UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

“SISTEMA DE GESTIÓN EN LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27032 CON ENFOQUE EN MODALIDAD DE TELETRABAJO PARA EL PROFESIONAL DE CONTADURÍA PÚBLICA EN UNA EMPRESA INDUSTRIAL EN EL MUNICIPIO DE SOYAPANGO”

TRABAJO DE INVESTIGACIÓN PRESENTADO POR:

CRUZ RIVERA, ERICK GUSTAVO

GÓMEZ MANZANO, HERMES MANRRIQUE

VÁSQUEZ DE GUILLEN, JOSELIN IVANIA

PARA OPTAR AL GRADO DE:

LICENCIATURA EN CONTADURÍA PÚBLICA

NOVIEMBRE 2020

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	:Msc. Roger Armando Arias Alvarado.
Secretario General	:Msc. Francisco Antonio Alarcón Sandoval
Decano de la Faculta de Ciencias Económicas	:Lic. Nixon Rogelio Hernández Vásquez.
Secretaría de la Facultad de Ciencias Económicas	:Lic. Vilma Marisol Mejía Trujillo
Directora de la Escuela de Contaduría Pública	:Lic. Gilberto Díaz Alfaro
Coordinador General de Seminario de Graduación	:Lic. Mauricio Ernesto Magaña Menéndez
Coordinador de Seminario de Procesos de Graduación de Contaduría Pública	:Lic. Daniel Nehemías Reyes López
Docente Director	:Lic. Carlos Nicolás Fernández Linares.
Jurado Evaluador	: Lic. Carlos Nicolás Fernández Linares. : Lic. Daniel Nehemías Reyes López : Lic. Abraham de Jesús Ortega Chacón

Noviembre 2020
San Salvador, El Salvador, Centro América

AGRADECIMIENTOS

Agradezco a Dios, por guiar mis pasos con sabiduría, darme fortaleza en momentos de flaqueza. A mi madre Carolina Manzano por todo su amor, comprensión y sacrificio, a mi padre Hermes Gómez, mis hermanas por estar siempre a mi lado dándome ánimos y empujándome a seguir; a mi grupo de trabajo, por abonar sus conocimientos, compromiso y dedicación a seguir a pesar de la situación y los problemas acontecidos durante este año; a los asesores que nos brindaron su tiempo, consejos y apoyo en la trayectoria del trabajo y a todos aquellos que de alguna manera brindaron su apoyo en muchos aspectos profesionales a lo largo de este camino.

Hermes Manrrique Gómez Manzano

Agradezco muchísimo a Dios por cuidarme, darme sabiduría e inteligencia y permitirme culminar mi carrera de contaduría pública, a mis padres, mi Madre una extraordinaria mujer que ha luchado tanto por sacarme adelante, por ser tan fuerte e inteligente, y por darme todo su apoyo, a mi Padre un hombre que me aconseja y me da su apoyo y su conocimiento en todo lo que puede, y por tener la paciencia de explicarme; a mis hermanos por aconsejarme, cuidarme, y estar ahí siempre que los necesito; a mis familiares por su apoyo, a mis catedráticos por su conocimiento, a mis compañeros de tesis por el esfuerzo y dedicación, a la universidad de el salvador por darme la oportunidad de prepararme, y a todos, Gracias.

Erick Gustavo Cruz Rivera

Agradezco a Dios por ser mi guía, estar conmigo en cada momento. A mi madre por inculcarme a seguir mis sueños pese a las adversidades, A mi padre por ser mi ejemplo, por dedicarme tiempo, por brindarme sus conocimientos y experiencias a largo de mi vida, por motivarme y apoyarme, A mí esposo por su apoyo y acompañamiento incondicional, que con su respaldo me ayuda alcanzar mis objetivos y metas. A mi hija por ser el motor por la motivación constante a seguir adelante, pero más que nada, por su amor y comprensión por haberme apoyado en todo momento.

Joselin Ivania Vásquez de Guillen

INDICE

Contenido

ÍNDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN EJECUTIVO

Actualmente en El Salvador debido a la situación que se vive con respecto a la emergencia de COVID-19, un gran número de empresas del sector industria han puesto en práctica la modalidad teletrabajo como una opción inmediata o alternativa ante la situación que se ha generado.

Por tanto el profesional de la contaduría pública se ha visto afectado para trabajar en esta modalidad, debido a que algunas de las empresas no cuentan con las medidas adecuadas para establecer mecanismos de seguridad en la información para el control de sus actividades; no obstante, pueden contar con diversas formas para que la información sea transmitida con conexión vía remota, pero es importante contar con medidas, políticas y controles necesarios para la transmisión de información financiera valiosa de la entidad.

Dado lo anterior, surge este proyecto de investigación mediante el cual es un sistema de gestión en la seguridad de la información con enfoque en modalidad de teletrabajo para que la organización pueda mitigar los riesgos y dar respuesta de manera oportuna a los incidentes informáticos.

Para ello se tomará como base las buenas prácticas planteadas en la norma ISO 27032 con el fin de generar una guía que brinde a los encargados de TI, los lineamientos para identificar los riesgos a los cuales están expuestos de acuerdo a la información que tienen publicada en el ciberespacio y que puede llegar a afectar el objetivo del negocio, generando los controles

necesarios a implementar de tal forma que aseguren de manera óptima los diferentes activos de información.

La investigación posee un enfoque cualitativo, el cual requiere un proceso apropiado para el estudio de la problemática, basando la investigación inicialmente en la observación de la problemática que permite establecer hipótesis que expliquen cómo se originó el problema, sus consecuencias, al igual que verificar y comprobar la falta de una guía de gestión, la cual podrá deducir causas y medir sus efectos.

De acuerdo a los resultados de la investigación se ha concluido que la empresa tiene la necesidad de implementar un sistema de gestión ya que es vulnerable ante las amenazas y riesgos de ciberataques.

INTRODUCCIÓN

La seguridad informática busca garantizar la disponibilidad, integridad y confiabilidad de la información financiera que se gestiona a través de medios tecnológicos, permitiendo un crecimiento en las organizaciones, fomentando la innovación y ventajas competitivas en el mercado que se desempeñan.

Sin embargo, es importante tener claro que no existen mecanismos, controles o herramientas que permitan tener la seguridad de la información en un cien por ciento, garantizando la continuidad de los servicios y/o las operaciones críticas de las organizaciones. La investigación se desarrolla en 3 capítulos los cuales se dividen en:

El capítulo I se desarrolló un marco teórico, conceptual, técnico y legal en el cual se muestran las principales definiciones para la comprensión de la *ciberseguridad*, sus generalidades y la importancia que esta posee. Adicionalmente a eso el marco teórico incluye normas, leyes que regulan el uso y manejo de la *ciberseguridad*.

En el capítulo II se describe la metodología que se implementa durante la investigación y para la obtención de los resultados fueron necesarias incluir el enfoque y tipo de investigación, delimitar el espacio; adicionalmente definir técnicas e instrumentos para el proceso de análisis de la información y posteriormente la presentación de los resultados.

En el capítulo III se ha desarrollado la propuesta que consiste en un sistema de gestión de *seguridad de la información* basado en la norma ISO 27032 con enfoque en modalidad de teletrabajo para el profesional de contaduría pública en una empresa industrial en el municipio de Soyapango.

Finalmente, como parte fundamental y necesaria, se presentan las conclusiones y recomendaciones derivadas de las unidades de análisis, objeto de estudio, así como los anexos a utilizar.

CAPÍTULO I MARCO TEÓRICO

SITUACIÓN PROBLEMÁTICA

En el país muchas de las empresas y sectores más importantes de El Salvador utilizan y han utilizado diversas herramientas de las tecnologías de la información en sus labores diarias, la evolución de las tecnologías de la información (TIC) marca un momento crucial y decisivo en la sociedad mundial, pues ha contribuido de gran manera en el desarrollo de la misma.

Debido al auge y expansión tecnológica las empresas han dirigido esfuerzos para el desarrollo de software que permitan sistematizar procesos, y que permitan la conexión desde cualquier lugar del país, dichos sistemas ayudarían al profesional de contaduría pública a realizar sus funciones en la modalidad de teletrabajo.

El uso de las conexiones remotas puede llegar a ser un aliado para las empresas en la actualidad, ya que para el año 2020 las empresas se han visto afectadas por la pandemia del coronavirus (COVID-19); las empresas salvadoreñas se han visto en la obligación de suspender sus actividades laborales y posteriormente a restablecerlas gradualmente, lo cual afecta la economía no solo de las empresas, sino que también la economía del país, y es por esto que muchas de las empresas tienen que adaptarse y trabajar en la modalidad de teletrabajo; muchos profesionales de la contaduría pública están realizando sus labores mediante sistemas o software,

lo cual puede llegar a ser un problema para las pequeñas o medianas entidades, ya que no todas cuentan con los recursos suficientes para implementarlo.

1.1 *CIBERSEGURIDAD*

1.1.1 Antecedentes

El mundo poco a poco se va volviendo cada vez más digital, por lo que las empresas deben de hacer uso de las herramientas de información y comunicación para desarrollar sus actividades; por lo tanto, el profesional en contaduría pública se debe adaptar a los nuevos cambios y al nuevo entorno laboral de las comunicaciones digitales en El Salvador.

Los objetivos de la seguridad han ido evolucionando con el paso de los años, la evolución de la seguridad en las empresas no ha quedado atrás y ha experimentado un cambio sustancial desde sus inicios, principalmente motivado por los avances tecnológicos, aplicaciones, datos almacenados y, por tanto, aumenta el riesgo de seguridad debido a que la información es muy valiosa para los ciberdelincuentes.

En los años 2000 los ciberdelincuentes explotaban vulnerabilidades informáticas de sistemas operativos, hardware y otras aplicaciones, también tuvo una gran relevancia la adopción masiva del email y las posibilidades de ingeniería social que ofrecía. Se combinaron firewalls y antivirus para proteger los sistemas de los ciberataques, asentando la base de las infraestructuras de seguridad empresariales. Pero la protección proporcionada comenzó a caer frente a la velocidad a la que los ataques evolucionan en sofisticación e impacto.

En la década del 2010, los ciberataques alcanzaron niveles de sofisticación sin precedentes. Los criminales se unieron en organizaciones profesionales y empezaron a desarrollar malware de día cero. Los ciberataques se volvieron sigilosos y difíciles de identificar, los virus podrían estar ocultos en todos los sitios, desde documentos adjuntos, información comercial falsa hasta archivos de imagen.

Ante esta situación, se desarrollaron soluciones de seguridad avanzada con tecnología de prevención de amenazas para bloquearlas antes de que pudieran actuar.

> "El riesgo tecnológico tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Su incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad." (Castro, 2011)

En la actualidad la tecnología informática es primordial para el desarrollo de toda empresa, la información que una organización maneja se debe considerar como un activo que es muy importante para la misma, que puede ser causante incluso de la quiebra de una institución si no es utilizada y respaldada de una manera técnica que permite la integridad de sus datos. Caso sobre un ciberataque en los últimos años. (Consultoría para la implementación de un marco de *ciberseguridad* ISO/IEC 27032, 2018)

Muchas de las empresas en nuestro país utilizan aplicaciones que les facilitan la comunicación, y no tanto por el hecho de estar en diferentes lugares, sino que es más bien por la facilidad de comunicación y desarrollo de las diferentes actividades de las empresas.

Con lo anterior surge la problemática que se vuelve más relevante para las entidades, y es que en un mundo globalizado que cambia constantemente con respecto a las TIC, la tecnología de las comunicaciones trae consigo riesgos, amenazas y vulnerabilidades, lo que obliga a las entidades a conocer un marco normativo y legal que permita el control, seguridad y reconocimiento de las mismas.

En el país muchas de las empresas y sectores más importantes utilizan diversas herramientas de las tecnologías de la información en sus labores diarias, la evolución de estas, marca un momento crucial y decisivo en la sociedad mundial, pues ha contribuido de gran manera en el desarrollo de la misma.

Ahora que muchas personas están en modalidad de teletrabajo es importante proteger los dispositivos y equipos que se utilicen para acceder, ya que hasta cierto punto se encuentran vulnerables ante los riesgos cibernéticos y pueden ser punto fácil de extracción de la información financiera, implementación de virus, phishing, malware, entre otros.

1.1.2 Importancia de la ciberseguridad.

Tener canales online y utilizar las redes sociales es una necesidad para cualquier empresa. Pero esto implica que activos muy importantes como la continuidad del negocio, los datos de los clientes y de los empleados estén expuestos a nuevos riesgos. Un error de programación, un defecto en un software de terceros etc. son suficientes para abrir la puerta a fugas de millones de registros.

Las amenazas a la seguridad de los sistemas digitales se encuentran a través de programas maliciosos, malware, programas espía, spyware, virus informáticos, gusanos o troyanos que pueden acceder a las cuentas de correo o a las estructuras informáticas de la empresa, estos llegan a través de sistemas mal programados y ser utilizados por los hackers para acceder a los sistemas, en teoría, blindados de una entidad.

Estos sistemas mal diseñados pueden facilitar puertas de entrada a elementos digitales no deseados. Podemos encontrar también diferentes formas de entrada de estos intrusos a través de los problemas de acceso que puedan generar los propios usuarios del sistema con sus descuidos en el momento de iniciar sesión, con contraseñas visibles, etc.

