UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

SISTEMA DE GESTIÓN DE EMPRESAS DEDICADAS A LA INDUSTRIA TEXTIL DEL MUNICIPIO DE SAN SALVADOR QUE GARANTICEN LA SEGURIDAD DE LA INFORMACIÓN BASADOS EN NTS ISO 27001:2013

PRESENTADO POR GRUPO E25

Alvarado Mendoza, Humberto Ernesto

García Montiel, Romeo Alejandro

Molina Platero, Arturo Ernesto

PARA OPTAR AL GRADO DE:

Licenciado en Contaduría Pública

NOVIEMBRE 2019 SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

AUTORIDADES UNIVERSITARIAS

Rector	:	Master Roger Armando Arias Alvarado
Secretario General	:	Ing. Francisco Antonio Alarcón Sandoval
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 Seminario de Graduación	:	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	:	Lic. José Felipe Mejía Hernández
Jurado evaluador	:	Lic. Daniel Nehemías Reyes López Lic. José Gustavo Benítez Estrada Lic. José Felipe Mejía Hernández

Noviembre 2019

San Salvador, El Salvador, Centro América.

AGRADECIMIENTOS

A Dios gracias por la oportunidad de culminar uno de los muchos propósitos en mi vida, a mi madre Marlene Mendoza por enseñarme que todo esfuerzo y perseverancia tiene su recompensa, por su apoyo incondicional, a mis hermanas Mercy y Darlyn por su valioso apoyo en este proceso, a mi compañera de vida Sofía Gonzales por apoyarme en toda decisión y etapa en este proceso, también a mis compañeros con quienes compartí este camino universitario en general a todas las personas por sus muestras de cariño y orgullo al verme triunfar académicamente.

Humberto Ernesto Alvarado Mendoza

A mis amadas abuela y madre, Carmen Mejía y Zulma Platero por todo el apoyo absoluto que me han proporcionado a lo largo de mi vida, a mi Abuelo José Platero, amigos y compañeros con quienes compartí en este arduo y maravilloso camino universitario; agradezco enormemente todo su apoyo y cariño.

Arturo Ernesto Molina Platero

Agradezco en primer lugar a mi madre Consuelo Montiel 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 pendientes de mí en todo mi desarrollo profesional y académico, en especial a Katherine Hernández por todo su apoyo incondicional. En tercero, y no menos importante a mi equipo de trabajo por su esfuerzo en la culminación de esta etapa y demás amigos que han estado siempre acompañándome en este proceso universitario.

Romeo Alejandro García Montiel

ÍNDICE

Índice de Tablas

Índice de Figuras

Índice de Anexos

RESUMEN EJECUTIVO

La integridad, disponibilidad y confidencialidad de la información de La industria textil es de gran importancia, ya que dichas entidades la necesitan para una toma de decisiones oportuna y comunicar lo requerido, 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 entidades dedicadas a la industria textil. 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 descriptivo, 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 las industrias textiles, para ello se emplearon entrevistas con las cuales se recolectará la información que se analizarán para la comprobación de hipótesis. Se obtuvo la participación de tres encargados de diferentes áreas, quienes respondieron a la entrevista, de cuyos resultados los más destacados fueron: la gran mayoría de los entrevistados tiene poco o nada de 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 la industria textil 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, la cual 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 las industrias textiles puedan diseñar e implementar un SGSI integral a corto plazo, según sus necesidades y homogenizarlas con los requerimientos de seguridad que solicite. Es necesaria la capacitación y concientización sobre temas de seguridad de la información y normativa aplicables a esta, a la alta dirección de las textiles, con la finalidad que logren un adecuado diseño e implementación de un SGSI, además de que se agregue el área de seguridad en la información en la gestión de riesgos de la industria, con el objetivo que se le brinde la prioridad requerida en el plan de tratamiento de los riesgos corporativos.

INTRODUCCIÓN

En la actualidad toda empresa se basa en la información para tomar decisiones que permitan la continuidad del negocio, transformándose así en un activo de vital importancia para cualquier entidad, siendo necesario salvaguardarla ante posibles eventos que puede causar descomposición en los datos. Dada la importancia de la información, organizaciones internacionales de estandarización han elaborado normas de buenas prácticas para el resguardo y buen uso de la información y de los activos en general.

Además, 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 las Industrias Textiles 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 la situación actual de la información en las industrias textiles, hace referencia a las generalidades de gestión de seguridad de la información y por último se hace mención del marco legal y normativo aplicable a este trabajo.

El capítulo III describe la metodología implementada para la 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 las industrias textiles.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

Históricamente la industria textil se ha posicionado entre los sectores manufactureros más importantes de El Salvador, durante los últimos años dicho sector ha impulsado el desarrollo económico debido al aumento en el volumen de producción y la intensificación de las exportaciones, la industria textil ha logrado cierto cometido debido a la modernización de sus sistemas de manufactura e información, su proximidad geográfica y los costos de producción atractivos ante el resto de la región (JM Rivera Pineda, 2007)

A causa del crecimiento experimentado a través del tiempo, en el año 2017 se efectuaron varias denuncias sobre espionaje industrial a diversas entidades desde financieras hasta la industria textil, esto debido a fáciles accesos a los datos. Actualmente existe muchas formas de ataques informáticos cuyo fin es la de lograr obtener información para cometer actos ilícitos, de esta manera llegar a afectar a una organización. Las organizaciones que utilizan redes informáticas empezaron a entender la vulnerabilidad de los sistemas de información y la importancia de disponer de recursos cualificados para proyectar y establecer métodos y políticas de seguridad para salvaguardarlos. (JM González Flores, 2011)

Para el caso en El Salvador no es una excepción al ser entidades que depende de la innovación en estilos de ropa como: camisas, sudaderas, ropa interior, gorras etc., ya que durante décadas operó como un sencillo sistema de maquila, en la actualidad y debido al crecimiento del sector, dicha industria ha desarrollado sistemas de fabricación notablemente modernos que requieren de protección de la información. (JM González Flores, 2011)

La mayoría de industrias textiles a menudo experimentan problemas con la información debido que no cuentan con un sistema integrado, esto se debe a diferentes factores, de los cuales podemos mencionar, que las computadoras donde se almacena la información no están restringidas para el uso de cada trabajador, facilitando el robo de información por medio de USB, además no se tiene sistema de respaldo de seguridad de los datos ya sea que estos se pierdan por descuido del trabajador o por apagones eléctricos debido a que no se tiene una planta para mantener unos minutos encendidas las computadoras para guardar los cambios realizados.

1.2. ENUNCIADO DEL PROBLEMA

Debido al aumento en el uso de la tecnología como forma de innovación en empresas de la industria textil la información manejada por estas se ha convertido en un activo sustancial y por ende se debe enfatizar su importancia en asegurar la confidencialidad, integridad y disponibilidad de la misma, con el propósito de suministrar confianza a la administración de que los datos de clientes, proveedores y de la empresa están protegidos contra pérdidas que se deriven de ataques cibernéticos, robo por parte de terceras personas y procesamiento inadecuados de la misma por parte del personal de la empresa.

Por todo lo antes mencionado, el enunciado del problema se estructuró de la siguiente forma: ¿Qué amenazas pueden materializarse en las empresas de la industria textil de El Salvador, en el municipio de San Salvador, no disponer de un sistema de gestión de la seguridad de la información que les permita salvaguardar la confidencialidad, disponibilidad e integridad de la información?

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Debido a que las entidades industriales textiles poseen y procesan datos contables y administrativos, que carecen 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 misma, tal recurso se encuentra expuesto a todo tipo de amenazas como resultado de la vulnerabilidad existente, ya que no se generan las medidas sugeridas por la Organización Internacional de Estandarización (ISO por sus siglas en ingles).

Ante esta problemática se procede a resaltar la necesidad 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. Novedad

Aunque la seguridad informática en la industria textil sea un tema poco usual en los académicos contables e incluso entre contadores que ejercen la profesión (ya sea en una organización o de forma independiente) es novedoso que profesionales de la contabilidad tomen participación en áreas vinculadas a las tecnologías de la información, debido a los cambios que está surgiendo la profesión en temas de carácter tecnológicos, Además, el tema es novedoso debido a que no existe una investigación para sistemas de gestión para el sector industrial textil.

1.3.2. Factibilidad

La investigación es factible ya que existe información bibliográfica sobre los elementos que conforman la temática en estudio, entre ellos se cuenta con guías de aplicación, libros en formato físico y electrónico, legislación local e internacional, normativa internacional, que se consideran insumos de importancia para la problemática en investigación, es importante mencionar que se posee la versión de la norma internacional de estandarización número 27001:2013 aplicada en El Salvador además, se cuenta con el apoyo de un asesor metodológico especialista asignado por la Escuela de Contaduría Pública de la Facultad de Ciencias Económicas de la Universidad de El Salvador. Se cuenta con la colaboración de personal que

trabaja en las empresas textiles quienes proporcionaran ayuda con recopilación de información, explicación de procesos, llenado de encuestas y cualquier otra información necesaria para realizar la evaluación a la problemática.

1.3.3. Utilidad social

El diseño de un sistema de seguridad informática servirá a todos los empleados de las empresas, así como a las principales gerencias de tecnología, administrativas, generales, contadores públicos, departamentos de auditoría y demás entes relacionados con el sector de la industria textil, para resguardar activos tecnológicos de suma importancia, contribuyendo con el cumplimiento de los objetivos para este sector.

Al sector estudiantil de la carrera de contaduría pública y carreras afines, ya que dentro del pensum de la carrera no se profundiza temas relacionado a este, lo cual servirá como materia de apoyo y ayuda para trabajos de investigación u otros usos.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo general

Diseñar un sistema de gestión de la seguridad basada en la en la norma técnica salvadoreña ISO/IEC 27001:2013 que garantice la integridad, confidencialidad y disponibilidad de la información tanto física como lógica de las empresas dedicadas a la industria textil en El Salvador.

1.4.2. Objetivos específicos

- Determinar los requerimientos y la estructura de un sistema de gestión de seguridad tanto física como lógica.

- Diagnosticar la situación de la empresa de la industria textil en relación a los mecanismos que utilizan para salvaguardar la información.
- Proponer un sistema de gestión de seguridad de la información para las empresas dedicadas a la industria textil.
- Analizar modelos de sistemas de gestión seguridad de la información que resulten de interés para el diseño de la propuesta del trabajo de investigación.

