respondió que no desea este modelo de gestión personalizado.

Gráfico N° 16. Interés de un SGSI personalizado para puestos de bolsa