Los profesionales de la contaduría pública en la manera de lo posible deben evitar utilizar los servicios públicos de Wifi para acceder o intercambiar información confidencial. Los hackers pueden acceder fácilmente a flujos de datos públicos e interceptar datos intercambiados en formato de texto plano. Si se plantea utilizar un ordenador público, invierta en software VPN para un cifrado de extremo a extremo o asegúrese de que todos los datos intercambiados permanezcan

dentro del almacén cifrado. Por ende, es de vital importancia que las empresas inviertan en *ciberseguridad* para proteger sus negocios de las amenazas cibernéticas.

Así mismo generar confianza a sus clientes a través de la implementación de los mecanismos de transferencia segura de información y validación de usuarios. Esto busca que las empresas entiendan la importancia de la reputación digital, sobre todo si se tiene o se recibe información privada de clientes.

1.1.3 Implementación de *Ciberseguridad*

La *Ciberseguridad* ha pasado de ser un elemento complementario a una necesidad crítica para todas las empresas en su proceso de transformación digital. Hoy en día, las amenazas a la *ciberseguridad* son un problema mundial, vemos amenazas que aumentan a un ritmo alarmante, tanto en cantidad como en sofisticación.

La ciberseguridad es un tema del cual tenemos que ocuparnos de manera prioritaria. Por la cual la naturaleza de la relación de la ciberseguridad con otros focos de trabajo son los siguientes:

Figura 1 ***Focos de Trabajo***

Fuente: (Implementacion de un Marco de *Ciberseguridad*, 2019)

Para el profesional de contaduría pública los sistemas informáticos están abarrotados de información importante que los hackers quieren obtener, por tanto, es necesario protegerse ante los peligros de la era actual implica llevar a cabo procesos de *ciberseguridad* que se sustenten sobre su efectividad y para hacerlo, es necesario conocer las cuatro fases en la que se desarrolla.

Figura 2: ***Fases de la Implementación de la Ciberseguridad***

Fuente: (Implementación de un Marco de *Ciberseguridad* ISO 27032, 2019)

- Fase I: Entendimiento de la Organización

En esta fase se realiza un trabajo importante de inmersión en los procesos de la empresa para conocer el funcionamiento de éstos y que usó realizan del ciberespacio y sus servicios.

- Fase II: Análisis de Riesgos

La toma de decisiones en cuanto a los controles y medidas de seguridad que se van a implementar debe estar basada en la gestión de los riesgos y el alineamiento con las necesidades de la empresa.

- Fase III: Plan de Acción

Este plan afrontará diferentes estrategias que incluirán y deberán aplicarse a diferentes niveles de la organización.

- Fase IV: Implementación

Esta fase del proyecto se focalizará entonces en la implementación de controles que deberán tener en cuenta el nivel de madurez en la gestión de la seguridad existente

1.2 SEGURIDAD DE LA INFORMACIÓN

La tecnología informática es primordial para el desarrollo de toda empresa, la información financiera que una organización maneja se debe considerar como un activo que es muy importante para la misma, que puede ser causante incluso de la quiebra de una institución si no es utilizada y respaldada de una manera técnica que permite la integridad de sus datos.

¿Qué es la seguridad de la información?

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos. (Seguridad de la Información, 2020)

> "Las políticas de seguridad de la información son un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo adecuado de todos los activos de una empresa,

teniendo el propósito de proteger la información, los recursos y la reputación de la misma." (Politicas de seguridad informática, 2019)

Los avances tecnológicos brindan a las empresas del sector industrial mayores herramientas para el desarrollo de negocios, un ejemplo son los sistemas ERP que integra diferentes módulos y los cuales interactúan entre sí como planillas, contabilidad, operaciones, inventarios, facturación, es necesario recalcar que cada uno de ellos administra datos y genera información importante para la organización a tal grado que con la misma se mejora el criterio de la toma de decisiones, indicadores que se utilizan para el monitoreo de los resultados.

> "Cada 30 de noviembre se conmemora el día internacional de la seguridad informática, un día donde el objetivo es buscar crear conciencia sobre la importancia que tiene la seguridad de la información en tu empresa", este evento se empezó a celebrar en 1988 en Estados Unidos, bajo el nombre de Computer Security Day, como iniciativa de la Association for Computing Machinery (ACM), y de ahí se extendió a otros países.

La seguridad informática es el área de la información enfocada en la protección de la infraestructura computacional y todo lo relacionado con esta, incluyendo la información contenida. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

A la hora de hablar de seguridad de la información, siempre suele hablarse de tecnologías, pero, en realidad, los auténticos protagonistas de la seguridad en las empresas son los empleados, que son los que utilizan los dispositivos tecnológicos para gestionar el principal activo de la

organización: la información. Es fundamental fomentar el desarrollo de una cultura de seguridad en la empresa formando y concienciando al personal en *ciberseguridad*, teniendo siempre presente las políticas, normativas y procedimientos de seguridad establecidas; supervisando que se cumplen las buenas prácticas en seguridad definidas; y realizando acciones de sensibilización y concienciación en seguridad de manera continua.

Seguridad de la información, Seguridad informática y *Ciberseguridad*. Diferencias:

Sí, existe cierto grado de confusión actualmente en torno a los términos seguridad de la información, seguridad informática y *Ciberseguridad.*

El concepto de *seguridad de la información* no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. Se puede definir que la seguridad de la información es el mecanismo que se aplica en cualquier empresa u organización para brindar protección a la información o datos tanto de manera física como digital.

La seguridad de la información es el paraguas que cubre a las otras dos disciplinas. No se quiere decir que con eso sea más importante, pero sí más amplia. Comprende todos los aspectos que pueden afectar a la seguridad de la información de empresas y organizaciones, desde la selección de un candidato en proceso de selección, hasta la continuidad de negocio, pasando por la seguridad física y lógica (parte de la seguridad informática), y muchas más áreas.

> "La seguridad de la información es la disciplina que se encarga de proporcionar la evaluación de riesgos y amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, bajo la normativa o las buenas prácticas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de la información de activos." (Excellence, 2020)

> "Por otro lado, *la seguridad informática* es el conjunto de métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital que estos almacenan; dentro de esta categoría, se puede mencionar la seguridad computacional, la cual se ciñe a la protección de los sistemas y equipos para el procesamiento de datos de una empresa." (Diferencias entre seguridad informática y SI , 2020)

El ámbito de la seguridad informática debe contemplar las redes de comunicación y los elementos que la conforman, además de los equipos informáticos que se encuentran conectados a ellas o interconectados entre sí.

Y tenemos *la ciberseguridad* que se menciona anteriormente que se encarga exclusivamente, de brindar una protección a la información digital, la que se encuentra en los sistemas interconectados.

1.2.1 La seguridad de la información en la actualidad

Hoy en día, existen muchas amenazas conocidas como malware (cookies, gusanos, virus, troyanos, etc.) que ponen en riesgo la privacidad del usuario y el funcionamiento de nuestros ordenadores y redes. Con la creciente ciberdelincuencia, personas y empresas se esfuerzan en

asegurar sus sistemas y redes para luchar contra malwares y otros problemas graves que afectan la Seguridad Informática. Nos encontramos ante un escenario en el que las amenazas y los ciberataques no dejan de crecer de un año a otro:

- De 2015 a 2016, el número total de incidentes de seguridad aumentó un 91%.
- Se estima que se producen 309.854 ataques diarios.
- En 2016 se detectaron 113.1 millones de incidentes de seguridad.

Según el ministro Margallo, España es el tercer país del mundo que más ataques cibernéticos recibe". (La importancia de la seguridad informática en tu empresa, 2019)

> "Con el uso de las herramientas tecnológicas y la implementación de otras alternativas o formas de laborar como el trabajo desde casa o fuera de las instalaciones de la organización, se vuelve necesario implementar políticas que permitan resguardar la información así como mantenerla disponible y de fácil acceso a los usuarios correctos; el robo de información de clientes, proveedores, empleados, rutas de tránsito, precios, costos y otra información empresarial, ha causado que las empresas carezcan de credibilidad y rentabilidad en el sector industrial según el Organismo Salvadoreño de Normalización (OSN)". (Politicas de seguridad informática, 2019)

Como se menciona anteriormente el desarrollo de las nuevas tecnologías posibilita la obtención de mucha información, que en la mayoría de organizaciones no es considerada como un activo importante, en El Salvador, hay cierto reconocimiento para algunos bienes intangibles como

la propiedad intelectual, marcas y logos de las empresas; pero no se le toma mucha importancia a bienes considerados información como: base de datos de clientes, conocimiento comercial, documentos legales; contratos en los que se establece términos de negociación que en las manos incorrectas pueden derivar en repercusiones negativas.

En El Salvador, las organizaciones y sus sistemas de información financiera están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos. (Normalización, 2019)

1.2.2 Beneficios de la seguridad de la Información.

(5 Beneficios de implementar un sistema de gestión de seguridad de la información, 2019)

- Definir legalidades para obtener la seguridad de la información.
- Ayuda a tener un programa o sistema de identificación para reconocer la información que se va a proteger, es decir las revisiones que se hacen diariamente para así poder tener actualizado lo más posible los datos que sean requeridos, tener un control de lo que está respaldado.

- ❑ Cumplimiento de los aspectos relacionados con la información, como es la protección o seguridad de los datos, la privacidad o el control de la tecnología de la información.
- ❑ Disponer de un sistema de gestión de seguridad de la información conforme a las normas ISO 27000 es una llave de oro que abre nuevos mercados y clientes.
- ❑ Disminución de los gastos por incidentes de violación en la seguridad, los beneficios no se aprecian en forma de ganancia económica evidente.

Las empresas tienen mayor dependencia a los sistemas de información, por ende, tienen mayor vulnerabilidad a las amenazas concernientes a la seguridad integral, además a consecuencia de la interconexión entre empresas por medio del internet, también existe el riesgo de pérdida de información o incluso robo de la misma.

Es por ello que las empresas deben tener en cuenta el tema de la seguridad de la información muy en serio, ya que hoy en día independientemente de la pandemia, el uso del ciberespacio es casi necesario para las labores diarias.

1.3 TELETRABAJO

1.3.1 Reseña Histórica del teletrabajo

La Comunidad Europea generó en 2002 un marco de acuerdo para regular el trabajo a distancia, estableciendo su carácter voluntario y garantizando los derechos al igual que cualquier otro trabajador. Se establece además la responsabilidad del empleador de contar con normas y herramientas de protección de datos.

La Agencia Europea para la Seguridad y la Salud en el Trabajo comprende que los riesgos que surgen en relación al proceso de digitalización de la economía son diferentes. En un estudio que se está realizando sobre los desafíos a la seguridad y salud del teletrabajador, se destaca el riesgo a la hiperconectividad y sus consecuencias en el establecimiento de límites entre lo laboral y la vida privada, lo que incrementa el estrés y trastornos del sueño. También se observa un aumento de los riesgos ergonómicos vinculados al uso de las TIC, junto con una sobrecarga cognitiva.

En Chile entra en vigencia el 1 de abril de 2020 la modificación al código del trabajo en materia de trabajo a distancia. Esto es evidentemente una reacción a la situación provocada por la actual pandemia, y no consecuencia de una comprensión de los desafíos laborales propios de una sociedad digital. Tampoco corresponde a una estrategia nacional de desarrollo económico a la luz de los desafíos de la 4ª revolución industrial.

Concretamente, esta nueva reforma establece el derecho a desconexión, lo que significa que el empleado tiene 12 horas al día en las cuales no está obligado a responder consultas o requerimientos. El empleador también debe proporcionar todos los equipos, herramientas y materiales para el teletrabajo, (Teletrabajo: una historia llena de desafíos, 2020)

En América Latina no hay cifras ni datos estadísticos que nos permitan hablar de cantidad de teletrabajadores y recursos disponibles. Sin embargo, es sabido que ya existen numerosos casos de teletrabajadores por cuenta propia y numerosas experiencias desarrolladas en empresas, sobre todo multinacionales que aplican teletrabajo como política. Podemos citar casos como la petroquímica Dow, Laboratorios Roche, IBM o la alemana Siemens, entre otras.

Durante la crisis sanitaria que abate al mundo entero, se escucha más frecuentemente el término teletrabajo, como medio alterno para que los empleados continúen desempeñando sus labores desde sus residencias ante las restricciones gubernamentales para prevenir el contagio del virus COVID-19.

Si bien El Salvador desde hace mucho tiempo algunas empresas habían optado por la singularidad del teletrabajo en ciertas áreas de sus negocios, lo hacían bajo el principio de la autonomía de la voluntad de las partes.

Encaminados a regular e implementar la modalidad del Teletrabajo en El Salvador, el 20 de marzo de 2020 y durante la emergencia nacional por la pandemia del Covid-19, la Asamblea Legislativa aprobó el Decreto No. 600, que contiene la Ley de Regulación del Teletrabajo; la cual es aplicable en el sector Privado, en el sector Público, y en las Autónomas; en dicha normativa se establecen las condiciones bajo las cuales se ejecutará el teletrabajo, en concordancia con lo regulado en Código de Trabajo y demás leyes de carácter laboral.

1.3.2 Ventajas y desventajas del teletrabajo.

Las ventajas son múltiples, tanto para el trabajador como la empresa o institución, y la economía del país. El Teletrabajo implica trabajar remotamente, no necesariamente todos los días, pero sí con cierta frecuencia.

La experiencia de más de 10 años, en otras latitudes, enseña que la recuperación del tiempo (y costo) del desplazamiento periódico, aumenta la motivación y la productividad del trabajador.

El estrés que causa el traslado diario de los trabajadores a sus centros de trabajo es considerable. La liberación de ese estrés mejora inmediatamente la actitud del trabajador, al sumarle el tiempo y el costo ahorrado, tenemos como resultado un considerable aumento en la productividad.