1.5. FORMULACIÓN DE HIPÓTESIS

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, al ser implementado la información generada y procesada en la industria textil conserve su confiabilidad, disponibilidad e integridad.

1.5.2. Determinación de las 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. LIMITACIÓN DE LA INVESTIGACIÓN

La implementación de políticas de seguridad informática en la organización objeto de estudio, dependerá exclusivamente de las gerencias y altos mandos de la entidad.

CAPÍTULO II. MARCO TEÓRICO

2.1. SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA INDUSTRIA TEXTIL

La seguridad informática cobra importancia a medida que la sociedad y las empresas adoptan las nuevas tecnologías, en un ecosistema digital que se ve cada vez más amenazado por la ciberdelincuencia en todas sus formas. Los delincuentes están afinando sus técnicas para romper la seguridad de las empresas y los usuarios, y las tensiones geopolíticas están incrementando el volumen de ataques cibernéticos entre regiones clave. (Forrester, 2019)

Las industrias textiles al ser empresas que manejan información sensible como lo son datos de diseños, clientes o proveedores, entre otros, afrontan cada día riesgos provenientes de diversas fuentes que pueden perjudicar de manera significativa sus sistemas de información ya sea por ataques de terceros, errores propios al configurar sistemas y demás. 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 debilitar a una organización.

Para lograr este propósito 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.

La mayoría de entidades realiza objetivos, usualmente relacionados con el mercado y los negocios, y necesita que, desde los procesos de operaciones hasta las políticas de utilización de recursos, sean determinados a un nivel general, de forma confiable. Es normal relacionar la información con computadoras y redes, pero existen otras formas en que puede representarse, 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 sistema de gestión pretende cubrir esa actividad.

Muchas organizaciones tienen una idea equivocada en cuanto a los SGSI ya que consideran que diseñar e implementar estos sistemas es muy difícil, y que está enfocado a grandes corporaciones, lo que puede terminar provocando un manejo caótico o confuso 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. El cumplimiento de la norma ISO 27001:2013 puede ayudar a las empresas a demostrar a sus clientes o socios la seriedad con la que abordan la seguridad de la información. La certificación acreditada en la norma ISO 27001:2013, es una potente demostración del compromiso de la empresa durante la gestión de la seguridad de la información.

Entre los objetivos globales de un SGSI se pueden mencionar:

Los objetivos globales 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 que permita integrarse con otros sistemas de gestión ya implantados o a implementar a futuro.

2.2. PRINCIPALES DEFINICIONES

Las siguientes definiciones ayudarán a entender de mejor manera los términos técnicos básicos relacionados con la investigación, así como los aspectos de seguridad y el sector empresarial en el que se implementarán:

Industria textil: Agrupa las actividades dedicadas a la fabricación y obtención de fibras, hilado, tejido, tintado, y finalmente el acabado y confección de las distintas prendas, estas serán el enfoque al cual estará dirigida la investigación. (Ecured, 2016)

Información: Es un conjunto organizado de datos procesado que producen un mensaje que cambia el estado de conocimiento del sujeto o sistemas que recibe dicho mensaje. (Idalberto Chiavenato)

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC 27001:2005) este concepto nos sirve para entender el alcance del trabajo de investigación.

Confidencialidad: Propiedad de la información que garantiza que no esté accesible a personal no autorizado, sino que solo a aquellos autorizados a tener acceso a dicha información.

Disponibilidad: propiedad de estar disponible y utilizable cuando lo requiera una organización.

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 LAS INDUSTRIAS TEXTILES Y SEGURIDAD INFORMÁTICA

2.3.1. Generalidades de la industria textil

La industria textil es considerada uno de los sectores más importantes de El Salvador, ya que contribuye al ingreso de divisas a través de la participación en el mercado extranjero, además representa una de las mayores fuentes de empleo, ocupando uno de los primeros lugares en absorción de mano de obra en la ocupación directa y permanente de muchos trabajadores. (CAMTEX 2017).

Las empresas del sector industrial textil representan un área de vital importancia en la economía del país, en los últimos años se ha visto abordado por el incremento de inversiones extranjeras que consolidan la importancia de las textiles esto ha conllevado a que la información que manejan tanto de clientes como de proveedores sea de suma importación y haya necesidad de que ésta se resguarde de manera eficaz y eficiente.

Para lograr este fin las empresas deben aplicar medidas de seguridad con un sistema de gestión de riesgo con base a un Estándar Internacional como lo es la ISO/IEC 27001 dicha norma será aplicada a los diversos procesos de información sensible para la industria textil, tanto de terceros como de sí mismos (elaboración de diseños de ropa, manejo de sistemas de maquila, 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.

2.4. GENERALIDAD DE NORMA TÉCNICA SALVADOREÑA ISO/IEC 27001:2013

2.4.1. Antecedentes de la Norma Técnica Salvadoreña ISO/IEC 27001:2013

Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI's de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo. Actualmente, la última edición de 2013 este estándar se encuentra en inglés y en francés tras su acuerdo de publicación el 25 de septiembre de 2013. (ISO 27000.ES)

2.4.2. Generalidades de Norma Técnica Salvadoreña 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.

Tabla 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	***Mejora continua***

Fuente: *NTS ISO/IEC 27001:2013*

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 relación 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 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.

2.5. LEGISLACIÓN APLICABLE

La seguridad informática posee un marco legal que la regula, permitiendo desarrollar y aplicar lineamientos para el resguardo de la información que se genera dentro de las organizaciones. En la tabla 2, se muestran las leyes y artículos que se relacionan con la seguridad informática.

Tabla 2. *Legislación aplicable a la seguridad informática*

LEY APLICABLE	ARTÍCULO	DESCRIPCIÓN
Ley especial contra los delitos informáticos y conexos.	Art. 1 Objeto de la ley.	La ley en su contenido posee como objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley.
Ley especial contra los delitos informáticos y conexos.	Art. 8 Posesión de equipos o prestación de servicios para la vulneración de la seguridad.	La ley establece prisión para la posesión de equipos prestación de servicios para la vulneración de la seguridad. El que utilizando las Tecnologías de la Información y la Comunicación posea, produzca, facilite, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso; con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o preste servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente Ley, será sancionado con prisión de tres a cinco años.
Ley especial contra los delitos informáticos y conexos.	Art. 9 Violación de la seguridad del sistema.	La persona que sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, será sancionada con prisión de tres a seis años. En igual sanción incurrirá quien induzca a un tercero para que de forma involuntaria, ejecute un programa, mensaje, instrucciones o secuencias para violar medidas de seguridad. No incurrirá en sanción alguna quien ejecute las conductas descritas en los Arts. 8 y 9 inciso primero de la presente Ley, cuando con autorización de la persona facultada se realicen acciones con el objeto de conducir pruebas técnicas o auditorías de funcionamiento de equipos, procesos o programas.

Ley especial contra los delitos informáticos y conexos.	Art. 11 Fraude informático.	El que, por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado con prisión de tres a seis años.
Ley especial contra los delitos informáticos y conexos.	Art. 12 Espionaje informático.	El que con fines indebidos obtenga datos, información reservada o confidencial contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, será sancionado con prisión de cinco a ocho años. Si alguna de las conductas descritas en el inciso anterior se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas, resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada, confidencial o sujeta a secreto bancario, la sanción será de seis a diez años de prisión.
Ley especial contra los delitos informáticos y conexos.	Art. 13 Hurto por medios informáticos.	El que, por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, será sancionado con prisión de dos a cinco años.
Ley especial contra los delitos informáticos y conexos.	Art. 15 Manipulación de registros.	Los Administradores de las Plataformas Tecnológicas de instituciones públicas o privadas, que deshabiliten, alteren, oculten, destruyan, o inutilicen en todo o en parte cualquier información, dato contenido en un registro de acceso, uso de los componentes de éstos, será sancionada con prisión de cinco a ocho años. Si las conductas descritas en el inciso anterior, favorecieren la comisión de otro delito, la sanción se agravará hasta en una tercera parte del máximo señalado.

Ley especial contra los delitos informáticos y conexos.	Art. 19 Alteración, daño a la integridad y disponibilidad de los datos.	El que violando la seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento, será sancionado con prisión de tres a seis años.
Ley especial contra los delitos informáticos y conexos.	Art. 23 Divulgación no autorizada.	El que sin autorización da a conocer un código, contraseña de acceso o cualquier otro medio de acceder a un programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse así mismo, a un tercero o para cometer un delito, será sancionado con prisión de cinco a ocho años. Igual sanción tendrá el que sin autorización revele o difunda los datos o información, contenidos en un sistema informático que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, con el fin de obtener algún tipo de beneficio para sí o para otro. Si alguna de las conductas descritas en los incisos anteriores pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado, será sancionado con prisión de seis a doce años.
Ley especial contra los delitos informáticos y conexos.	Art. 25 Obtención y transferencia de información de carácter confidencial.	El que deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las Tecnologías de la Información y la Comunicación, incluidas las emisiones electromagnéticas, será sancionado con prisión de cinco a ocho años. (Asamblea Legislativa de El Salvador, 2016)
Ley de Propiedad Intelectual.	Art. 1 objeto de la ley.	Las disposiciones contenidas en la presente ley tienen por objeto asegurar una protección suficiente y efectiva de la propiedad intelectual, estableciendo las bases que la promuevan, fomenten y protejan.

Ley de Propiedad Intelectual.	Art. 32 programas informáticos.	Programa de ordenador, ya sea programa fuente o programa objeto, es la obra literaria constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador, o sea, un aparato electrónico o similar capaz de elaborar informaciones, ejecute determinada tarea u obtenga determinado resultado. Se presume que es productor del programa de ordenador, la persona que aparezca indicada como tal en la obra de la manera acostumbrada, salvo prueba en contrario.
Ley de Propiedad Intelectual.	Art. 33 contrato de programas informáticos.	El contrato entre los autores del programa de ordenador y el productor, implica la cesión ilimitada y exclusiva a favor de éste de los derechos patrimoniales reconocidos en la presente ley, así como la autorización para decidir sobre su divulgación y la de ejercer los derechos morales sobre la obra, en la medida que ello sea necesario para la explotación de la misma, salvo pacto en contrario. (Asamblea Legislativa de El Salvador , 1993)

Fuente: *Ley especial contra los delitos informáticos y conexos; Ley de propiedad intelectual*

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACION

3.1. ENFOQUE Y TIPO DE LA INVESTIGACIÓN

Para la investigación se utilizó el estudio descriptivo, 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 las industrias textiles, para ello se emplearon entrevistas con las que se recolectó los datos, que fueron analizados.

3.2. DELIMITACIÓN ESPACIAL Y TEMPORAL

3.1. Espacial

La delimitación espacial de la investigación se centró en una empresa industrial textil en el departamento de San Salvador cuyo domicilio está ubicado en el municipio de San Salvador.

3.2.2. 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, pero para efectos del trabajo de investigación comprenderá del año 2014 hasta el año 2020.

3.3. SUJETOS Y OBJETO DE ESTUDIO

3.3.1. Unidades de análisis

Para esta investigación, las unidades de análisis fueron el gerente, el contador corporativo y el ingeniero informático de la industria textil que opera en el municipio de San Salvador.

3.3.2. Población y marco muestral

Como fue citado en el apartado anterior, se cuenta con un universo finito, es decir las tres áreas ya antes mencionados de la industria textil establecida 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.

3.4. TÉCNICAS, MATERIALES E INSTRUMENTOS

3.4.1. Técnicas y procedimientos para la recopilación de la información

Se utilizó la entrevista para la obtención de información por parte de la industria textil que demuestre la perspectiva de la problemática de manera que se pudiera realizar un estudio a través de los datos cualitativos obtenidos, utilizándolos para su posterior análisis, con la finalidad de determinar el comportamiento y posibles soluciones al problema.

3.4.2. Instrumentos de medición

El instrumento de medición utilizado fueron las entrevistas, 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 la industria textil (ver anexo N° 1).

3.5. CRONOGRAMA DE ACTIVIDADES

Tabla 3. *Cronograma de actividades*

Actividad	FEB.		MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE			
	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 de seminario																																						
Desarrollo del anteproyecto																																						
Corrección del anteproyecto																																						
Entrega del Anteproyecto																																						
Elaboracion del capitulo I																																						
Correciones del capitulo I																																						
Entrega del capitulo I																																						
Elaboración del capitulo II																																						
Correciones del capitulo II																																						
Entrega del capitulo II																																						
Elaboración del capitulo III																																						
a. Elaboración de entrevistas																																						
b.Revisión y aprobación de las entrevistas																																						
c. Procesamiento de la información																																						
d. Diagnóstico de lainvestigación																																						
Correcciones capitulo III																																						
Entrega capitulo III																																						
Elaboracion del capitulo IV																																						
Desarrollo de la propuesta																																						
Correcciones al capitulo IV																																						
Entrega del capitulo IV																																						
Finalización de la investigación																																						
Preparacion para exposicion y defensa																																						
Presentación y Defensa																																						

Fuente: *Elaboración Propia*

3.6. PRESENTACIÓN DE RESULTADOS

Mediante la recolección de datos a través la entrevista que fue contestada por cada uno de los involucrados en la industria textil, 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 la industria de confección para obtener un SGSI a través de un diagnóstico.

Confidencialidad

Es importante resguardar la confidencialidad de la información dentro de la industria textil, y con la finalidad de conocer si dicha industria implementa 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 la entidad. Tal restricción es informada a los empleados de la siguiente manera: por medio de notificaciones del sistema de acceso restringido a los usuarios.

Otros aspectos relevantes son los medios que se utilizan para transferir información de los clientes, obteniéndose los siguientes: por medio de correo institucional y si es requerida física por medio de 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 entidad hace uso de controles a las instalaciones, como por ejemplo, la persona visitante tiene que llegar a recepción he identificarse y mencionar la persona qué necesita, el siguiente paso es que recepción llama al colaborador solicitado y si es posible resolver sin necesidad de entrar a la entidad más allá de la recepción se hace de esa

manera y si es necesario que la persona tenga que entrar el colaborador tiene que ir con la persona hacia el lugar donde se resolverá el asunto a tratar y al finalizar el mismo colaborador tiene que acompañar al visitante a la salida, la entidad cuenta con sistemas de video vigilancia, personal de vigilancia y sistema de alarmas.

Es importante conocer los métodos para la protección de la información física utilizada donde está se almacena en bodegas debido a que la cantidad de papel es mucho, pero esta información es guardada cuando si en el caso de ser proveedores ha sido pagada, además si ya ha sido auditada, o no se necesita de manera directa.

Concluyendo que, mediante los resultados obtenidos de la entrevista, se determina que industria textil 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.

Integridad

Según los resultados obtenidos, respecto a cómo la industria textil gestiona la integridad de la información, se puede determinar que a pesar de mantener varios controles, la mayoría van encaminados a resguardar la información física prioritariamente, restando importancia a la información digital, ya que ninguno práctica la criptografía de datos, de la industria textil no se realizan actualizaciones a los sistemas operativos de las computadoras, están en su mayoría con Windows 7 y solo las computadoras para nuevas áreas y nuevos puestos de trabajo tienen Windows 10 , cerca de 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 una de las políticas internas es realizar 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 algunas amenazas, nunca han sufrido una pérdida significativa de documentos digitales y no han sido blancos de software malicioso, lo cual no genera el interés de proteger la integridad.

El control de la documentación física mediante la autorización del uso y manejo por parte de los empleados es la segunda opción más utilizada por La industria textil, 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 se 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.

Disponibilidad

De acuerdo a los resultados obtenidos se determinó, que aunque se tienen 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 dentro de la industria, pero también es 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 prestan la debida atención al constante mantenimiento que deben recibir los sistemas informáticos, puede haber una tendencia 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 la entidad generan copias de respaldo de sus bases de datos de forma automática para algunas computadoras y en su caso en su mayoría son solo los jefes, existe la amenaza de que no garanticen la disponibilidad de la información ya que las copias de respaldo son generadas de forma manual por los colaboradores esto significa que ocasiones esta buena práctica puede ser olvida por el personal asignado para ejecutarla. Un aspecto muy importante a mencionar es que la industria brinda la debida protección de la documentación física a través de la asignación de bodegas donde se almacena la información pero para que la información venga de la bodega a la entidad se tarda un día a dos días aproximadamente, personal, esto quiere decir, que en el traslado de la bodega a la entidad 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 industria textil que no aplican medidas de seguridad, para que resguarden y protejan la información y pueda estar disponible en el momento oportuno.

CAPÍTULO IV. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EMPRESAS DEDICADAS A LA INDUSTRIA TEXTIL

4.1. PLANTEAMIENTO DEL CASO

La presente propuesta consiste en el diseño de un sistema de gestión para empresas dedicadas a la industria textil del municipio de San Salvador que garanticen la seguridad de la información basados 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 informáticos se encuentran cada vez más vulnerables a cierto tipo de amenazas que se valen de la fragilidad existente para poner en riesgo la seguridad de la información y para TEXTILES SALVADOREÑAS, S.A DE C.V. 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 involuntaria desde la propia organización o de forma externa o aquellos provocados accidentalmente como los desastres naturales o fallas técnicas.

Al estar al corriente que en muchos casos 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 nace la necesidad de proteger tal activo mediante el diseño de un SGSI donde se espera tenga participación toda la organización, con la coordinación y supervisión de alta dirección de TEXTLES SALVADOREÑAS, S.A. de C.V.

El SGSI contempla una apropiada estructura y planificación mediante la creación de controles basados en la valoración de riesgos; el sistema de gestión ayudará a través del establecimiento de diversas políticas alineadas a los objetivos estratégicos de la entidad 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.

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 1. Estructura del proyecto del SGSI

4.3. BENEFICIOS Y LIMITANTES

4.3.1. Beneficios

La propuesta del sistema de gestión de la información basado en la NTS ISO/IEC 27001:2013 pretende reducir el riesgo de que se produzcan pérdidas de información, conservando así su integridad y confidencialidad, además dicho sistema servirá como una garantía ante clientes y socios debido a que muestra cómo la entidad se preocupa por la información que maneja de terceros.

4.3.2. Limitantes

La presente propuesta está enfocada a la adopción de un SGSI basado en NTS ISO/IEC 27001:2013 sin embargo 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 etapa de planificación.

4.4. DESARROLLO DE CASO PRÁCTICO

Sistema de Gestión de Seguridad de la Información de TEXTILES SALVADOREÑAS, S.A. de C.V.

ÍNDICE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Índice de Figuras

Índice de Tablas

ETAPA 1. CONTEXTO DE LA ORGANIZACIÓN

1.1. COMPRENSIÓN DE LA ORGANIZACIÓN

1.1.1. Generalidades de la empresa

La empresa TEXTILES SALVADOREÑAS, S.A. de C.V., es una empresa con más de 24 años en el mercado, fue constituida el 26 de enero de 1995, la cual opera en el sector comercial dedicado a la venta de productos textiles fuera de la región de El Salvador. Dentro de la gama de productos que ofrece al mercado se encuentran: ropa para caballeros, ropa para dama, ropa para niños, niña y unisex.

1.1.2. Organización interna

La empresa tiene establecido las jerarquías para la toma de decisiones, como máxima autoridad se define a la junta directiva el cual aprueba todas las transacciones y actividades del entorno del negocio.