Para el patrono, el Teletrabajo trae, además del aumento en la productividad de los trabajadores, un ahorro importante del espacio de oficina requerido, esto se traduce de inmediato en una reducción de gastos operativos. Sin embargo, es más importante el cambio de mentalidad a que el Teletrabajo obliga. Cuando se trabaja bajo modalidad remota varios días por semana, pierde sentido el control de asistencia y cobra vigencia el control de la producción. Los procesos de control de la producción por trabajador, a su vez, promueven esquemas de compensación variable basados en productividad, los cuales ayudan a aumentar todavía más la productividad del trabajador y las utilidades de la empresa (o excedentes de la institución).

Ventajas para el trabajador

- Mayor autonomía y movilidad
- Aumento de la productividad
- Más oportunidades laborales
- Mayor especialización
- Más vida familiar, entre otros.

Ventajas para le empresa

- Menos problemas de convivencia entre empleados
- Mayor productividad debido a la implantación del trabajo por objetivos
- Menor coste por producción

- Menor infraestructura necesaria
- Más acceso a profesionales de alto nivel
- Eliminación de control horario, entre otros.

Figura 3: Beneficios del Teletrabajo

Fuente: (Webinar sobre Teletrabajo en la actualidad, 2020)

La economía de los países que utilizan el Teletrabajo causa un impacto en el consumo de combustible, que a su vez reduce el deterioro de las calles y mejora la calidad del aire y por ende la salud de los ciudadanos. Según las estadísticas de Costa Rica, si todos los que trabajan en oficinas dejaran de viajar tres veces por semana, el consumo nacional de petróleo se reduciría en un 10%; eso es como $130 millones al año (y aumenta con el precio del petróleo).

Obviamente, esto no se logra de la noche a la mañana; hay que invertir en infraestructura digital, una inversión altamente rentable, incluso si agregamos inversiones inmobiliarias, que pueden ser necesarias para implementar el Teletrabajo, debido a que muchos trabajadores no disponen en sus hogares de las condiciones necesarias.

Desventajas del teletrabajo

Ya no sorprende que cada vez sean más las empresas, pequeñas y grandes, que permiten a sus plantillas teletrabajar, debido a las facilidades que se obtiene del internet y el mundo cibernético. Muchas de estas han empezado a mejorar sus procesos, sus herramientas, etc. La tecnología interpuso una nueva forma de conectar a los empleados con la entidad de forma virtual, debido a esto, se pueden presentar ciertas situaciones negativas al utilizar esta modalidad tanto para el trabajador como el empleador entre las que podemos mencionar:

- **Posible desvinculación emocional del trabajador con la compañía:** Una de las consecuencias que se pueden dar a medio y largo plazo es que el trabajador pierda la vinculación con la compañía. El hecho de no reunirse con los compañeros y no compartir un espacio común, hace que el trabajador pierda nexo, unión y referencia emocional con la compañía.

- **Se elimina el ambiente laboral**: Si todos los empleados van a teletrabajar, el ambiente laboral ya no es que se reduzca, sino que se elimina totalmente.

- **Dificultad para controlar al empleado**: Cada vez más, el trabajo se mide por objetivos y resultados en lugar del número de horas que laboran de forma presencial, pero a día de hoy todavía hay empleos que no se pueden cuantificar de esta manera, como pueden ser los de atención al cliente.

- **Dificultad para el trabajo en equipo**: Cada vez son más las tareas y los trabajos que precisan de reuniones colaborativas entre sus trabajadores. Teletrabajar provoca que los empleados tengan mayores dificultades a la hora de reunirse si no existe un lugar físico en el que hacerlo. Puede hacerse de forma virtual, con videollamadas, pero no siempre es posible, ni los resultados son iguales.

- **Cambio en la cultura y organización de la empresa:** La compañía tendrá que dar un pequeño giro a su filosofía. La organización y la forma de gestionarla podría cambiar y debe estar preparada para ello.

- **Aislamiento**: La falta de ese ambiente de trabajo y de la relación con otros compañeros puede provocar que el trabajador termine considerándose excluido y sintiéndose demasiado solo. El contacto humano sigue resultando fundamental.

- **Descenso de la productividad**: No es fácil ni sencillo generar un ambiente de trabajo en tu propia casa, ni todos son capaces de inspirarse en centros coworking. Como resultado el rendimiento del trabajador puede verse afectado.

- **Reducción del aprendizaje**: En cierta manera, el aprendizaje puede reducirse, ya que el empleado puede terminar realizando tareas mecánicas y rutinarias, o únicamente funciones de su entorno. El aprendizaje grupal y colaborativo, tanto profesional como personal, ya no tiene cabida.

- **Pérdida de la confidencialidad**: Es uno de los grandes problemas y retos de las empresas actualmente. Los ciberataques continúan siendo uno de los grandes riesgos a los que se tienen que enfrentar las entidades. Muchos trabajos y algunas de las funciones que realizan los empleados, gestionadas desde fuera de la oficina, pueden poner en riesgo la confidencialidad de esta.

1.3.3 Definición de teletrabajo

El teletrabajo es una modalidad de empleo en la que se puede trabajar desde un lugar diferente al de la oficina, durante una parte importante del horario laboral. Sin embargo, a diferencia del trabajo remoto como empleado no se puede elegir el lugar donde se va a trabajar: es la propia empresa la que debe decidir cuál será el lugar habitual de trabajo, basándose en los términos del contrato.

¿Cómo funciona el teletrabajo?

Para que un profesional realice su actividad en modo teletrabajo, tan solo es necesario que la empresa incorpore a su método interno facilidades para desarrollar el empleo a distancia como una intranet bien definida, herramientas para trabajar desde casa, canales de comunicación vía email o videollamada, y facilidad para realizar reuniones a distancia.

El trabajo se efectuará con total normalidad, pero sin necesidad de que el profesional tenga que desplazarse todos los días a su puesto de trabajo, manteniendo la comunicación entre empresa y empleado.

1.3.4 Implementación del Teletrabajo en la empresa

Independientemente del tipo de teletrabajo que quiera implementar tu empresa, estos son los pasos básicos que debe llevar a cabo para que la experiencia sea lo más productiva y conciliadora posible:

- Para empezar, la compañía debe definir unos objetivos observables y medibles para todos y cada uno de los trabajadores. Por las características del trabajo, es posible que no todos los departamentos de la empresa puedan teletrabajar, y por eso es tan importante que el empresario estudie si el teletrabajo es viable antes de implantar cualquier modelo.
- Una vez definido este punto, el empresario deberá escoger los canales de comunicación más adecuados para comunicarse con los trabajadores (Slack, Skype, Trello, Asana…) y delimitar el número de reuniones o videollamadas que son necesarias al día o a la semana.
- Para poder ser productivos desde el primer día de teletrabajo tendrán que recibir la formación pertinente para saber manejar las nuevas herramientas del teletrabajo. Si trabajando desde casa utilizan los mismos programas o softwares que emplean durante los días de oficina no será necesaria la formación, pero si los métodos cambian tendrán que recibir alguna inducción pertinente.

- El empleado debe contar con el hardware y software necesarios para el desempeño de su trabajo desde casa, así como las medidas de seguridad pertinentes. La empresa deberá hacerse cargo de todas estas medidas antes de que comience el periodo de teletrabajo.
- El jefe inmediato debe de realizar un seguimiento periódico de las tareas y objetivos; lo anterior es necesario para determinar que el teletrabajo se está desarrollando de manera exitosa y oportuna.
- Teletrabajo y Protección de Datos. En la gran mayoría de las empresas se ha implementado una política de Protección de Datos para salvaguardar la información personal, de los usuarios, clientes y proveedores.
- Empresas para teletrabajar. Al día de hoy muchas empresas ofrecen la posibilidad de teletrabajar uno o más días a la semana, algunas compañías llevan tiempo apostando por la flexibilidad de horarios y la conciliación laboral de su plantilla.

Por la situación que presenta el país por el COVID-19 la implementación del teletrabajo ha sido de vital importancia para las empresas, el profesional de contaduría pública se ha tenido que acoplar a esta nueva modalidad ya que el trabajo que desempeña en su gran mayoría es presencial.

1.4 NORMATIVA TÉCNICA Y LEGAL

1.4.1 Normativa Técnica

El crecimiento de nuevas tecnologías aplicadas ha ido ganando cuerpo en los últimos años, esto ha permitido que las normas ISO para los sistemas de gestión hayan adquirido en las empresas papeles más importantes.

La organización internacional de estandarización (ISO) ayuda a las empresas a aplicar eficazmente las nuevas tecnologías además de gestionar de una mejor manera más conveniente los recursos. (Las normas ISO & Importancia y Beneficios , 2016)

Se tomará como referencia la normativa creada en el año de 2012 conformada por el comité técnico "ISO/IEC JTC1/SC 27 Seguridad de la información, *Ciberseguridad* y protección de la privacidad", atendiendo al reto de las nuevas amenazas por los huecos o espacios no cubiertos por normas anteriores. (Organizacion Internacional de Normalizacion, 2019)

Sistema de gestión de seguridad de la Información ISO 27001

Es una norma emitida por la organización internacional de normalización, el cual describe cómo gestionar la (Asamblea Legislativa, Decreto Legislativo No 611, 2005) seguridad de la información de una empresa. El objetivo principal de esta ISO es proteger la confidencialidad, integridad y disponibilidad de la información. (Normas ISO)

Esta norma puede ser implementada en cualquier tipo de entidad privada o pública, pequeña o grande. También permite la certificación de la empresa, eso significa que la empresa certificada confirma que la seguridad de la información da cumplimiento a esta norma.

Tratamiento del riesgo aplicando ISO 27001

La evaluación de riesgos es probablemente la parte más complicada de la implementación de esta norma, pero al mismo tiempo es la etapa más importante al iniciar el proyecto de la

seguridad de la información, esta incluye un conjunto de actividades coordinadas para dirigir y controlar una estrategia en relación al riesgo de una empresa, incluye por lo general: evaluación de riesgos, tratamiento de riesgos, aceptación y comunicación de riesgos. (ISO TOOLS, 2017)

Buenas prácticas para gestión de la seguridad de la información ISO 27002

Esta norma describe cómo se pueden establecer los controles, los cuales se deben de elegir por medio de una evaluación de riesgo de los niveles de activos más importantes de la empresa, esta sirve de apoyo para la implementación del sistema de gestión de seguridad de información.

La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. (OSTEC, 2016)

El acceso a la información, así como a los recursos de procesamiento deben de ser controlados, se tiene que ser prevenidos los accesos no autorizados a los sistemas de información, afín de evitar daños a documentos y recursos de información que estén al alcance del personal.

Gestión de la *Ciberseguridad* ISO 27032

Esta norma pretende garantizar la seguridad en los intercambios en la red para lograr hacerle frente de una manera más efectiva al cibercrimen con más cooperación entre todos, está orientada a garantizar un entorno seguro a través de directrices de seguridad como se puede

mencionar: La seguridad de la información (activos más importantes), seguridad en redes, seguridad de internet y la protección de la infraestructura crítica de la información. (Maria Camilo Arevalo, 2019)

La norma (ISO/IEC 27032) facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo. De esta manera, puede ayudar a preparar, detectar, monitorizar y responder a los ataques. La organización espera que ISO/IEC 27032 permita luchar contra ataques de ingeniería social, hackers, malware, spyware y otros tipos de software no deseado.

Como se observa, el ISO 27032 aporta un marco metodológico y de buenas prácticas en la implementación de la *Ciberseguridad* en las empresas, complementando al ISO 27001 en el aporte de nuevos controles relacionados al Ciberespacio. (Deloitte, 2019)

La ISO 27032 ayuda a la implementación de los controles en varias áreas dentro de la entidad; ejemplo de esto el personal debe de capacitarse y realizar campañas de seguridad para una constante actualización de conocimiento. Así mismo las aplicaciones deben de tener niveles de accesos y validaciones, sesiones, políticas y autenticación de los accesos del personal a las redes, sistemas dentro de la entidad (Maria Camilo Arevalo, 2019)

Manual de Buenas Prácticas en el Teletrabajo de la OIT año 2011

Extracto de El Salvador (Teletrabajo: una historia llena de desafíos, 2020)

1.4.2 Normativa Legal

Ley de Regulación del Teletrabajo

Art. 1.- La presente ley tiene como objeto promover, armonizar, regular e implementar el teletrabajo como un instrumento para la generación de empleo y modernización de las instituciones públicas, privadas y autónomas, a través de la utilización de tecnologías de la información y comunicación.

Art. 3.- Para efectos de la presente ley se entenderá por teletrabajo una forma de desempeñar la relación de trabajo de carácter no presencial, total o parcialmente, por tiempo determinado o de manera indefinida, fuera del centro de trabajo y utilizando como soporte las tecnologías de la información y la comunicación:

Tecnologías de la información y comunicación (TIC's):

Es el conjunto de servicios, infraestructura, redes, software, aplicaciones informáticas y dispositivos que tienen como propósito, facilitar la prestación de los servicios en las instituciones y empresas, procurando la satisfacción de los usuarios y clientes. Así como las tecnologías que se necesitan para la gestión y transformación de la información, en particular los componentes tecnológicos que permiten crear, modificar, almacenar, proteger y recuperar esa información.

Ley especial contra los delitos informáticos y conexos

Art. 1.- La presente Ley tiene por 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

Acceso Indebido a Sistemas Informáticos

Art. 4.- El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, será sancionado con prisión de uno a cuatro años.