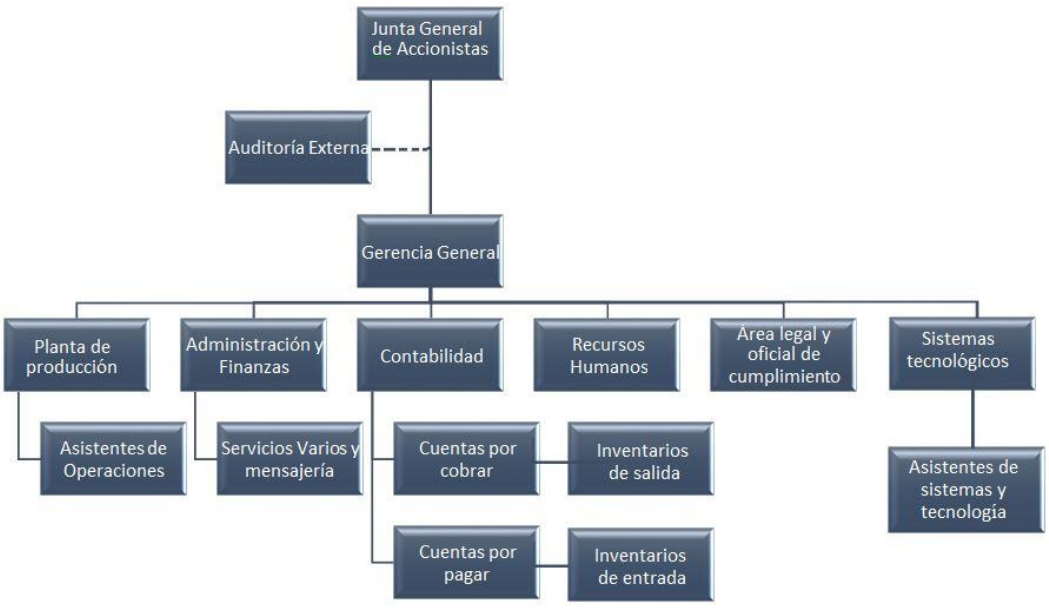

Figura 1.*Organigrama de TEXTILES SALVADOREÑOS, S.A. de C.V.*

1.1.3. Misión y visión

- **Misión:** Fabricar y comercializar ropa de excelente calidad y precios accesibles, asegurando la disponibilidad y el servicio, mantenimiento costos operativos a través del aprovechamiento de nuestros recursos. Basándonos en principios de ética, generando relaciones duraderas y de confianza con nuestros clientes, proveedores y empleados. Todo esto cumpliendo cabalmente con las obligaciones sociales y sobre todo comprometidas con el medio ambiente.
- **Visión:** Construir una empresa sólida y solvente; y ser una de las empresas líder en el ramo para ser apta de competir en el mercado internacional.

1.1.4. Objetivos y valores

Valores: Ética profesional, compromiso, confianza, lealtad, creatividad, responsabilidad y honradez.

1.1.5 Partes Interesadas

De las partes interesadas de la industria textil 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.

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 la organización.

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 a la empresa textil.

Auditoría externa: el sistema permitirá fortalecer los procesos de control interno de la textil que posteriormente son evaluados por los auditores externos.

Instituciones financieras: el SGSI generará mayor confianza en la información proporcionada por la industria textil para la adquisición de futuros servicios financieros que contribuyan al crecimiento de la entidad.

Establecimiento del alcance del SGSI.

Como se ha mencionado anteriormente que la finalidad principal de la industria textil, es la comercialización de productos textiles, 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 inter-compañías 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, esto para que todos las partes

relacionadas tengan el conocimiento acerca, del sistema para evitar futuros malentendidos en la organización.

ETAPA 2. LIDERAZGO

2.1. LIDERAZGO Y COMPROMISO DE LA ALTA DIRECCIÓN CON EL SGSI

Dentro de la norma NTS ISO/IEC 27000:2013 se aclaran ciertos principios y uno de ellos establece que dentro de la empresa es compromiso de la alta dirección liderar el cumplimiento de las políticas internas como externas establecidas, así como también apoyar al personal suministrando herramientas necesarias como capacitaciones y asignación de recursos necesarios para que desarrollen sus actividades de manera que agreguen valor a la entidad.

Para conseguir el compromiso de la alta dirección la NTS ISO/IEC 27000:2013 establece en su apartado cinco que la organización debe crear un SGSI, en el cual se incluyan prioridades y objetivos para la ejecución del mismo acompañado de un plan inicial; con la finalidad que se comprenda la importancia y objetivos del sistema. Para efectos del presente trabajo se consideran entendidos de sus compromisos.

Con el propósito de garantizar el funcionamiento del SGSI en TEXTILES SALVADOREÑAS, S.A DE C.V. es necesario contar con la ayuda y compromiso de la alta dirección, debido a que es el mayor responsable de su implementación y mejora, entre algunas de las acciones a seguir para cumplir dicho objetivo se listan las siguientes:

- Aceptar y establecer la política del SGSI: en el cual el gerente general de TEXTILES SALVADOREÑAS, S.A DE C.V., se compromete a dar cumplimiento a la política, objetivo y controles establecidos en el sistema.
- Delegar roles y responsabilidades: consiste en establecer los diferentes roles y su función que tiene cada empleado como también las responsabilidades dentro del SGSI.

- Contribuir a alcanzar los objetivos de la seguridad de la información: el compromiso de la gerencia general para definir objetivos y el, cumplimento de estos hacia el negocio que se pretenden alcanzar mediante la ejecución del sistema de información donde ambos deben formar parte para su planificación y ejecución.
- Suministrar 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: en la fase de planificación y alcance del sistema de seguridad se establece la medición de los riesgos con la finalidad de indicar cuáles son y el impacto que pueden tolerar; así como los parámetros de medición.
- Garantizar la realización de auditorías internas: para la evaluación del cumplimiento de los controles internos del SGSI, es necesario que existan auditorías internas que velen por el cumplimiento de estas.

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

TEXTILES SALVADOREÑAS, S.A DE C.V. JUNTA DIRECTIVA

AUTORIZACIÓN DE IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI

Yo francisco Boyle, gerente general y presidente de la junta directiva de TEXTILES SALVADOREÑAS, S.A DE C.V. en la sesión No._08__, de la junta directiva celebrada el día __05__, de _marzo___del año __2019__, en uso de las atribuciones legales y reglamentarias autorizo EL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORACIÓN (SGSI) PARA TEXTILES SALVADOREÑAS, 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. _____

Francisco Boyle

Presidente de Junta Directiva, Textiles Salvadoreñas, S.A. DE C.V.

2.2. POLÍTICA DE SEGURIDAD DEL SGSI

2.2.1. Presentación de la política de seguridad

En el caso de TEXTILES SALVADOREÑAS, S.A DE C.V. la información es un activo primordial, 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 seguridad y dando cumplimiento a los requerimientos legales, contractuales y regulatorios vigentes que le sean de aplicación.

La presente política deberá ser revisada por lo menos 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.

2.2.2. Política de seguridad

TEXTILES SALVADOREÑAS, S.A DE C.V. como entidad dedicada a la elaboración y confección de prendas de vestir, en el cumplimiento de su misión, visión y objetivos estratégicos apegados a sus valores corporativos y con la finalidad de satisfacer las necesidades de los clientes, motivo por el cual la alta dirección. A través del comité de seguridad de la información de la entidad, ha decidido promover y difundir a todos los niveles de la entidad la política siguiente:

“La entidad TEXTILES SALVADOREÑAS, S.A DE C.V., es responsables de cumplir con todos los requerimientos legales, contractuales, normativos y procedimentales establecidos por la alta dirección, dentro de sus áreas asignadas, que permita garantizar la disponibilidad, integridad y confidencialidad de los activos de información, para mantener una buena seguridad que posibilite continuidad del negocio”

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

- Salvaguardar todos los activos de información frente a amenazas internas o externas producidas de forma voluntaria o accidental.
- Integrar medidas de seguridad en los sistemas de información con el propósito de minimizar todos los riesgos de error humano y sucesos de origen natural.
- Concientizar a los usuarios sobre la responsabilidad de la información y sobre el establecimiento de una cultura de uso seguro.
- Denegar el acceso no autorizado a los sistemas de información, bases de datos y servicios de información y servidores.
- Detallar una herramienta de gestión, con la intención de minimizar riesgos tanto operativos como tecnológicos.
- Inspeccionar constantemente la política a fin de mantenerla actualizada y garantizar su eficiencia y eficacia, así mismo incorporar cualquier modificación que sea necesaria en función de posibles cambios que puedan afectar.
- Asegurar que los riesgos se mantengan a un nivel aceptable.

2.1.2. 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 y cada uno de los incidentes tanto interno como externo en materia de seguridad utilizando las directrices establecidas por TEXTILES SALVADOREÑAS, S.A DE C.V.
- TEXTILES SALVADOREÑAS, S.A DE C.V. dispondrá de una estructura organizacional para gestionar la seguridad de la información asegurando que se proveerán los recursos necesarios para su correcto funcionamiento.
- 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 salvaguardar los activos que almacena información de TEXTILES SALVADOREÑAS, S.A. DE C.V.
- TEXTILES SALVADOREÑAS, 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 posibles debilidades relacionadas con los sistemas de información.
- Los usuarios responsables de las áreas organizacionales y de seguridad de la información deben dar un adecuado cumplimiento de los requerimientos legales, regulatorios y contractuales, así como los establecidos en los documentos del SGSI.

2.3. ESTRUCTURA ORGANIZACIONAL DEL SGSI

2.3.1. 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 el departamento de sistemas y tecnología 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 TEXTILES SALVADOREÑA. 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.