Interferencia del Sistema Informático

Art. 6.- El que intencionalmente y por cualquier medio interfiera o altere el funcionamiento de un sistema informático, de forma temporal o permanente, será sancionado con prisión de tres a cinco años.

Se considerará agravada la interferencia o alteración, si ésta recayera en programas o sistemas informáticos públicos o en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión y transporte de energía, de medios de transporte u otros de servicio público, o destinados a la prestación de servicios financieros, la sanción de prisión será de tres a seis años.

Violación de la Seguridad del Sistema

Art. 9.- La persona que sin poseer la autorización correspondiente transgrede la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, será sancionado 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 Reguladora del Ejercicio de la Contaduría

Con respecto a la Ley Reguladora del Ejercicio de la Contaduría Publica el profesional contable tiene la responsabilidad de cumplir con todas las obligaciones en ella contenida, él no debe eludir ninguna responsabilidad a la vez de concientizarse que en la medida que vaya cumpliendo cada una de estas estará garantizando el ejercicio legal de la profesión.

El contador público debe asegurarse por todos los medios posibles que desarrollara su profesión cumplimiento totalmente con las obligaciones emanadas de esta Ley, también no debe soslayar la responsabilidad de abstenerse de ejecutar todos aquellos actos que la contraríen. La responsabilidad legal del contador público frente a la presente Ley debe representar el mecanismo que impulsará el desarrollo de la contaduría pública en el nuevo contexto socioeconómico, puesto

que existe una obligación por parte de aquel de asumir esa responsabilidad y en la medida en que él ejerza la profesión tal y como la ley lo estipula estará gozando de un reconocimiento público entre todos los sectores de la sociedad que magnificará su rol. (Asamblea legislativa de El Salvador , 2017).

1.5 PRINCIPALES DEFINICIONES

Las siguientes definiciones fueron tomadas de los libros: seguridad en equipos informáticos y (Gómez Vietes, 2013) como implantar un SGSI. (Gómez, 2018). Estos conceptos se utilizarán en el desarrollo de la investigación ya que son términos importantes en el área tecnológica y vital para que la parte financiera comprenda y se relacione con el lenguaje aplicado.

- ✓ **Activo de información:** Componente que sustenta uno o más procesos de negocio de una entidad y genera alto valor a la entidad. Los activos de información pueden ser de diversos tipos, entre ellos: datos o información, servicios (procesos), programas informáticos, dispositivos físicos, redes de comunicación, soportes de información, equipamiento auxiliar e instalaciones físicas e intangibles (marcas).
- ✓ **Autenticación:** Es la situación en la cual se puede verificar que un documento pertenece a quién el documento dice. Aplicada a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aplicar algún modo de que se pueda verificar que dicha persona es quien dice ser.
- ✓ **Ciber-amenaza o amenaza cibernética:** Potencial ocurrencia de una situación que pudiera convertirse en un ciberataque.

- ✓ **Ciberataque o ataque cibernético:** Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de la materialización de un crimen y mediante la cual, dichos agentes comprometen la seguridad de la información de la entidad.
- ✓ **Ciberespacio:** Entorno complejo resultante de la interacción de personas, software y servicios en internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.
- ✓ **Computación en la nube:** Modelo informático que permite obtener, desde cualquier lugar y bajo demanda, acceso a través de una red a un conjunto compartido de recursos informáticos configurables, el cual se puede conformar y suministrar rápidamente con un esfuerzo de gestión mínimo o con una interacción mínima con el proveedor de los servicios.
- ✓ **Confidencialidad de datos:** Protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros.
- ✓ **Crackers:** Es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- ✓ **Disponibilidad:** Acceso a la información cuando se requiere, teniendo en cuenta la privacidad. Evitar "caídas" del sistema que permitan accesos ilegítimos, que impidan el acceso al correo.
- ✓ **Gestión de la seguridad de la información:** Procesos mediante los cuales se previene, detecta y se responde a incidentes de seguridad de la información implicando un mantenimiento continuo, revisión y auditoría a dichos procesos.

- ✓ **Hackers:** Es un término general que se ha optimizado históricamente para describir a un experto en programación. Recientemente este término se ha utilizado con frecuencia con un sentido negativo, para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa, aunque no siempre tiene que ser esa su finalidad.
- ✓ **Herramientas de seguridad:** un conjunto de herramientas de seguridad informática libres y de código abierto y de red para llevar a cabo rutinas de seguridad, diagnóstico de red y monitoreo de seguridad.
- ✓ **Integridad de datos:** se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.
- ✓ **Malware:** la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.
- ✓ **Phishing:** es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. (Ltd.)
- ✓ Riesgo cibernético: Posibles resultados negativos derivados de fallas en la seguridad de la infraestructura tecnológica o asociados a ataques cibernéticos.
- ✓ **Secuestro de información:** Este es uno de los más sofisticados y modernos malwares ya que lo que hace es secuestrar datos (encriptándolos) y pedir un rescate por ellos Normalmente, se solicita una transferencia en bitcoins, la moneda digital, para evitar el

rastreo y localización Este tipo de ciberataque va en aumento y es uno de los más temidos en la actualidad

- ✓ **SGSI:** Es un conjunto de procesos que comprende las políticas, estructura organizativa, los recursos, procedimientos, procesos necesarios para implementar y mejorar de manera continua la Seguridad de la Información tomando como base los riesgos a los cuales se enfrentan la organización.
- ✓ **Smishing:** Es una forma de phishing mediante la cual alguien intenta obtener información privada a través de un mensaje de texto o SMS El smishing es una amenaza emergente y en crecimiento en el mundo de la seguridad en línea
- ✓ **Suplantación de Identidad:** Es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndose a un sitio web falso
- ✓ **Vishing – Voz:** Es una nueva estafa que pretende suplantar la identidad del afectado a través de VoIP (Voice over IP), recreando una voz automatizada semejante a la de las entidades bancarias.

CAPÍTULO II- METODOLOGÍA DE INVESTIGACIÓN

2.1 ENFOQUE Y TIPO DE INVESTIGACIÒN

Al analizar la naturaleza del problema y sus objetivos, se determinó que la investigación debe abordarse bajo el enfoque cualitativo el cual requiere un proceso inductivo, interpretativo, interactivo; apropiado para el estudio de la problemática, basando la investigación en la falta de un sistema de gestión en la seguridad de la información que permita establecer hipótesis que expliquen cómo se originó el problema, sus consecuencias, al igual que verificar y comprobar la verdad de los acontecimientos, lo cual podrá deducir causas y medir sus efectos. *(Ítem 2.5 Análisis de la información)*

Posteriormente, por medio de instrumentos y técnicas se *recolectarán* los datos, a través de (cuestionario/entrevista), para obtener información de los procesos desarrollados, experiencias del personal en el tema de estudio, con el objeto de realizar un análisis de los resultados en relación al supuesto planteado.

2.2 DELIMITACIÓN DE LA INVESTIGACIÓN

2.2.1 Espacial

Para la realización de la investigación se consideró una empresa del sector industria dedicada a venta de pinturas y otras mezclas químicas del municipio de Soyapango del departamento de San Salvador, al igual que el personal que laboran en dicha empresa en el departamento de contabilidad.

2.2.2 Temporal

El periodo dentro del cual está comprendida esta investigación es de enero a septiembre de 2020 que corresponde al periodo en que fue creada la ley de Regulación del Teletrabajo en El Salvador, al igual que fue el periodo donde se genera mayor irrupción de las nuevas tecnologías con el cual se identificó la problemática.

2.3 SUJETOS Y OBJETO DE ESTUDIO

2.3.1 Unidad de Análisis

La unidad de análisis del problema de investigación es una empresa del sector industria dedicada a venta de pinturas y otras mezclas químicas del municipio de Soyapango del departamento de San Salvador, enfocada específicamente al personal que labora en dicha empresa y está personalmente involucrado en las operaciones tecnológicas y de seguridad de la entidad, los cuales son:

1.Gerente General

2. Contador General

3. Encargado del área TI

Ya que estos poseen un alto nivel de conocimiento sobre el funcionamiento y las operaciones que la empresa realiza. Por consiguiente, se desarrolló una guía de entrevista/cuestionario definido por la función de cada uno de los entrevistados o el entrevistado.

2.3.2 Universo

Para la presente investigación dada su naturaleza de estudiar la situación de una empresa del sector industria en el municipio de Soyapango, se tomará como universo al departamento de contabilidad que se mantiene trabajando en modalidad de teletrabajo con información confidencial para la empresa.

Dado que la población objeto de estudio es inferior a 30 se realizará la investigación cualitativa con el 100% del universo sin aplicación de técnicas de muestreo.

2.4 VARIABLES E INDICADORES

Las variables que componen las hipótesis de investigación son las siguientes:

2.4.1 Variable Independiente

La adecuada implementación de medidas para aumentar el grado de la seguridad de la información:

- Mejorar el resguardo de la información que se comparte entre usuarios desde puntos de partida, y un sistema que corresponde al punto de destino de la información.
- Poseer más controles que sean capaces de brindar confiabilidad a los usuarios de la información y brindar la seguridad en que la información no será infectada con archivos maliciosos.
- Utilizar las normas de seguridad que brindan organismos internacionales para constatar el cumplimiento de las medidas mediante una certificación internacional.
- Garantizar que la información de la empresa no estará disponible ni será revelada a personas, organizaciones o procesos no autorizados.

2.4.2 Variable Dependiente

Aumentar el grado de seguridad que se transmite a través de diferentes medios a través del internet a modo que posea las características de disponibilidad, confiabilidad e integridad que permita asegurar que la información no ha sufrido cambios o alteraciones maliciosas:

- Fortalecer las relaciones de negocios con sus clientes manteniendo la confidencialidad de su información.
- Fortalecer las relaciones de negocios con sus proveedores manteniendo la confidencialidad de su información.
- Mantener la información exacta y completa, tal como fue finalmente elaborada, así como sus métodos de proceso según los lineamientos de control interno.

2.5 TÉCNICAS E INSTRUMENTOS

Las técnicas utilizadas para recolectar la información serán por medio de entrevistas a las unidades de análisis antes mencionadas como lo son el contador general, el gerente general o contralor de la empresa y el encargado del área informática de una empresa de fabricación de pinturas.

El instrumento utilizado fue una guía de preguntas especializadas para cada unidad de análisis, la información obtenida se realizó mediante una entrevista presencial. Tomando nota mediante grabación de audios y también recolectado mediante respuestas por escrito según la disponibilidad y método más conveniente para los entrevistados.

La información obtenida de las entrevistas se procesó en Microsoft Word para que de manera posterior se trasladará al documento que se encuentra en la nube para que todos los integrantes pudieran tener acceso en tiempo real para hacer sus aportes y cualquier corrección además de ello se compartió el documento a los asesores para que pudieran ver el avance y el aporte de cada integrante del equipo en la conformación a la narrativa.

De manera objetiva de cada tema se logró formar una opinión de las variables investigadas con el instrumento, el análisis de los resultados que se tomaron en cuenta el conocimiento teórico y empírico, además de los aspectos concretos de la problemática, para poder conformar el planteamiento del problema y comprobar las hipótesis planteadas.

El diagnóstico de los datos fue elaborado visualizando las variables de estudio, se desarrolló evaluando la validez y el contexto de cada una de las preguntas orientadas a la problemática y variables para dar respuesta y formarse una idea de cómo se encuentra la situación de la seguridad de la información al interior de la empresa.

Principalmente de las unidades de análisis que son las que manejan la información se obtuvo y también se tomó en cuenta algunos aspectos del marco normativo legal, así como también del marco normativo internacional.

2.6 DIAGNÓSTICO DE LA INFORMACIÓN

2.6.1 Generalidades del SGSI

- ✓ Entendimiento de la organización
- ✓ Análisis de riesgos
- ✓ Plan de acción
- ✓ implementación

2.6.2 Descripción de Funciones de los sujetos de análisis

Tabla 1*: *Descripción de puestos de trabajo

DESCRIPCIÓN DE PUESTO DE TRABAJO	CONTADOR GENERAL	CONTRALOR	SOPORTE TI
JEFE INMEDIATO	Contralor	Gerente General	No posee jefe inmediato, sino que trabaja en función de problemas, reportaría y otras funciones para todos los usuarios en la empresa.
SUBALTERNOS	Gerentes de cada área	Auxiliares contables y personal de facturación	No posee.
FUNCIONES DEL PUESTO	Supervisar el buen funcionamiento de todas las áreas de la empresa, elaboración de procedimientos y procesos en la mejora continua.	Encargado de la contabilidad de la empresa a través de las diferentes áreas que posee la empresa, además de cumplir con obligaciones formales y legales que se requieran	Verificar el buen y adecuado funcionamiento de los sistemas de la empresa, así como de los equipos informáticos mediante la constante revisión de hardware y software, así como también de equipos y herramientas utilitarias.

INTERVENCIÓN EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA	No posee una intervención directa, solamente la verificación de que las cifras sean confiables y correctas en las distintas áreas de la empresa.	Se encarga de que las cifras de la información sean razonables de acuerdo a normativa, con respecto al seguimiento de la información y su resguardo, solo a los controles establecidos como usuarios, y carpetas personalizadas con claves para cada empleado, y con respecto a información más confidencial solo se maneja entre la alta jefatura como medida de seguridad.	Principalmente es la persona encargada de mantener en resguardo la información valiosa de la empresa a través de Firewall, backups en servidores y discos duros externos mediante copias de respaldo de la información en tiempo real a corto plazo y un backup de archivos diario a toda la información actual.
FUNCIONES DURANTE EL TELETRABAJO	Controlar el trabajo que hacían los empleados desde sus casas, mediante reportes semanales de avances de trabajo, así como también reuniones en video llamada semanales para constatar el avance del trabajo de cada empleado.	Cumplir con las obligaciones de pagos a proveedores, planillas, servicios, obligaciones en línea con distintas instituciones, además de la contabilización de esa información.	Dar soporte técnico del uso y manejo de sistemas alojados en los servidores de la empresa, en las computadoras personales de cada empleado, además del correcto funcionamiento de los mismos, elaboración de reportes de información, dar mantenimiento a los sistemas, conexiones de las máquinas, velar por el adecuado y oportuno funcionamiento de los servidores que recibía la información de cada usuario trabajando desde casa.

2.6.3 Narrativa de la información de entrevistas

Con respecto a la información proporcionada por el **Contador General** pudimos constatar que todos los procesos de todos los departamentos están automatizados, son pocos los procesos

que se realizan de manera manual, refiriéndose esto a utilizar programas utilitarios como por ejemplo Excel para generar reportes y llevar ciertos controles.

Asimismo, hay procesos, procedimientos y reportes que no alcanzan a cubrir el sistema, por ello; es necesario utilizar otras herramientas para llevar un control acerca de dichos procedimientos, por ejemplo: planillas, recursos humanos, expedientes de empleados, descuentos y retenciones laborales, entre otros.

Para el sistema y sus módulos es necesario que se tenga un administrador o un usuario maestro que sea el encargado de informática el cual asigna o quita derechos, privilegios, funciones a usuarios, teniendo una parametrización para que la información no se vea afectada o modificada por cualquier usuario, por eso es necesario que se realice esta acción de control.

Además de ello, en ciertos casos suceden errores involuntarios por parte de los usuarios al ingresar información, copiar y pegar productos o archivos, eliminar o renombrar ciertos datos, para evitar estos inconvenientes es necesario solventar y revisar la línea del tiempo y estado activo del usuario que realizó esos errores o acciones indebidas, restaurando o reponiendo la información que por error se modificó.

Esto lo realiza mediante las bases de datos siendo esta la forma más práctica y adecuada para modificar los datos, teniendo en cuenta la autorización de la gerencia, que se remite a un correo de autorización o confirmación para modificar el error y cuál fue el motivo por el que se realizó el mismo, esto con fines de control y teniendo un respaldo por si alguna entidad requiere

alguna revisión, ejemplo: el Ministerio de Hacienda o la auditoría, teniendo un amparo de la información.

Para el caso del mantenimiento de los equipos físicos y servidores, cuando se presenta alguna falla o mal funcionamiento, se tiene que intervenir verificando los errores para así sustituir la parte dañada o en el peor de los casos, reponer el equipo en su totalidad.

Se presentan diversos inconvenientes cuando las partes dañadas son los discos duros de los equipos ya que ahí se almacena la mayor parte de información que manejan los usuarios, pero esto se solventa con copias de seguridad que se realizan en tiempo real siempre y cuando sean documentos que se encuentren alojados en el servidor. Se debe tener cuidado en ese aspecto respecto al almacenamiento de los documentos ya que se encuentran vinculados con el servidor principal.

Cuando el contador llegó a laborar alrededor de un año, debía de cerciorarse del funcionamiento del sistema y todos sus módulos. Sin embargo, se encontraban manuales obsoletos que no aportan mucho pero aun así funcionaban como una ayuda. Se tiene un área de soporte técnico que es el encargado del manejo de la información, soporte, permisos y mantenimientos de los equipos.

Para el respaldo y resguardo de la información se tiene como mayor exponente un disco duro servidor y uno externo, también para datos de manejo recurrente es conveniente la utilización

de una USB para importar los documentos al no poseer una nube de información y que más usuarios puedan acceder a lo mismo.

La seguridad de la información de la empresa, es de vital importancia ya que se maneja; elaboración de insumos, fórmulas y cálculos para la producción de los productos. Con respecto a la situación actual de la pandemia, por disposiciones del gobierno se envió a los empleados a casa, pero había obligaciones de pagos a proveedores, pagos de planillas, despachos de producto y otros aspectos más, por tanto, fue necesario que el personal implementará la modalidad de teletrabajo.

La empresa al no contar con el equipo necesario para todo el personal que implementa la modalidad de teletrabajo, acordó con algunos empleados el uso de sus propios recursos. Aun así, había que adaptarse a la situación y forma de trabajo, debido a que de forma remota era más complicado hacer llegar las indicaciones o pedir avances de trabajos a los empleados que estaban laborando desde casa, debido a diversos motivos o excusas que proporcionaban.

Además de ello, se tenían que pensar e implementar estrategias de control, para agilizar procesos que no entorpecieron el trabajo de algunos que dependían del trabajo de algún compañero o compañera, por ello; fue necesario realizar procedimientos y formas de trabajo de manera obligatoria los cuales se fueron puliendo y optimizando de diferentes formas. En cuanto a las formas de transmisión de órdenes, manejos de trabajo, transmisión de información, envío de reportes, memorándum se dio por medio de correo institucional, página web.

Refiriéndonos al almacenamiento de la información, no se puede afirmar o negar la fiabilidad del mismo ya que en ocasiones fallan los dispositivos por factores alternos como, por ejemplo: los problemas de energía o tormentas eléctricas que en más de una ocasión se han presentado dañando la infraestructura de la empresa y afectando de forma negativa en el equipo informático.

En cuanto a manuales o políticas de seguridad, no se poseen, solo se tienen limitación de páginas web y ocio, firewall y parametrizaciones de usuarios en los distintos sistemas.

Acerca de los Sistemas de Gestión en la Seguridad menciona que son importantes porque estamos en un mundo donde toda la información se maneja de manera digital, no obstante, la entidad no ha capacitado al personal, lo que sí se tiene claro es la importancia de una creación, implementación y optimización para el cumplimiento de la seguridad, haciendo la accesibilidad fiable tanto para los usuarios de los sistemas como para las autoridades y la gerencia general o cualquier autoridad que requiera saber o respaldarse.

Con respecto **a la información proporcionada por el Contralor,** se le preguntó si en la empresa con anterioridad se había implementado la modalidad del teletrabajo a lo cual respondió que no, todo esto por la situación de la pandemia.

El área de administración y ventas fueron las áreas que pudieron trabajar en la modalidad antes mencionada, el área de producción fue la única que no pudo trabajar desde casa, debido a

que su forma de laborar es solo presencial, por lo que el contralor expresó que se tiene registrado que en abril y mayo no hubo producción.

El contralor exteriorizó que para controlar a su personal fue un arduo trabajo dado que, no sabía si estaban trabajando o si estaban viendo una película o haciendo otra cosa, porque no cuentan con herramientas que permitan el control de sus empleados, todo esto debido a que era la primera vez que como empresa que trabajaban en una modalidad desde casa.

Muchos empleados no pudieron desempeñar su trabajo desde su hogar puesto que no contaban con los recursos (computadora e internet), entre otras cosas, aun siendo parte del área de administración o ventas, sin dichas facilidades era complicado que llevaran a cabo sus responsabilidades.

El contralor comentó que las redes sociales no le parecen ideales para la trasmisión de la información confidencial de la empresa, o plataformas como Zoom. También, expresó su disconformidad frente a lo inseguro que es y hace referencia a un caso en particular que salió en las noticias en donde la plataforma Zoom había sufrido un hackeo y expuso mucha información de ciertas empresas, pero al no contar con otra plataforma para comunicarse con sus empleados, se vieron obligados a utilizarla, en consecuencia; las empresas se han visto obligadas a cifrar su información.

De igual forma, comenta que no hay mucha información que robar, debido a que ellos poseen de momento; un sistema rudimentario por lo que un hacker no robaría en gran medida, solo la información de las ventas, que sí es importante.

Sobre las políticas o manuales de la *ciberseguridad* en la empresa, el contralor manifiesta que no están claramente definidas. Poseen firewall, paquetes de antivirus, pero menciona que la empresa trabaja en un sistema de forma rudimentaria y esto conlleva a que no posean mucha información en los servidores, por lo que no invierten en sistemas de protección de datos.

La empresa no está preparada para un ataque virtual, hackeo o robo de información confidencial, lo único que ellos pueden hacer ante una situación así es recuperar la información ya que se realiza un backup todos los días de la información que manejan, por lo tanto, si en algún caso hipotético llegaran a hackear el sistema, se compraría otro servidor y se transferirá la información de los backup para continuar operando.

Se le preguntó a su vez sobre qué pensaría acerca de la creación e implementación de un sistema de gestión en la seguridad de la información, a lo cual el respondió que cualquier cosa que ayude a sumar es ganancia, ya que con un sistema de gestión bien definido él no tendría por qué preocuparse por el robo o alteración de la información confidencial de la empresa.

Con respecto a **la información proporcionada por el encargado de TI** se pudieron recopilar muchos datos de vital importancia en la empresa, con esto se dio a conocer que la misma cuenta con herramientas tecnológicas como servidores, discos extraíbles, entre otros; así como también un mantenimiento preventivo y correctivo de todos los equipos con un período constante de tres meses. Además, posee antivirus actualizado que lleva un constante control de los procesos de back up de la información de todas las áreas y departamentos en periodo diario y semanal.

Se cuenta también con algunas parametrizaciones de los sistemas entre departamentos donde el acceso es restringido en algunos niveles y los únicos que poseen acceso sin restricción son los del área de soporte TI.

Durante la entrevista también se manifestó que no se cuenta con controles ante el robo de información, dejándolos completamente vulnerables frente a cualquier hackeo de información, aunque se hayan tomado algunas medidas, como, por ejemplo: pocos usuarios que poseen acceso sin restricción a internet, la mayoría no poseen acceso a redes sociales ni páginas de ocio, esto ayuda de alguna manera a que la comunicación sea estrictamente por medio de correos institucionales.

En definitiva, se consideró que es de vital importancia un sistema de gestión que sea complejo y requiera de esfuerzo por parte de la organización tanto económica como capacitando al personal y así poder garantizar la seguridad de la información y de los clientes o partes interesadas, aumentando sin duda su confianza.

2.7 CRONOGRAMA DE ACTIVIDADES

TAREAS	INICIO	FIN	DIAS	AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE			
CAPÍTULO 1 - MARCO TEÓRICO																			
Áreas de Investigación	09/08/2020	15/08/2020	6																
Marco Normativo y Legal	16/08/2020	29/08/2020	13																
Definiciones	30/08/2020	08/09/2020	9																
Entrega de Capítulo 1	10/09/2020	10/09/2020	1																
CAPÍTULO 2 - METODOLOGÍA DE LA INVESTIGACIÓN																			
Enfoque y Tipo de Investigación	11/09/2020	16/09/2020	5																
Delimitación de la Investigación	17/09/2020	23/09/2020	6																
Sujetos y Objetos de Estudio	24/09/2020	30/09/2020	6																
Técnicas e Instrumentos de Investigación	01/10/2020	09/10/2020	8																
Diagnóstico	09/10/2020	09/10/2020	1																
Entrega de Capítulo 2	10/10/2020	10/10/2020	1																
CAPÍTULO 3 - PROPUESTA DE SOLUCIÓN																			
Generalidades del SGSI	11/10/2020	17/10/2020	6																
Fase 1: Entendimiento de la organización	18/10/2020	26/10/2020	8																
Fase 2: Análisis de Riesgos	27/10/2020	02/11/2020	6																
Fase 3: Plan de Acción	03/11/2020	07/11/2020	4																
Caso Practico	08/11/2020	20/11/2020	1																
Entrega de Capítulo 3	21/11/2020	30/11/2020	1																
Defensa de trabajo de investigación	21/11/2020	30/11/2020	1																

CAPÍTULO 3: PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27032

3.1 PLANTEAMIENTO DEL CASO

Con base a los resultados obtenidos, se evidenció la necesidad de proponer un Sistema de Gestión de Seguridad de Información usando como referencia la ISO/IEC 27032:2012, con el fin que la empresa de ventas de pinturas arquitectónicas tenga una guía de cómo gestionar los riesgos de *ciberseguridad*, dado que no posee políticas, medidas o procesos que controlen el riesgo de violación en su información financiera, además de ello, sirva como una guía para otras empresas que les interese salvaguardar la información valiosa de sus entidades antes los riesgos cibernéticos emergentes actualmente en el mercado.

Generalidades del SGSI

Los sistemas y procesos que hacen uso de información son, para toda la empresa, activos de gran importancia, por activos que deben ser resguardados. La protección infinita como tal no existe, ya que siempre hay, o habrá, una vulnerabilidad técnica, un riesgo imposible de mitigar o erradicar, etc. con los que las organizaciones deben convivir y por tanto siempre existe cierto nivel de riesgo.