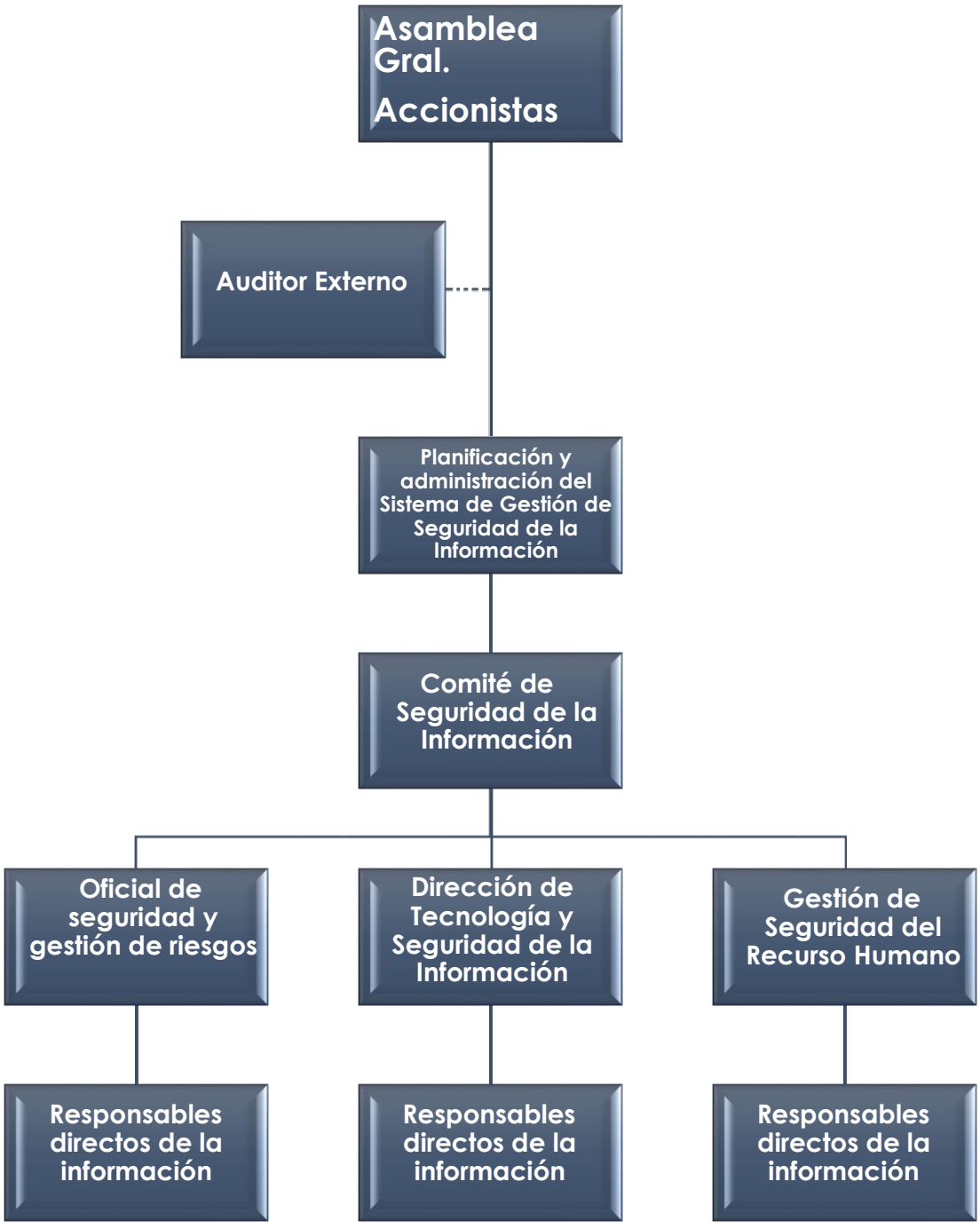

Figura 2. *Organigrama del SGSI*

2.3.2. 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.

Asamblea general de accionistas: 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:

Aprobar la política de seguridad de la información.

- Asegurar el establecimiento de la política y de los objetivos de seguridad de la información.
- Garantizar la disponibilidad de recursos para el SGSI.
- Transmitir la importancia de una gestión de seguridad eficaz y conforme a los requerimientos del SGSI.
- Apoyar y dirigir a las personas involucradas para contribuir en la eficiencia y eficacia del SGSI.
- Fomentar una cultura de seguridad de la información en la organización.
- 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

- Enfocarse en la contribución de precisar en los objetivos propuestos por la organización en relación a la política de seguridad de la información.
- Brindar apoyo necesario para que la entidad tenga eficiencia y eficacia en su en relación a la seguridad de la información.
- Identificar necesidades de instruir alguna área donde se muestren deficiencias, para fortalecer el desempeño de los colaboradores respecto al SGSI.
- 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

- Revisar la política de seguridad de la información y toda la documentación que posee la organización con relación al sistema de gestión de seguridad de la información.
- Identificar el nivel de madurez que tiene la organización en cuanto a la implementación de controles.
- Realizar un análisis de riesgo y observaciones de todas las partes interesadas.
- Determinar vulnerabilidades y amenazas que no fueron tratadas en evaluaciones anteriores.
- 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, 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 la Administración. Dentro de sus responsabilidades están:

- Diseñar conjuntamente con las demás áreas del SGSI la política de Seguridad de la información y demás lineamientos específicos.
- Elaborar los objetivos de seguridad de la información con la ayuda de las demás áreas del Sistema de gestión.
- Crear y definir lineamientos para la conformación de grupos de respuestas frente a incidentes de seguridad.
- Realizar acciones correctivas y preventivas relacionadas con la seguridad de la información.
- Establecer el alcance con la participación del resto de áreas del sistema.
- Ejecutar el plan de seguridad definido en los documentos del sistema de seguridad.
- Promover la realización de auditorías enfocadas a garantizar la seguridad de la información y la mejora continua.
- Participar en la elaboración de programas de capacitación y promover su cumplimiento.
- Coordinar y participar en labores de auditoría y consultoría y manejo de información.
- Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- 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 sistema de gestión 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 la industria textil. Estará integrado por representantes de la gerencia general, administración y finanzas, contabilidad y recursos humanos. Se detallan las responsabilidades del comité:

- Participar en la divulgación de la política de seguridad de la información.
- Garantizar el cumplimento de lo establecido en los documentos del SGSI.
- Tener participación en el análisis de riesgo de la información.
- Efectuar revisiones periódicas de la documentación vinculada a la operatividad del sistema de gestión.
- Colaborar en las actividades de seguridad y supervisar los planes de trabajo de las unidades organizacionales y de seguridad.
- Reportar de manera oportuna y eficiente las vulnerabilidades e incidentes de seguridad.
- Participar en la implementación de controles, lineamientos y procedimientos de seguridad, según los riesgos detectados.
- Amparar la ejecución de medidas correctivas que sean señaladas por las auditorias.
- Contribuir en el análisis de riesgo y ejecutar medidas necesarias para mitigar el riesgo asociado a los sistemas de información.
- 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 de la textil. 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, finanzas,

recursos humanos, 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

- Debe interpretar y conocer sobre la normativa legal vigente vinculada con la seguridad de la información bajo el contexto de las operaciones de la industria textil.
- Velar por el cumplimiento de la legislación aplicable a la seguridad de la información por parte de la industria textil.
- Actualizar la normativa legal vigente dentro del SGSI de la industria textil.
- Gestionar la implementación de las políticas de seguridad de la información junto con las demás áreas del sistema.
- Determinar los controles del SGSI.
- Atender las auditorías al SGSI y facilitar información sobre las políticas y controles implementados.

Gestión de riesgos

- Identificar los riesgos que amenazan los activos de información.
- Establecer un programa continuo que permita monitorear las vulnerabilidades y administrar los planes de su mitigación.
- Definir los mecanismos para la gestión de los riesgos de seguridad de la información.
- Informar al comité de seguridad de la información aspectos relacionados con la gestión de riesgos.

- Asegurarse la industria textil 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:

- 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 de la industria textil.
- Participar en la creación de la política de seguridad de la información y demás lineamientos específicos.
- Ser parte integral en el diseño de los objetivos de seguridad de la información.
- Determinar los roles y responsabilidades de seguridad a los responsables directos de la información.
- Responsable de los procesos de control de acceso, seguridad física, seguridad lógica y seguridad de los sistemas informáticos.
- Asignar límites a los usuarios de los sistemas.
- Realizar una comprobación que los controles determinados cumplen con los requerimientos.
- Proponer modificación de políticas o nuevas políticas de seguridad cuando sean necesarios.

Gestión de seguridad del recurso humano: es el responsable del personal de la industria textil. Sera gestionada por el área organizacional de recursos humanos. A continuación, se describen las siguientes actividades que debe ejecutar:

- Capacitar periódicamente y concientizar al personal de la textil en relación a la seguridad de la información
- 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:

- Deben conocer la estructura organizacional del SGSI y quienes serán los participantes de este.
- Cumplir con las políticas, controles y directrices de seguridad de la información
- Asistir a las capacitaciones gestionadas por el área de recursos humanos relacionadas con la seguridad de la información.
- Definir, mantener, documental, actualizar y mejorar de forma continua los procedimientos en beneficio de la seguridad de la información.
- 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.
- Hacer un uso adecuado de los activos de información de los cuales es responsable.
- Tomar participación y apoyar en la identificación, valoración y tratamiento de los riesgos de seguridad.

- Proponer mejoras los controles o políticas de seguridad del SGSI que estén vinculadas con los procesos de su trabajo.
- Mantener la integridad, disponibilidad y confidencialidad de la información que procesan para la realización de sus actividades.
- Trabajar en conjunto con el resto de áreas del SGSI.

ETAPA 3. PLANIFICACIÓN

En esta etapa se realizaron las actividades necesarias con la finalidad de garantizar que el diseño del SGSI para la industria textil 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. Para dicha actividad se utilizó 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

3.1. IDENTIFICACIÓN Y LEVANTAMIENTO DE LOS ACTIVOS DE LA INFORMACIÓN

Los activos de información en la empresa, dentro del alcance del SGSI, son fundamentales para una correcta implementación de un SGSI. En la primera actividad de esta etapa se definió una clasificación de los activos en la tabla propuesta N° 1, y en la tabla propuesta N° 2 se presenta el levantamiento de activos de información de la empresa Textiles Salvadoreñas, S.A. de C.V. y una breve descripción de cada uno y adicionalmente se identificó el área responsable de cada uno de los activos, a partir del organigrama.

Tabla 1. *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)*

Tabla 2. *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 órdenes 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	Base de datos de gestión de pago	Datos/información	Base de datos donde se gestiona los pagos a clientes representados u otros textiles, fechas de contratación, control de órdenes de entrega de productos o servicios, formas de pago, control de documentación de soporte, fechas de pago, montos de pago, liquidaciones de contratos	Contabilidad

A6	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
A7	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 3 meses.	Todos los empleados
A8	Computadoras de escritorio	Equipos informáticos	Los equipos de cómputo asignados al personal de la empresa	Todos los empleados
A9	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 8 cámaras instaladas en toda la empresa.	Administración y finanzas
A10	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
A11	Computaras portátiles	Equipos informáticos	Es un equipo informático personal que puede ser transportado fácilmente.	Gerentes generales
A12	Sistema de alarmas	Equipo auxiliar	Equipos electrónicos instalados en lugares estratégicos para detectar movimientos sospechosos mediante sensores, uso de contactos magnéticos, detectores de humo.	Administración y finanzas
A13	Escáner	Equipos informáticos	Periférico de la computadora que permite digitalizar imágenes impresas para transferirla a un dispositivo externo	Todos los empleados
A14	Oficinas	Instalaciones	Instalación física donde se realizan las operaciones de la entidad y el procesamiento de datos	Todos los empleados

A15	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
A16	Instalaciones eléctricas	Instalaciones	Conjunto de cableado y otros dispositivos para la distribución de energía eléctrica a todas las plantas de producción de la entidad	Servicios Externos
A17	Bodega de almacenamiento de información	Instalaciones	Sala o espacio físico donde se realiza la manufactura de los diferentes productos que comercializa la empresa.	Administración y finanzas
A18	Maquilas	Personal	Personal encargado a la atención a visitantes y llamadas, proporcionando información autorizada por sus superiores.	Recursos Humanos
A19	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
A20	Personal de contabilidad	Personal	Encargados del procesamiento de información financiera y contable de la entidad.	Recursos Humanos
A21	Diseñadores de producto	Personal y Redes de Comunicación	Encagado de la elaboración de diseños de las diferentes productos de la textilera	Recursos Humanos .
A22	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
A23	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
A24	Servidor Windows	Redes de Comunicación	Computador bajo sistema operativo Windows que provee de servicios en una red.	Servicios Externos

A25	Correos electrónicos	Redes de Comunicación	Red de comunicación que permite transmitir y recibir información.	Servicios Externos
A26	Sistemas operativos	Software	Software básico que facilita la interacción entre el usuario y demás programas un ordenador	Servicios Externos
A27	Antivirus y firewall	Software	Software de administración de seguridad	Servicios Externos
A28	Aplicaciones de trabajo	Software	Herramientas y accesorios incorporados al ordenador.	Servicios Externos
A29	Documentación física clasificada	Soportes de información	Soporte físico del registro de las operaciones de la organización.	Todos los empleados
A30	Documentación digital clasificada	Soportes de información	Soporte digital de los registros de las operaciones de la organización.	Todos los empleados
A31	Copias de respaldo	Soportes de información	Medidas de seguridad y reserva de los archivos y directorios de la organización	Contabilidad y Recursos Humanos
A32	Manuales de usuarios	Soportes de información	Instructivos o guías de orientación.	Administración y finanzas
A33	Planta eléctrica	Equipamiento auxiliar	Generador de electricidad a través de combustión	Servicios externos

Fuente: Elaboración propia

3.2. 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.

Con base a lo anterior, y para facilitar el proceso de identificación de amenazas y vulnerabilidades la Tabla propuesta N°3, "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.

3.2.1. Riesgos de los activos de información

Una vez que determinadas diferente activos que posee la organización se procedió a identificar los riesgos asociados a dichos activos, por tal razón la Tabla propuesta N°4 , "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 3. *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 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.

	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.
Desastres de origen industrial	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 intencionado	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 y fallos no intencionados	Errores de 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 y fallos no intencionados	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.
	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
Actos deliberados	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 (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.
Actos deliberados			
	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.
Actos deliberados	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, indebida asignación roles y permisos.

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

Tabla 4. *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 A33	X		
R2	Accesos no autorizados a oficinas, sistemas de información y equipos	A1 hasta A12, A14 hasta A33.		X	X
R3	Ataques de hacking no ético (interno y externo)	A1 hasta A12, A21 hasta A31,	X	X	X
R4	Uso de privilegios de forma inadecuada	A1 hasta A1, A11 A15, A22, A23 A29 hasta A31		X	X
R5	Interceptar sin autorización la información enviada o recibida	A22, A23,A25,A28 y A29 hasta A31.		X	X
R6	Robo, extravío o sabotaje de la información que es propiedad de la entidad.	A1 hasta A11, A14 hasta A17, A22 hasta A31 y A33.	X	X	X
R7	Indisponibilidad de los servicios proporcionados por fallas generadas por los sistemas informáticos o eléctricos.	A1 hasta A10, A12, A15, A16, A22 hasta A33	X	X	
R8	Cambios o alteración de privilegios sin la respectiva autorización por parte del administrador	A1 hasta A8, A10, A11, A15,A21 hasta A31.		X	X
R9	Acciones no intencionales por parte del administrador	A1 hasta A16, A23, A24, A29 hasta A32.		X	

	R10	Uso inadecuado o divulgación no autorizada de información de autenticación	A1 hasta A9, A11, A13, A14, A17, A22, A23, A25 y A29 hasta A32.		X	X
	R11	Modificación de la información sin autorización pertinente	A1 al A7,A10,A21, A25 y A29 hasta A32.	X	X	
	R12	Extracción no autorizada de equipos	A8,A9,A11,A13.	X	X	
	R13	Manipulación de los sistemas informáticos para propiciar daños o fraudes	A1 hasta A8, A11,A23 y A24 hasta A32.	X	X	
	R14	Instalación de software no autorizado en los equipos informáticos de la entidad	A1 hasta A8, A10, A11, A21, A23 hasta A28, A30 y A31	X	X	X
	R15	Suplantación de identidad de los usuarios y administradores	A1 hasta A11, A25, A27, A28 hasta A32.		X	X

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

3.2.2. Análisis y evaluación de riesgos

Para la evaluación de riesgos es necesario tomar en cuenta lo siguiente:

- 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.

3.2.3. 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° 5.

La valoración de los riesgos se realizó tomando en cuenta la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (conocido como MAGERIT).

Tabla 5. *Escala de probabilidad de ocurrencia*

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

Fuente: *Elaboración propia*

Para determinar el nivel de riesgo de los activos, se muestra en la tabla propuesta N° 6 el nivel de riesgo según el valor obtenido del producto entre la probabilidad de ocurrencia, provenientes de la tabla propuesta N° 5. 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 6. *Escala de valoración de nivel de riesgos*

Nivel de riesgo	Gestión del riesgo
Riesgo Grave	Requiere de atención máxima y es necesario ejecutar acciones inmediatas que consigan mitigar, compartir, transferir o eludir el riesgo.
Riesgo Alto	Se necesita atención urgente y ejecutar medidas para mitigar el nivel de riesgo
Riesgo Moderado	Se requiere de medidas rápidas e idóneas que permitan disminuir el riesgo a bajo o mínimo
Riesgo Bajo	El riesgo se puede mitigar con actividades propias y mediante acciones preventivas para disminuir el riesgo
Riesgo Mínimo	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)*

3.2.4. Mapa de riesgo

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° 3 “Gráfico 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.

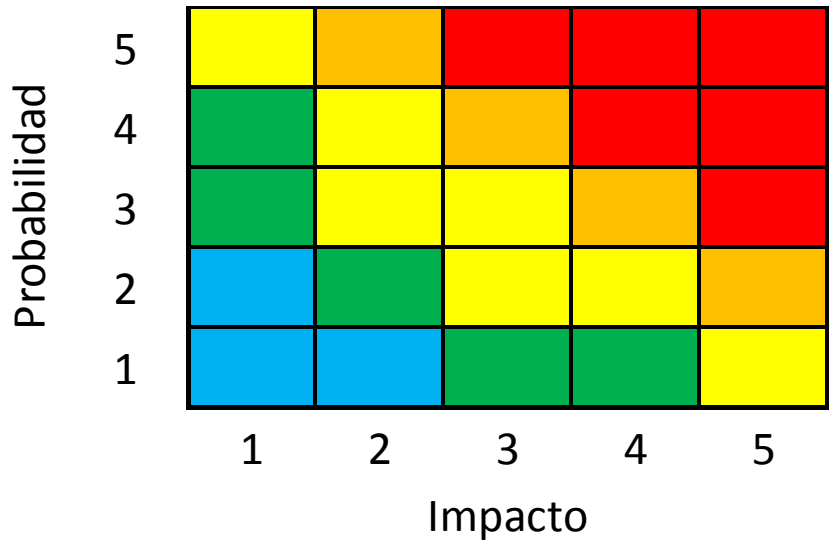

***Figura* 3**.*Gráfico mapa de calor*

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, 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.

3.2.5. 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 TEXTILES SALVADOREÑAS S.A. de C.V. Primero se define el nivel de riesgo cualitativo, el cual se expone en la tabla propuesta N°7 partiendo del impacto que este puede ocasionar a los objetivos de la seguridad de la información: Disponibilidad (D), Integridad (I) y Confidencialidad (C). Además de la probabilidad de ocurrencia del mismo.

Tabla 7. *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)*

3.3. PLAN DE GESTIÓN DE RIESGOS

Una vez realizado la evaluación del riesgo a la cual se encuentran expuestos los activos de información de TEXTILES SALVADOREÑAS S.A. 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 y con qué frecuencia este puede suceder, ante lo mencionada se presentan cuatro estrategias básicas para la gestión del riesgo en la tabla 8, que sirve como guía ante las acciones a seguir por parte de la administración antes y después que el riesgo se materialice.

Tabla 8. *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: *International Federation Red Crescent Societies*

Una vez determinadas 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 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° 9, la cual muestra las opciones que se establecieron para cada uno de los riesgos identificados.

Tabla 9. *Determinación de opción de tratamiento a riesgos de los activos de información*

Código de Riesgo	Riesgo	Riesgo	Opción de Tratamiento
R1	Desastres naturales	MODERADO	Transferir 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

Fuente: *COBIT 5*

3.3.1. 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. 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° 9, donde se definió la opción de tratamiento a cada riesgo. A continuación, en la tabla propuesta N° 10 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 Textiles Salvadoreñas S.A. DE C.V.).