En la empresa, la implementación de un SGSI ayudará a definir procedimientos y políticas y a establecer la planificación e implementación de controles de seguridad, basados en una evaluación de riesgos previos, siempre alineado con los objetivos de negocio de la organización y

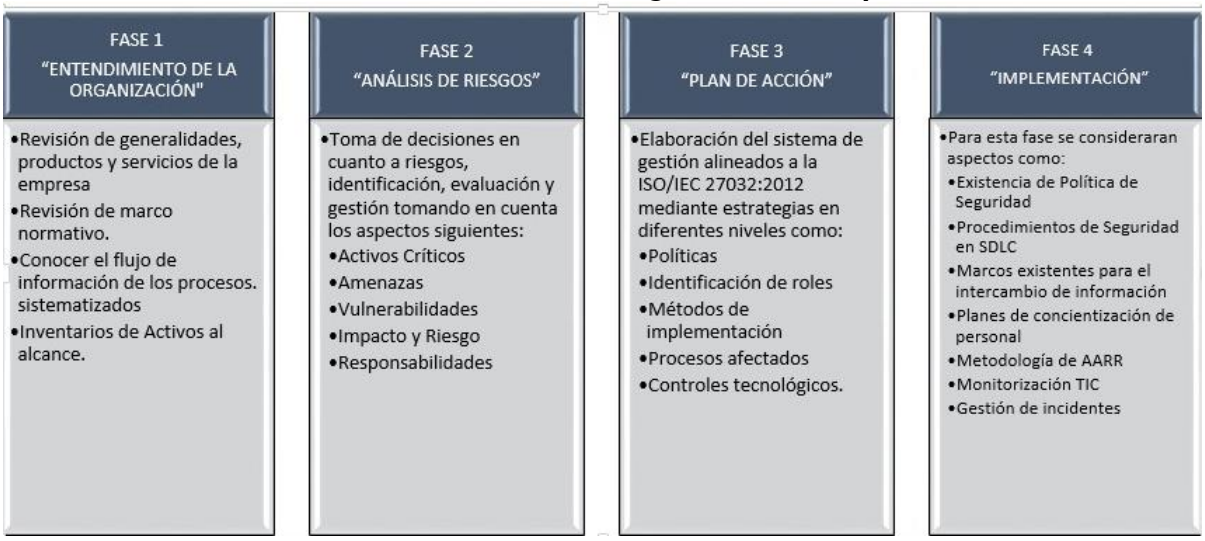
con la finalidad de mantener un nivel de riesgo por debajo del umbral que se defina al amparo de este SGSI.

Con un SGSI, la organización conocerá los riesgos a los que está sometida su información financiera. Con estos riesgos decide si los asume, los evita, los minimiza, los transfiere o planifica su Mitigación mediante la planificación de la implementación de controles.

Objetivo de un SGSI

Desarrollar principalmente un aporte en nivel de seguridad adecuado en los procesos de negocio de la empresa relacionados con la gestión de sus procesos de información financiera adecuándose a los requerimientos de seguridad cada vez más demandados por el mercado y trasmitir confianza en las metodologías utilizadas a los empleados del área de contabilidad de la empresa.

Tabla 2: ***Estructura del Sistema de Gestión de Seguridad de la Información***



3.2 BENEFICIOS Y LIMITANTES DE UN SGSI

3.2.1 Beneficios de un SGSI

Un SGSI se compone de los siguientes beneficios a las empresas:

- Se tiene un enfoque global donde se definen las políticas de seguridad en la información que conformaran las bases del resto del SGSI. Dichas políticas de seguridad deberán ser conocidas, aprobadas y promovidas por la dirección.
- El establecimiento de una metodología de gestión de la seguridad clara y en forma estructurada.
- Se implica a toda la empresa para llevar a cabo este sistema, desde la dirección hasta el usuario final mediante una estructura de roles y responsabilidades que abarcan gran parte de la empresa.
- Se pueden definir los requerimientos para la gestión de la seguridad de la información desde un punto de vista global, siendo mediante criterios comunes y procedimientos lógicos para todas las áreas implicadas.
- Un sistema SGSI no finaliza con la implementación de una serie de medidas o controles para gestionar el riesgo de la empresa, sino que es un proceso constante de revisión y actualización mediante riesgos con sus respectivos controles en constante revisión.
- Una mejora continua permite establecer una planificación para ir alcanzando los objetivos en diferentes situaciones, de forma que el sistema de gestión se va ampliando gradualmente, y permite tener en marcha un proceso de revisión para asegurar que los problemas no se repitan en reiteradas ocasiones, se implementan mejoras justificadas, permitiendo evolucionar paso a paso.

3.2.2 Limitantes del SGSI

- El tiempo que puede tomar el diseño e implementación del sistema podría ser extenso debido a que según como la empresa decida abordar las distintas áreas que la conforman, y que tan minuciosos serían los controles y políticas, de esa forma se tendría un parámetro para definir que tendría que usarse un largo periodo de tiempo.

- La resistencia al cambio por los usuarios de los sistemas y aplicaciones, debido a que se tienen métodos y procedimientos específicos realizados por los empleados, por tanto, una nueva forma de trabajo y controles más definidos y técnicos vendría a ser trabajo extra y una manera de aprender a cómo utilizar los sistemas de una manera correcta y segura.

- Podrían generarse problemas técnicos al aplicar ciertos controles tanto a los sistemas como al hardware utilizado por problemas de compatibilidad, procesamiento de datos, transferencia de archivos, entre otros.

- La inversión a realizar primeramente para el diseño de un sistema de gestión de seguridad de información específicamente para la empresa en investigación, al basarse en una norma ISO y cumplir sus lineamientos y estándares, debe de ser personal capacitado para la estructuración del documento en sus diferentes fases.

3.3 CASO PRÁCTICO

Principalmente el SGSI se centrará en procesos relacionados con la actividad de las áreas administrativas y financieras de la empresa, en su mayoría gestionadas por el área contable, esto con el fin de gestionar mediante niveles de seguridad definidos por la alta gerencia para la toma de decisiones en la implementación.

La seguridad de la información es un desafío cuando se implementa la modalidad teletrabajo. Una de las mayores preocupaciones del área de Informática, es garantizar la confidencialidad, integridad y disponibilidad de los datos que soportan la actividad de cada organización.

Sean datos confidenciales o no, la información es valiosa y requiere de sistemas efectivos de protección, que no necesariamente están asociados a encerrar la información y a los trabajadores en el espacio físico de una oficina.

Entre los temores que existen al momento de adoptar teletrabajo están el de poner en riesgo la información financiera, especialmente porque se cree que al compartir datos con dispositivos remotos se corre mayor riesgo de que sean víctimas de ataques o filtraciones.

Este temor es válido, pero ello no significa que no sea superable. Al momento de adoptar la modalidad teletrabajo, bien sea con equipos entregados por la oficina o por el uso de dispositivos de propiedad de los trabajadores, es necesario que se tomen las medidas pertinentes para garantizar la seguridad de la información.

La propuesta o solución a la problemática de la empresa es crear un sistema de gestión de seguridad de la información con el fin de formar una guía con medidas y prácticas que contengan entendimiento de la organización y sus procesos sistematizados, además de identificar los riesgos emergentes que pueden suceder.

Crear un plan como tal, que en esencia será el SGSI que contendrá una serie políticas, roles de usuarios y parametrización, métodos para implementar el plan adaptados a las necesidades de la empresa bajo la modalidad del teletrabajo como base y también alternando trabajo presencial según se disponga a las especificaciones de las actividades de trabajo de los empleados. Finalmente, la fase de implementación dejando formatos que servirán para validar los procesos y medidas y verificar que se estén cumpliendo los procedimientos contenidos en el SGSI.

3.3.1 Fases para realizar un SGSI

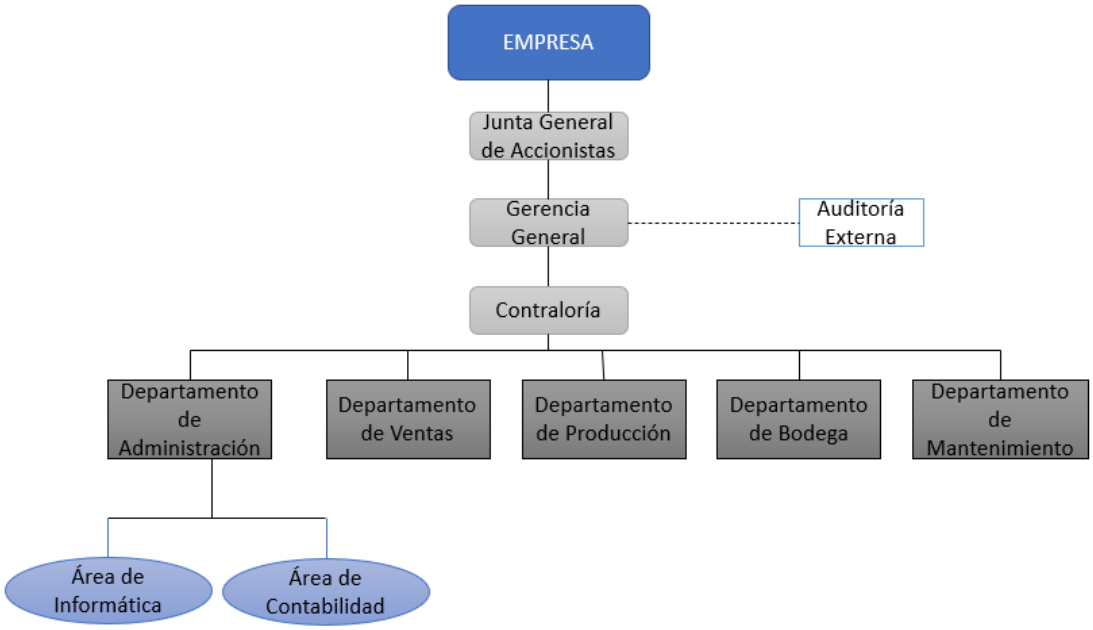
Fase 1 "Entendimiento de la organización"

En esta primera fase se realiza un importante trabajo de introducción en los procesos del funcionamiento de la empresa en lo que respecta a la automatización de la información y ver sus métodos.

Además, se tendrá en cuenta que en esta fase se tendrá un alcance en cuanto al equipo tecnológico que se posee a través de una idea del tamaño y cantidad de procesamiento de información, cantidad de empleados, y en qué áreas se desempeñan.

Conocimiento de la compañía.

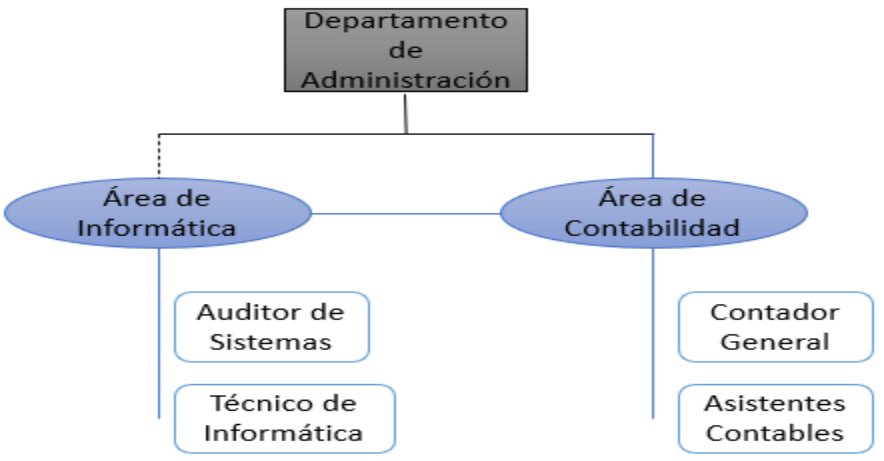
La siguiente figura se representa la estructura organizacional:



Fuente: Proporcionado por la empresa

El mapa de puestos de trabajo de la empresa está en función de cumplir los objetivos como una entidad privada orientada a la venta de productos.

Estructura de la organización (Administración)



Organigrama Elaboración propia

En la estructura anterior se toma como referencia de área de aplicación y de principal relevancia en la conformación de las áreas de análisis sensibles de la empresa con respecto a la información y el manejo de la misma.

Objetivo: Conocer la empresa a fin de establecer su tamaño, tipo de organización, tipo de tecnologías, entre otros aspectos que permitirán determinar la ruta para la elaboración de un sistema de gestión de seguridad de la información.	
Información General	
Nombre	"Empresa de Pinturas Arquitectónicas de El Salvador"
Sector	Fabricación de pinturas, barnices y productos de revestimiento similares; tintas de imprenta y masillas (Según definición de actividades económicas – Ministerio de Hacienda
Tipo de organización	Sector Privado
Objetivo del negocio	Diseñar pinturas arquitectónicas atractivas, útiles y de alta calidad que cumplan las necesidades del cliente.
Misión	Producir y ofrecer pinturas arquitectónicas industriales y en aerosol que ofrezcan una solución de cubrimiento y embellecimiento adecuada a la necesidad y capacidad económica de los mercados en donde operamos.
Visión	Ser la opción de cubrimiento y embellecimiento preferida en el mercado local para brindar protección a las superficies, reconocida por el balance entre calidad y precio
Cantidad de procesos	Con base al organigrama, se estima que tienen alrededor de 30 procesos desde la adquisición de materias primas, materiales y otros, hasta la venta de sus productos al consumidor final.
No. De empleados	Aprox. 60

Información Alta Dirección	
Involucran a la alta dirección en temas de seguridad	La dirección de la empresa, ven como una necesidad el hecho de utilizar y tener en cuenta la seguridad informática ya que los tiempos van cambiando, así como el ámbito en el que se desenvuelve el mercado como los medios electrónicos, y lo medios de comunicación tradicionales están

	quedando rezagados, por tanto, el compromiso de la implementación y seguimiento de la seguridad, empieza desde junta directiva y gerentes de la empresa.
Cuentan con el apoyo de la alta dirección para la implementación de mecanismos de seguridad	Siempre y cuando se tengan planes de creación y posterior implementación de la guía de gestión de la seguridad se debe de presentar a la gerencia debido a que se debe de tomar muchos aspectos en cuenta como el tiempo de ejecución, el personal de la empresa, presupuesto, contratación de la empresa o técnicos para la creación y ejecución de la guía de gestión.
La alta dirección es capacitada en temas de seguridad	Los que integran la alta gerencia solamente poseen formación en temas y áreas de finanzas, administrativas, mercadeo y otros, pero ninguno tiene una formación integral en el tema, entonces con esta premisa, aun así, comprenden la importancia del área para resguardar los activos digitales que se poseen.
Presentan periódicamente a la Alta dirección el estado de seguridad de la compañía con reportes de incidentes, planes de acción, entre otros.	Desgraciadamente no se realiza este control o procedimiento, ya que cada vez que surgen problemas o fallas se les da seguimiento hasta su pronta solución, pero no se lleva un reporte o bitácora de los mismos, solo se tiene como salvaguarda, los precedentes que han pasado para basarse en ello para dar una solución y arreglo de los problemas suscitados que puedan presentarse.