Tabla 10. *Plan de gestión de riesgo*

Riesgos	Activos	Opción de tratamiento de riesgo	Actividades a realizar	Controles	Responsable
Desastres naturales	Desde A10 hasta A33	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	A1 hasta A12, A14 hasta A33.	Evitar el riesgo	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.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

Ataques de hacking no ético (interno y externo)	A1 hasta A12, A21 hasta A31,	Reducir el riesgo	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 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.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. ✓ 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.	
			Revisar frecuentemente las bitácoras de entrada a las áreas de seguridad y los Log de eventos de seguridad		
Uso de privilegios de forma inadecuada	A1 hasta A1, A11 A15, A22, A23 A29 hasta A31	Reducir el riesgo	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 súper 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	A22, A23,A25,A28 y A29 hasta A31.	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 A11, A14 hasta A17, A22 hasta A31 y A33.	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.	✓ A.8.2. Clasificación de la información. ✓ A.8.3. Gestión de medios (dispositivos donde se guarda información).	
			Clasificación de la información según su confidencialidad. Asegurar la aplicación del bloqueo de dispositivos externos en los equipos de cómputo de la empresa	✓ 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.	
			Verificar continuamente los Log de eventos de seguridad	✓ 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.	A1 hasta A10, A12, A15, A16, A22 hasta A33	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 hasta A8, A10, A11, A15,A21 hasta A31.	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 A16, A23,A24,A29 hasta A32.	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, A11, A13, A14, A17, A22, A23, A25 y A29 hasta A32.	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,A10,A21, A25 y A29 hasta A32.	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	A8,A9,A11,A13	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 hasta A8, A11,A23 y A24 hasta A32.	Evitar el riesgo	Garantizar una adecuada segregación de responsabilidades Verificar continuamente los Log 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 hasta A8, A10, A11, A21, A23 hasta A28, A30 y A31	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 hasta A11, A25, A27, A28 hasta A32.	Reducir el riesgo	Verificar continuamente los Log 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) (Águila Portillo, Cruz Reyes, & Hernández Villacorta, 2009) (Franco, 2015) (Figueroa, Flores, & Samayoa, 2013)*

CONCLUSIONES

- La seguridad informática en las empresas de la industria textil muestra vulnerabilidad y/o riesgos, esto producto a que la normativa con la que cuentan, no está basada en criterios técnicos o estándares internacionales especializados en el tema, adicional las amenazas informáticas están al asecho para provocar perdida o alteración de datos, así como fallos en los sistemas de información que interfieran en las operaciones de las empresas del sector.

- 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.

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

- La carencia de una metodología de seguridad para las industrias textiles 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.

RECOMENDACIONES

Después de realizada la investigación, se recomienda lo siguiente:

- A las empresas del sector de la industria textil, fortalecer la seguridad informática para lo cual optar por asistencia técnica para la elaboración, aprobación e implantación, de políticas fundamentadas en estándares internacionales; como lo es la Norma Técnica Salvadoreña ISO/IEC 27001:2013 "Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requerimientos".

- Que las gerencias de las empresas textiles capaciten 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 la entidad), con la finalidad que logren un adecuado diseño e implementación de un SGSI.

- Que los responsables de la gestión de riesgos organizacionales en las industrias textiles, 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.

- Se recomienda a las industrias textiles 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 la cual servirá como base para minimizar los eventuales riesgos que poseen cada entidad textil.

BIBLIOGRAFIA

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.

Brandy echogoyen, Salina R., Reyes Portillo S.L. (2017). Sistema de gestión de seguridad para los puestos de bolsa de productos y servicios que garantice la integridad, confidencialidad y disponibilidad de la información.Universidad de El Salvador.

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.

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.

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

Mateo Cruz. L.M.,Estrada. Irving. O.,Canizalez H.(2016) . Para empresas del sector de logística y transporte de carga del municipio de antiguo Cuscatlán basadas en la norma técnica salvadoreña iso/iec 27001:2013.San Salvador, El Salvador.

ANEXO

Anexo 1. Modelo de encuesta de entrevista de trabajo

Encuesta realizada a la industria textil.

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

Entrevista

Dirigido a: Gerente responsable, contador corporativo y ingeniero informático de la administración de la industria textil.

Tema de Investigación: SISTEMA DE GESTIÓN PARA EMPRESAS DEDICADAS A LA INDUSTRIA TEXTIL DEL MUNICIPIO DE SAN SALVADOR QUE GARANTICEN LA SEGURIDAD DE LA INFORMACIÓN BASADOS EN LA NORMA TÉCNICA SALVADOREÑA ISO/IEC 27001:2013

Objetivo: Recopilar información necesaria referente a la forma en cómo las industrias textiles en El Salvador gestionan la integridad, confidencialidad y disponibilidad de la información física y digital que procesan.

Indicaciones:

Pregunta 1. ¿Cuál es la forma en que la organización informa a los usuarios sobre restricciones de uso de información confidencial?

Objetivo: conocer la existencia del riesgo de que la información sea modificada por personal no autorizado e identificar la existencia de un compromiso de la alta dirección en relación a la confidencialidad y protección de la información.

Pregunta 2. ¿Cuál es el medio que más utilizan para solicitar o transferir información perteneciente a los clientes?

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

Pregunta 3. ¿Qué tipo de actividades son realizadas para concientizar al personal en cuanto a la importancia de la seguridad de la información?

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.

Pregunta 4. ¿Cuáles son los medios y/o lugares de almacenamiento para el resguardo de la información digital propia y de terceros?

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

Pregunta 5. ¿Qué controles aplican en la textil

para mantener la integridad de la información?

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.

Pregunta 6. ¿Cuáles son los métodos utilizados para la protección de la documentación física?

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.

Pregunta 7. ¿Qué tipo de controles son implementados en la entidad para que la información esté disponible en el momento oportuno?

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

Pregunta 8. En alguna ocasión ha sucedido pérdida de información, (si la respuesta es sí, realizar la siguiente pregunta), Cuando ha sucedido la pérdida de información (física o digital) en la organización, ¿Cuáles fueron los factores que la originaron?

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

Pregunta 9. En caso de un siniestro, ¿Cuál sería el plan de acción para recuperar la información perdida a causa de un siniestro?

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

Pregunta 10. ¿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.

Pregunta 11. ¿Tiene conocimiento sobre la norma ISO/IEC 27001: 2013?

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

Pregunta 12. Si se diseñara un Sistema de Gestión de Seguridad de la Información personalizado para la industria textil, ¿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.

Pregunta 13. Si se diseñara un Sistema de Gestión de Seguridad de la Información personalizado para la industria textil, ¿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.

Anexo 2.Encuesta de entrevista a gerente general

Encuesta realizada a la industria textil.

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

Entrevista

Dirigido a: Gerente responsable, contador corporativo y ingeniero informático de la administración de la industria textil.

Tema de Investigación: SISTEMA DE GESTIÓN PARA EMPRESAS DEDICADAS A LA INDUSTRIA TEXTIL DEL MUNICIPIO DE SAN SALVADOR QUE GARANTICEN LA SEGURIDAD DE LA INFORMACIÓN BASADOS EN LA NORMA TÉCNICA SALVADOREÑA ISO/IEC 27001:2013

Objetivo: Recopilar información necesaria referente a la forma en cómo la industria textil e El Salvador gestionan la integridad, confidencialidad y disponibilidad de la información física y digital que procesan.

Indicaciones: Conteste las siguientes preguntas con la mayor objetividad posible.

Pregunta 1. ¿Cuál es la forma en que la organización informa a los usuarios sobre restricciones de uso de información confidencial?

R/Si

Notificaciones del sistema de acceso restringido a los usuarios.

Objetivo: conocer la existencia del riesgo de que la información sea modificada por personal no autorizado e identificar la existencia de un compromiso de la alta dirección en relación a la confidencialidad y protección de la información.

Pregunta 2. ¿Cuál es el medio que más utilizan para solicitar o transferir información perteneciente a los clientes?

R/Correos institucionales y fichas de clientes en sistema financiero.

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

Pregunta 3. ¿Qué tipo de actividades son realizadas para concientizar al personal en cuanto a la importancia de la seguridad de la información?

R/No hay difusión del tema.

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.

Pregunta 4. ¿Cuáles son los medios y/o lugares de almacenamiento para el resguardo de la información digital propia y de terceros?

R/Servidores privados y un backup internacional.

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

Pregunta 5. ¿Qué controles aplican en los diferentes textiles para mantener la integridad de la información?

R/Cada reporte que se elabora tiene que analizarlo cada jefe debido a que ellos son los que presentan los mismo a la administración.

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.

Pregunta 6. ¿Cuáles son los métodos utilizados para la protección de la documentación física?

R/La mayoría de información se maneja de forma digital para reducir gastos de papelería, administración y almacenaje sin embargo es imprimible en caso de ser necesario.

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.

Pregunta 7. ¿Qué tipo de controles son implementados en la entidad para que la información esté disponible en el momento oportuno?

R/Registro en las bases del sistema financiero SAP.

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

Pregunta 8. En alguna ocasión ha sucedido pérdida de información, (si la respuesta es sí, realizar la siguiente pregunta), Cuando ha sucedido la pérdida de información (física o digital) en la organización, ¿Cuáles fueron los factores que la originaron?

R/En los últimos 5 años nada significativo.

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

Pregunta 9. En caso de un siniestro, ¿Cuál sería el plan de acción para recuperar la información perdida a causa de un siniestro?

R/Descargar el backup de los servidores internacionales.

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

Pregunta 10. ¿En el caso de las licencias de los diferentes programas, se tienen las licencias originales para cada computadora?

R/Si, debido a que es necesario para determinar en un dado caso quien envía esa información.

Objetivo: Determinar si la entidad cuenta con las licencias originales.

Pregunta 11. ¿Conoce acerca de los Sistemas de Gestión de Seguridad de la Información?

R/Parte del pensum de mi formación académica y el rol que me corresponde dentro de la empresa involucran ejes transversales al tema.

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

Pregunta 12. ¿Tiene conocimiento sobre la norma ISO/IEC 27001: 2013?

R/Básico.

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

Pregunta 13. Si se diseñara un Sistema de Gestión de Seguridad de la Información personalizado para la industria textil, ¿le sería atractivo implementarlo para mejorar la integridad, confidencialidad y disponibilidad de la información que se procesa en la organización?

R/Estaría sujeto a un análisis de costo - benéfico en función del nivel de prioridad del riesgo a tratar sin embargo en términos generales no parece ser un riesgo potencial alto ya que su probabilidad de incidencia es bajo a pesar que puede tener consecuencias graves.

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

Anexo 3.Encuesta de entrevista a contador general

Encuesta realizada a la industria textil.

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

Entrevista

Dirigido a: Gerente responsable, contador corporativo y ingeniero informático de la administración de la industria textil.

Tema de Investigación: SISTEMA DE GESTIÓN PARA EMPRESAS DEDICADAS A LA INDUSTRIA TEXTIL DEL MUNICIPIO DE SAN SALVADOR QUE GARANTICEN LA SEGURIDAD DE LA INFORMACIÓN BASADOS EN LA NORMA TÉCNICA SALVADOREÑA ISO/IEC 27001:2013"

Objetivo: Recopilar información necesaria referente a la forma en cómo la industria textil e El Salvador gestionan la integridad, confidencialidad y disponibilidad de la información física y digital que procesan.

Indicaciones: Conteste las siguientes preguntas con la mayor objetividad posible.

Pregunta 1. ¿Cuál es la forma en que la organización informa a los usuarios sobre restricciones de uso de información confidencial?

R/Si se tienen accesos limitados según sea su función y la necesidad, es decir, solo los jefes pueden dar acceso a las personas para poder ingresar memorias USB o desbloquear su navegador de internet, lo malo de este caso es que no se maneja con la objetividad debido a que muchos tienen los accesos sin necesitarlos.

Por medio de notificaciones del sistema de acceso restringido a los usuarios.

Objetivo: conocer la existencia del riesgo de que la información sea modificada por personal no autorizado e identificar la existencia de un compromiso de la alta dirección en relación a la confidencialidad y protección de la información.

Pregunta 2. ¿Cuál es el medio que más utilizan para solicitar o transferir información perteneciente a los clientes?

R/Correos institucionales y fichas de clientes en sistema financiero, en raro caso el uso de memorias USB ya que todo se utiliza por medio del correo institucional.

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

Pregunta 3. ¿Qué tipo de actividades son realizadas para concientizar al personal en cuanto a la importancia de la seguridad de la información?

R/No se tiene ninguna acerca de este tema, debido a que no se a sufrido con pérdidas en la información que la entidad se haya enterado.

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.

Pregunta 4. ¿Cuáles son los medios y/o lugares de almacenamiento para el resguardo de la información digital propia y de terceros?

R/Es por medio de servidores privados o backup internacionales, se crean accesos en carpetas colocadas en la red donde solo tienen acceso los equipos de trabajo.

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

Pregunta 5. ¿Qué controles aplican en los diferentes textiles para mantener la integridad de la información?

R/El jefe inmediato de cada colaborador tiene el deber de verificar la información debido a que son un filtro para que esta sea mandada a la administración.

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.

Pregunta 6. ¿Cuáles son los métodos utilizados para la protección de la documentación física?

R/Pues en el caso de la contabilidad se tiene una bodega asignada para guardar las facturas de los clientes o papeles importantes estas se almacenan en cajas rotuladas de cada compañía y se envían para el resguardo de las mismas cabe mencionar que debido al movimiento de inventarios la cantidad de papelería es alta y no se puede tener en el departamento.

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.

Pregunta 7. ¿Qué tipo de controles son implementados en la entidad para que la información esté disponible en el momento oportuno?

R/Si es documentación física se manda a traer a las bodegas donde están almacenadas si es que estas ya fueron guardas, en caso de que se tengan a la mano y es necesaria se entrega, si se requiere de forma digital se escanea la información para ser enviada, si son programas como Excel, SAP u otros es más fácil porque se tiene a la mano.

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

Pregunta 8. En alguna ocasión ha sucedido pérdida de información, (si la respuesta es sí, realizar la siguiente pregunta), Cuando ha sucedido la pérdida de información (física o digital) en la organización, ¿Cuáles fueron los factores que la originaron?

R/En los últimos años no ha ocurrido algo significativo, y si ocurriera no se tiene en si un plan pero si los archivos de relevancia están escaneados y guardados en la red.

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

Pregunta 9. En caso de un siniestro, ¿Cuál sería el plan de acción para recuperar la información perdida a causa de un siniestro?

R/Descargar la información de la red es necesario que cada colaborador tenga que guardar sus reportes en la red ya que si ocurre un siniestro tiene los soportes en otro lugar además que en su computadora personal.

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

Pregunta 10. ¿En el caso de las licencias de los diferentes programas, se tienen las licencias originales para cada computadora?

R/Si para cada una en específico según sea lo que el trabajador necesite tiene su licencia personal ya que es importante ver en los diferentes sistemas la procedencia de la información.

Objetivo: Determinar si la entidad cuenta con las licencias originales.

Pregunta 11. ¿Conoce acerca de los Sistemas de Gestión de Seguridad de la Información?

R/Si tengo conocimientos al respecto.

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

Pregunta 12. ¿Tiene conocimiento sobre la norma ISO/IEC 27001:2013?

R/En términos generales puedo decir que tengo un conocimiento básico a cerca de esta ISO.

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

Pregunta 13. Si se diseñara un Sistema de Gestión de Seguridad de la Información personalizado para la industria textil, ¿le sería atractivo implementarlo para mejorar la integridad, confidencialidad y disponibilidad de la información que se procesa en la organización?

R/Si media vez encaje con las mismas metas de la entidad es bienvenido.

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

Anexo 4.Encuesta de entrevista a ingeniero en sistemas

Encuesta realizada a la industria textil.

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

Entrevista

Dirigido a: Gerente responsable, contador corporativo e ingeniero informático de la administración de la industria textil.

Tema de Investigación: "SISTEMA DE GESTIÓN PARA EMPRESAS DEDICADAS A LA INDUSTRIA TEXTIL DEL MUNICIPIO DE SAN SALVADOR QUE GARANTICEN LA SEGURIDAD DE LA INFORMACIÓN BASADOS EN LA NORMA TÉCNICA SALVADOREÑA ISO/IEC 27001:2013"

Objetivo: Recopilar información necesaria referente a la forma en cómo la industria textil e El Salvador gestionan la integridad, confidencialidad y disponibilidad de la información física y digital que procesan.

Indicaciones: Conteste las siguientes preguntas con la mayor objetividad posible.

Pregunta 1. ¿Cuál es la forma en que la organización informa a los usuarios sobre restricciones de uso de información confidencial?

R/ Si.

Por medio de notificaciones del sistema de acceso restringido a los usuario, por ejemplo el internet está bloqueado para los colaboradores mas no para los jefes pero los jefes pueden dar la autorización para que sus trabajadores puedan tener internet, además no se permite el acceso a memorias USB, pero esto es si el jefe pide que tengan este acceso lo tienen libre en este caso la mayoría de colaboradores tienen el acceso.

Objetivo: conocer la existencia del riesgo de que la información sea modificada por personal no autorizado e identificar la existencia de un compromiso de la alta dirección en relación a la confidencialidad y protección de la información.

Pregunta 2. ¿Cuál es el medio que más utilizan para solicitar o transferir información perteneciente a los clientes?

R/ En el caso de los que estamos en el área de sistemas no tratamos mucho con los clientes en una manera directa pero si se le pide a los departamentos que lo hacen que lo hagan en primera instancia por correo electrónico y si no es posible de esta manera que sea por USB.

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

Pregunta 3. ¿Qué tipo de actividades son realizadas para concientizar al personal en cuanto a la importancia de la seguridad de la información?

R/No se tiene ninguna de este tema en este momento, debido a que no se ha sufrido con pérdidas en la información en la entidad que nosotros nos hayamos enterado.

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.

Pregunta 4. ¿Cuáles son los medios y/o lugares de almacenamiento para el resguardo de la información digital propia y de terceros?

R/Es por medio del almacenamiento de este en la memoria de la computadora o por medio de la red que se tiene cada departamento ahí pueden tener sus archivos por cualquier inconveniente con la PC.

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

Pregunta 5. ¿Qué controles aplican en los diferentes textiles para mantener la integridad de la información?

R/ En este momento no se tiene un control por parte del área de sistemas debido a que no tocamos la información ya sea de contabilidad o de recursos humanos pero lo que si se tiene que hacer en todos los departamentos, es que el jefe inmediato debe revisar la información de los colaboradores antes de ser enviada a la dirección.

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.

Pregunta 6. ¿Cuáles son los métodos utilizados para la protección de la documentación física?

R/ Todos los departamentos tiene bodegas asignadas las cuales no están en estas instalaciones, esto es debido a que la cantidad de papel que se maneja es considerable.

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.

Pregunta 7. ¿Qué tipo de controles son implementados en la entidad para que la información esté disponible en el momento oportuno?

R/ Eso depende de cada departamento ya que si ellos no han enviado a la bodega lo que ya han procesado tienen la información física a la mano, pero si es enviada tienen que solicitar que se las traigan por medio del motorista ya que estas están almacenadas en cajas rotuladas y por fechas.

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

Pregunta 8. En alguna ocasión ha sucedido pérdida de información, (si la respuesta es sí, realizar la siguiente pregunta), Cuando ha sucedido la pérdida de información (física o digital) en la organización, ¿Cuáles fueron los factores que la originaron?

R/ Pues no ha sucesido nada significativo, debido a que cuando vienen visitantes o proveedores o clientes hay un proceso el cual él tiene que identificarse en recepción y recepción llama a la persona encargada al cual el visitante busca y el colaborador tiene que ir a recepción si es posible resolver en ese lugar no hay más acceso a las instalaciones pero si debe de entrar tiene que el colaborador acompañarlo y estar con desde la entrada y salida a manera de escoltarlo y además para que él no se pierda dentro de las instalaciones .

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

Pregunta 9. En caso de un siniestro, ¿Cuál sería el plan de acción para recuperar la información perdida a causa de un siniestro?

R/ Como antes lo mencione el colaborador debe guardar en la red si él lo desea pero no todos lo hacen en su mayoría solo lo guarda en su computador, en el caso de la información física ignoro si se tiene todo escaneado ya que las cosas de relevancia si se tienen que escanear.

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

Pregunta 10. ¿En el caso de las licencias de los diferentes programas, se tienen las licencias originales para cada computadora?

R/ Si para cada computadora se tienen licencias según los programas que el colaborador necesitara y estos tienen sus iniciales para conocer la procedencia de los archivos.

Objetivo: Determinar si la entidad cuenta con las licencias originales.

Pregunta 11. ¿Conoce acerca de los Sistemas de Gestión de Seguridad de la Información?

R/Si conozco en buena medida a cerca de ellos.

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

Pregunta 12. ¿Tiene conocimiento sobre la norma ISO/IEC 27001:2013?

R/ Si conozco de la norma aunque no es aplicada en esta industria pero si se que trata a cerca de la seguridad de la información.

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

Pregunta 13. Si se diseñara un Sistema de Gestión de Seguridad de la Información personalizado para la industria textil, ¿le sería atractivo implementarlo para mejorar la integridad, confidencialidad y disponibilidad de la información que se procesa en la organización?

R/Si sería atractivo debido a que podría llenar aquellos espacios que no están libres de riesgo y mejorar la calidad de la información.

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