Estructura de TI y Seguridad	
Que áreas existen en TI	Solo se tiene un área de informática que se denomina como “Soporte TI” que se encarga por el mantenimiento de los equipos, mantenimiento del sistema y otras aplicaciones, soporte técnico y elaboración de informes que

	se requieran de bases de datos de la información.
Cuentan con el apoyo de la alta dirección para la implementación de mecanismos de seguridad	Como anteriormente se había mencionado se debe de poseer un plan de acción que se componga de todos los elementos para ver si resulta útil y atractivo para que la dirección decida aprobar la implementación de la guía de gestión.
Existe un oficial de la seguridad	No se posee en la empresa.
Cuentan con área de riesgos – Que procesos realiza	Se cuenta con diversas áreas de riesgos aplicados a los distintos activos sensibles de la empresa, que serán detallados en la fase del sistema de gestión.

Descripción Tecnológica	
Ítem	**Descripción**
Que sistemas tiene	Se cuentan con un solo sistema que integra a varios módulos que se encargan de las diversas áreas que integra la empresa.
Cuantos son propios	Solo se tiene un sistema propio que se encarga de los libros de contabilidad, mediante una integración de las cuentas contables que genera el sistema para que haya una congruencia entre las cifras.
Cuantos son subcontratados	Solo se posee 1 sistema de subcontratación que se compone de distintos módulos, licencias de usuarios y soporte técnico mediante la validez de las licencias que son entre 2 y 4 años de validez.
Cuantos sistemas son por suscripción o licencia	Se tiene el sistema principal que es de licencias, que cada cierto tiempo se debe actualizar sus versiones, además de ello se tienen las licencias en los equipos en lo que son sistemas tanto operativos, como de procesamiento de datos y antivirus tanto del equipo informático de la empresa como el equipo informático en teletrabajo de los empleados bajo esta modalidad.

Seguridad informática y de la información.	
Ítem	**Descripción**
Hardware	Computadoras de escritorio (desktop), laptops o computadoras personales, dispositivos utilitarios de entrada y salida para los equipos, impresoras, escáneres, UPS, routers, servidores, estaciones de trabajo.
Software	Sistema por módulos para las áreas de la empresa, Sistemas Operativos para cada equipo en diferentes versiones, Suites informáticas de procesamiento de información, programas freeware, antivirus con licencias empresariales.
Cuentan con mecanismos de cifrado para transferencia de información	Se cuentan con conexiones VPN, conexión a internet mediante firewall a restricciones de páginas web, usuarios para algunos programas y transmisión de archivos mediante suite de correo electrónico empresarial.
Existen mecanismos de seguridad para acceso a internet	Se tienen firewall, antivirus donde cada uno de ellos poseen restricciones e historiales de navegación para constatar el recorrido y búsquedas de los usuarios para detectar riesgo y vulnerabilidades de información.

Fase 2 “Análisis de riesgos”

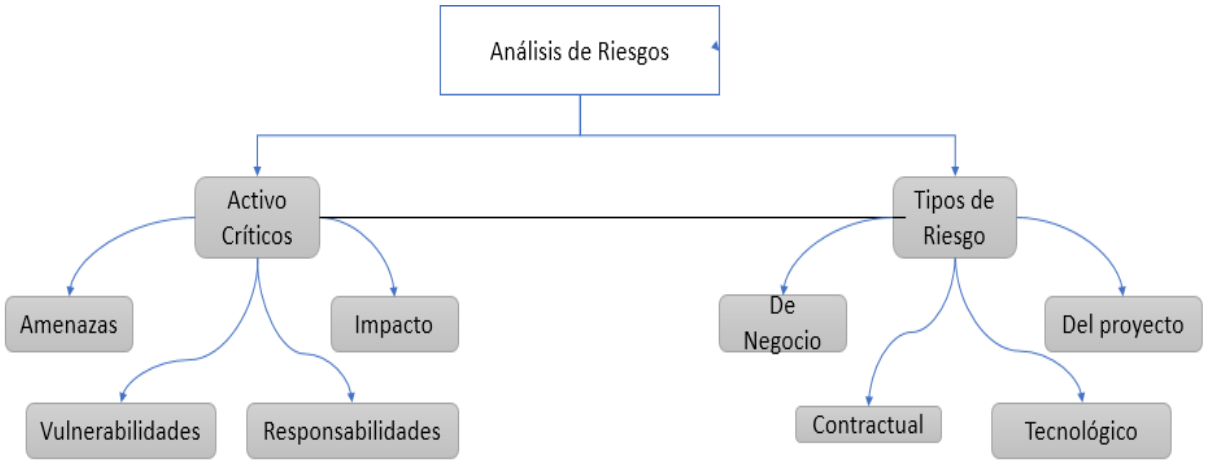
Se trata de recopilar información, teniendo en cuenta los procesos automatizados en cuanto a los activos que posea la empresa, separándolos en:

- Seguridad de la información
- Seguridad de las redes
- Seguridad de Internet
- Protección de la infraestructura física que contiene y maneja la información

Teniendo identificadas las áreas de estudio y análisis que posea la empresa se deberá tener en cuenta aspectos de medición o referentes para manejar los riesgos de cada área, siendo los siguientes:

- Prevención
- Protección y detección
- Respuesta y comunicación
- Recuperación y antecedentes
- Identificación de los Activos Críticos

Análisis de riesgos



Mapa: Elaboración propia

Activo Tipo: Información	Característica	Personal involucrado
Vital	-Licencias -Información Financiera -Información Legal -Manuales de Operación	-Área de TIC -Área Administrativa -Área de Contabilidad -Asesor Jurídico -Alta Gerencia
Personal	-Equipo de cada empleado en sus hogares, que al ser	-Área Administrativa -Área de Recursos Humanos

	personal contiene información y archivos de índole personal, a parte de la información valiosa de la empresa. -Expedientes de empleados permanentes y eventuales	-Empleados en Teletrabajo
Estratégica	-Procedimientos -Planes -Proyectos -Proyecciones de ventas	-Área de Ventas -Área de Producción -Alta Gerencia

Activo Tipo: Redes	Característica	Personal involucrado
Medios	-Red Pública de la empresa -Red privada de cada empleado en Teletrabajo -Tipo de Conexión (Ethernet, Wifi, ASDL, VPN)	-Área de Informática -Personal con acceso a cualquier tipo de internet (Residencial o Telefónico)
Soportes	-Transmisión pasiva -Transmisión activa -Dispositivos (Modem, Switch, Routers, PBX, Teléfonos)	-Área de Informática -Empresas de Telecomunicaciones -Técnicos en Soporte de Redes

-

Activo Tipo: Internet	Característica	Personal involucrado
Correo Electrónico	-Documentación -Respaldos de órdenes y seguimientos -Programación de actividades. Asignación de actividades de trabajo	-Área de Informática -Alta Gerencia -Empleados involucrados directamente
Bases de Datos Internos	-Documentos, reportes, movimientos, estados de información	-Usuarios de esta información
Bases de Datos Externos	-Documentos, reportes, movimientos, estados de información	-Usuarios de esta información
Página Web Interna (Empresa)	-Bases de productos	-Community Manager -Área de Informática

	-Información de Contacto de la empresa -Datos o generalidades de la empresa -Compras on-line	-Área de Ventas -Área de Marketing
Respaldos o Backup (Nube)	-Accesos a documentos -Usuario único o multiusuario de acceso -Modificación, edición, eliminación de archivos.	-Administrador de datos en la nube
Navegación en Internet	-Restricciones de usuarios -Accesos a paginas seleccionadas -Firewalls -Protección de Ip	-Área de Informática -Administrador de redes

-

Activo Tipo: Infraestructura física (Hardware)	Característica	Personal involucrado
Equipo Portátil	-Computadoras -Teléfonos -Otros	-Empleados modalidad Teletrabajo
Periféricos para procesamiento	-Impresoras -Scanner -Discos Removibles	-Empleados modalidad Teletrabajo
Medios Electrónicos	-CD-ROM -Discos duros removibles -Memorias removibles -DVD´s	-Empleados modalidad Teletrabajo
Otros medios	-Teléfonos Convencionales -Teléfonos IP -Fotocopiadoras	-Empleados modalidad Teletrabajo

Matriz de evaluación de riesgos

Empresa "Empresa de Pinturas Arquitectónicas de El Salvador"				
Elaborado por			**Autorizado por**	
Activo Tipo	**Información**			
Tipos de Riesgos	**Vulnerabilidades**	**Prevención**	**Detección**	**Respuesta**
Licencias	-Vencimiento	Tener control de vigencia de las licencias de cada dispositivo y usuarios	-Mensajes de Alerta por parte del equipo. -Perdida de funcionalidades del programa o aplicación.	-Realizar las gestiones con el proveedor del programa o aplicación para obtener claves nuevas o soporte técnico para las vigentes
	-Robo de seriales de licencias para n dispositivos o usuarios	Solo el usuario maestro o administrador de los equipos puede accesar a los códigos	En un equipo o varios se detecta como invalida el serial del programa, o impide realizar actualizaciones a nuevas versiones.	-Realizar un reporte o denuncia al proveedor y solicitar nuevos seriales para los equipos, realizar seguimiento de cómo se filtraron.
	-Sea adquirida de forma ilegal	Tener respaldo físico o electrónico de la compra de las licencias.	El antivirus o firewall detectan como amenaza los programas piratas o de comercialización ilegal.	Desinstalar los programas y reinstalarlos, si persiste, desactivar antivirus constatar la legalidad del programa

Información Financiera	-Se filtre por otros medios distintos de la forma oficial (Correo Electrónico)	Encriptar documentos con permisos para no permitirá la transmisión o envío por otros medios.	Se registra o rastrean documentos oficiales, por otras vías de comunicación, por medio de registro de navegación en internet.	Realizar un reporte de cada usuario, historial de navegación y transmisión de archivos en cada sesión del equipo.
	-Sea extraída de los equipos de la empresa o equipos del personal en Teletrabajo.	-Creación de usuarios para cada empleado tanto en equipo de la empresa como en equipo en Teletrabajo.	Registro de dispositivos de entrada/salida emparejados al equipo en uso y rastros de extracción de información.	Bloquear los puertos de salida y entrada de información de los equipos de la empresa y equipos en Teletrabajo.
	-Sea alterada en reportes o movimientos de cuentas	-Encriptar los documentos según sea la extensión mediante contraseñas, no edición de documentos, visualización solo de lectura	-Cifras diferentes, cuentas incorrectas, conceptos erróneos en contraste a información autorizada por la alta gerencia.	Proporcionar claves de edición y manipulación de archivos solo a personal de confianza y teniendo la responsabilidad de la información que manejan.
Información Legal	-Manipulación de la información con firmas, sellos, membretes.	Utilizar firmas electrónicas autorizadas y el membrete y sellos sea únicamente administrados por personal de gerencia.	Partes de información, datos, cifras, pueden diferir con lo realmente aprobado en cuanto a la información autorizada por la alta gerencia	Antes de presentar la información a instituciones, accionistas, o entes interesados, la gerencia debe de constatar que la información sea verídica y que finalmente se firme, selle.

	-Uso de aspectos de identificación falsificados por otros entes legales no autorizados por la empresa.	La empresa brinda a otros entes en cuanto al uso del nombre, logos, razón social u otro aspecto que haga alusión a la empresa.	La empresa se da cuenta por diversos medios que otras empresas, instituciones o terceros usan sus distintivos sin ninguna autorización previa.	La empresa denunciaría cualquier uso de la marca sin consentimiento a partir de las fases de denuncias en caso de que quien use sin autorización la marca se rehúse a retractarse del uso ilegal de la misma.
	-Filtrar información legal de la empresa por terceros.	Impedir la extracción de información mediante la desactivación de puertos de salida de información de los equipos.	La información legal la transfieren mediante medios a través del internet en distintas formas y plataformas.	Cifrar los documentos mediante contraseñas de eliminación, edición, vista ya sea en el mismo documento o en una carpeta comprimida indescifrable.
Manuales de Operación	-Manuales inexistentes	No se poseen manuales de operación de seguridad.	El hecho de que no se posean manuales para regular los riesgos resulta en una alta vulnerabilidad de los procesos y controles	La creación de un sistema de gestión para que posteriormente se llegue a implementar es la respuesta a mediano plazo que se pretende.
	-Manuales desfasados ante el entorno actual	No se poseen manuales de operación.	La falta de manuales de procedimientos impide detectar el desfase de su contenido y procedimientos.	Al realizar un plan de acción, es de vital importancia la conformación de manuales de procedimientos.

Equipo Personal Informático	Equipos informáticos de empleados en modalidad Teletrabajo	Se crea un usuario administrador aparte del usuario personal en cada equipo, esto con el fin de tener los controles de los equipos y se use una cuenta para el trabajo.	El empleado puede mantener las dos cuentas activas, su usuario personal y el usuario de la empresa para realizar actividades ajenas y que no pertenecen a la jornada laboral de la empresa.	Desactivar temporalmente durante la jornada laboral el usuario personal de cada empleado para impedir interrupciones o uso inadecuado del tiempo de trabajo.
	Expedientes de empleados	Los archivos, información y otros documentos tanto del empleado como los de la empresa se mantienen independiente su uso y transmisión mediante controles restrictivos.	-Los empleados pueden acceder, modificar o transferir documentos entre un usuario y otro.	Verificar las funciones y permisos de cada usuario a fin de verificar y realizar una nueva parametrización de roles y permisos para cada uno.
	Expedientes de empleados permanentes y eventuales.	Solo el área de recursos humanos maneja la información de cada empleado con base a su modalidad de contratación.	Los empleados pueden accesar a información confidencial de otros empleados siendo recursos humanos y gerencia los únicos autorizados a hacerlo.	EL área informática debe de revisar estas deficiencias de visibilidad de información confidencial y aplicar nuevos controles o maneras de presentación de información más selectiva.

Procedimientos internos de la empresa	Planes, proyectos, proyecciones de ventas.	La información que se genera del sistema de las distintas áreas de la empresa se resguarda y solo se permite generar a los usuarios autorizados.	Información de esta índole, se encuentra en posesión de terceros o de áreas que no poseen el permiso de utilizar o visualizar.	Revisar la información que se tiene para investigar el usuario que filtro la información y los motivos de ello, con el finde tomar cartas en el asunto hacia los culpables de eso.

Empresa "Empresa de Pinturas Arquitectónicas de El Salvador"				
Elaborado por		**Autorizado por**		
Activo Tipo	**Redes**			
Tipos de Riesgos	**Vulnerabilidades**	**Prevención**	**Detección**	**Respuesta**
Acceso a red pública de la empresa/ red de internet de cada empleado en Teletrabajo	Acceso Red pública de la empresa	La red de la empresa posee clave mediante cifrado de seguridad WSK en su router que hace más segura el acceso o violación a la red.	Usuarios tienen acceso a la red, que por alguna razón obtuvieron la clave de conexión y eso implica una conexión más lenta en cadena en todos los equipos conectados.	Realizar un reinicio en las configuraciones del router, cambiar claves de acceso y usuarios, a modo de ejercer un control más intenso en cuanto a la red de informática que maneja claves y usuarios de acceso a la red.
	Acceso a Red privada de cada empleado en Teletrabajo	Al ser una red residencial u otro tipo de conexión que se maneje en teletrabajo en	La red la utilizan varios usuarios en el lugar de teletrabajo del empleado por	Proporcionar internet a empleados con diversos problemas o limitantes de este

		un principio no tiene controles o filtros, se utilizan programas bloqueadores de páginas en el usuario del equipo empresarial.	tanto se tiende a navegar de forma lenta lo cual genera conflicto en el trabajo de cada empleado.	tipo para que no se vean interrumpido la velocidad óptima para el desempeño.
	Mal uso de los tipos de conexión que se manejan	Se tiene previsto el bloqueo de páginas de ocio en los equipos para que los usuarios no naveguen por las mismas.	Se puede utilizar la red para descargar o subir archivos lo cual interrumpe el óptimo funcionamiento de programas de la empresa.	El área de informática debe crear mecanismos a través de firewalls o programas que impidan la libre descargar y subida de archivos distintos de la organización con otros fines ajenos a la jornada laboral.
Soporte de Seguridad	Seguridad Activa	Se tiene un control en la gestión de permisos, credenciales y protección de equipos.	Dispositivos no controlados pueden acceder a la red sin permisos o credenciales.	Se puede detectar la señal y la clave Ip que generan y tratar de bloquear o expulsar de la red de la empresa.
	Seguridad Pasiva	Se tienen controles preventivos de escaneo y limpieza de equipos, recuperación de información, particiones a documentación mediante discos duros.	Incidentes o accidentes en los equipos informáticos que pueden llegar comprometer, dañar o perder información de la empresa.	Reanalizar las medidas de controles que se tienen y realizar un mantenimiento preventivo constante en los equipos y programas importantes.

	Daño en Hardware de conexión a redes (Router, Switch, Routers, PBX, Teléfonos)	La empresa se ampara al funcionamiento y calidad de la empresa proveedora del servicio, así como del equipo que distribuye	Daños o mal funcionamiento al equipo que es necesario para el correcto funcionamiento y distribución de los servicios de comunicación.	Hacer uso de las garantías, seguros, protección a daños que se tienen mediante clausulas en el contrato de los servicios en la empresa de telecomunicación

Empresa "Empresa de Pinturas Arquitectónicas de El Salvador"				
Elaborado por		Autorizado por		
Activo Tipo	**Internet**			
Tipos de Riesgos	**Vulnerabilidades**	**Prevención**	**Detección**	**Respuesta**
Uso de Correo Electrónico	Enviar información de la empresa a correos de terceros que no tienen relación de ningún tipo.	Se posee la información cifrada por tanto quien reciba la información debe de poseer la contraseñar para abrir documentos y archivos.	Se tiene registro de usuarios enviando las credenciales de documentos importantes para poder abrirse.	Detectar a las personas que están haciendo estas prácticas y sancionarlos según sea la gravedad a modo de impedir estas prácticas de forma recurrente.
Uso de bases de datos internos	Enviar información sensible e importante que solo se puede manejar dentro de los equipos	Mediante indicaciones o directrices se instruye al personal que estas prácticas no están permitidas.	Uno de los empleados ha violado las indicaciones y usa el correo para enviar bases de datos de un equipo a otro.	Sancionar al empleado para que no vuelva a suceder sin importar las justificantes que lo hayan llevado a hacer eso.
Uso de bases de datos externos	Se utilizan bases de datos de sistemas que pueden enviarse o	Se envía un memorándum a los empleados para los	Alguno de los empleados ha violado una de las	Sancionar a empleados que incurran en estas fallas y no

	transmitirse, pero con ciertas restricciones.	permisos y restricciones que posee este tipo de información.	restricciones o confunde el tipo de base de datos que envía.	permitir que sucedan, haciendo que sigan los lineamientos establecidos.
Administración de la página web de la empresa	Acceso a las bases de datos, código de fuentes y credenciales	Únicamente los que poseen los permisos, manipulación e información que posee la página web la administra el área de informática.	Se presentan errores en la interfaz de la página web.	Revisar el código de fuente, permisos y configuración de las partes que integran el sitio web del dominio que posee la empresa.
Respaldos o Backup de información en la nube	La información que se administra en la nube, presenta errores de datos y compatibilidad.	La información se sube en archivos comprimidos con credenciales para que no sean modificables o presenten problemas al abrirlos.	Al descargar los archivos, presenta errores en la extracción o sobre la misma descarga.	Verificar si en un principio se subieron correctamente los documentos, o si hubo errores en descargas para corregir esos inconvenientes.
Navegación en internet	Los equipos se encuentran en riesgo de adquirir virus de distintos tipos por la navegación en diversas páginas.	Se poseen antivirus y firewall con licencias empresariales, soporte técnico local e internacional de los programas.	En el análisis de antivirus se identifican archivos que puedan dañar los sistemas o el hardware.	Obtener el detalle de los archivos maliciosos y en caso que el antivirus no pueda eliminarlos o poner en cuarentena, realizar restricciones para eliminar esos archivos de forma de programación manual.

Empresa “Empresa de Pinturas Arquitectónicas de El Salvador”				
Elaborado por		Autorizado por		
Activo Tipo	**(Infraestructura) Hardware**			
Tipos de Riesgos	**Vulnerabilidades**	**Prevención**	**Detección**	**Respuesta**
Equipo de escritorio y portátil de la empresa	Daño en los circuitos internos de los equipos.	Mantenimiento preventivo y correctivo de los equipos a cargo del área de informática.	Mal funcionamiento en los equipos que genera fallas e imposibilita el óptimo funcionamiento.	Se debe tratar de identificar las partes que generan el mal funcionamiento y tratar de arreglar o reestablecer por una pieza nueva.
Periféricos de procesamiento	Fallos en la vinculación de periféricos que generan reportes impresos a partir del equipo informático.	Se les brinda un mantenimiento especial a los periféricos teniendo en cuenta según sea el caso no dañar el equipo en caso tenga garantía.	Al generar reportes se observan fallos o imperfecciones en la documentación generada.	En caso de que el mantenimiento de informática no logre solucionar los problemas, es necesario contactar al fabricante para solucionar o cambiar el equipo que genera problemas.
Dispositivos electrónicos de transferencia	Uso de dispositivos electrónicos para ingresar o extraer información.	Se toman como medidas la desactivación de los puertos usb ya que es el medio más utilizado para el almacenamiento de información	Empleados usan dispositivos diferentes al pendrive para el ingreso o extracción de la información de los equipos.	Verificar las formas o puertos que utilizan para introducir dispositivos y con base a ello desactivar o bloquear.

Fase 3 "Plan de acción"

En esta fase teniendo los resultados de las 2 fases anteriores se puede formular y estructurar el SGSI especializado y adaptado a las variables de trabajo de la empresa que deberá de contener niveles de diferente aplicabilidad los cuales son:

- Políticas
- Identificación de roles de usuarios
- Procesos automatizados afectados
- Controles tecnológicos
- Controles en *Ciberseguridad*

En el caso de la empresa, dada la situación actual en el ámbito de la Seguridad de la Información, en relación con los controles definidos en la ISO/IEC 27032, aplicándose la *ciberseguridad* en la modalidad de Teletrabajo, que se define a continuación

CHECKLIST DE GESTION DE SEGURIDAD DE LA INFORMACIÓN				
DOMINIO: SEGURIDAD DE LA INFORMACIÓN Según Norma ISO/IEC 27032				
Objetivo: *Planear, diseñar y recomendar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) enfocado a los procesos de las áreas de: División informática, control interno, administración servicios al personal, información financiera seguridad física en "Pinturas Arquitectónicas El Salvador"*				
Componente	***Procesos/Respuestas/Observaciones***	***SI***	***NO***	***N/A***
1- POLÍTICAS DE SEGURIDAD				
1-1 Políticas Generales				
1-2 Políticas de Control de Acceso				
1-3 Políticas de Correo Electrónico				
1-4 Políticas del Uso de Internet				

1-5 Políticas de Ciberseguridad				
1-6 Políticas de Uso de los Sistemas de Información financiera y administrativa				
1-7 Políticas de Realización de Copias de Respaldo				
2-AUTORIZACIONES DE ROLES DE USUARIOS				
2-1 Privilegios de Usuarios				
2-2 Atributos de Seguridad				
2-3 Aplicaciones con Privilegios				
2-4 Perfil de derechos de usuarios				
2-5 Definir Roles Parametrizados				
2-6 Preparación				
2-7 Detección y análisis				
2-8 Contención, resolución, recuperación				
2-9 Acciones posteriores al cierre contable				
3-PROCESOS AFECTADOS				
3-1 Dispositivos autorizados y no autorizados				
3-2 Software autorizados y no autorizados				
3-3 Privilegios administrativos				
3-4 Configuración de hardware y software				
3-5 Correos y navegadores en internet				
3-6 Controles de puertos de equipos				
3-7 Seguridad en Softwares				
3-8 Respuestas y gestión de incidentes				
4-CONTROLES TECNOLÓGICOS				
4-1 Control de acceso				
4-2 Acceso a servicios de Red				
4-3 Accesos a aplicaciones				
4-4 Acceso a Sistemas				
4-5 Controles Criptográficos				
4-6 Controles ante Software malicioso				
4-7 Controles de Registros y supervisión				

4-8 Controles de Comunicaciones				
4-9 Controles sobre vulnerabilidades técnicas				
5-CONTROLES EN CIBERSEGURIDAD				
5-1 Políticas de Ciberseguridad para sistemas y dispositivos.				
5-2 Actualización de políticas de almacenamiento y resguardo de información				
5-3 Normas de buenas prácticas de Ciberseguridad				
5-4 Realización de estudios de vulnerabilidad ante los riesgos de la ciberseguridad				
5-5 Uso de leyes locales e internacionales de aplicación ante riesgos de la ciberseguridad				
5-6 Inventarios de Hardware con acceso a la red sin asignación de roles.				
5-7 Verificación periódica de instalación de software legal en todo el equipo de la empresa				
5-8 Actualización en configuraciones de seguridad para dispositivos móviles ante riesgos de vulnerabilidad				
5-9 Capacitaciones sobre temas de ciberseguridad al personal de la empresa				
5-10 Actualización de controles ante riesgos emergentes				

Fase 4: "Implementación"

Pasos para su implementación

Para la implementación de un sistema de gestión se da las siguientes recomendaciones para la organización:

- ✓ La organización debe establecer el interés de implementar el sistema de gestión en la seguridad de la información para sus proyectos.
- ✓ Se debe comunicar a todas las partes interesadas de la organización la implementación del sistema de gestión en la seguridad de la información.
- ✓ Se debe establecer la política de gestión integrada y adoptar la normativa correspondiente.
- ✓ Se recomienda a la organización identificar una persona que represente a la gerencia de la organización para el sistema de gestión y el responsable de la implementación.
- ✓ Se recomienda a la organización la implementación y cálculo de los indicadores propuestos para el control de los procesos.
- ✓ Es importante la utilización, actualización y divulgación del sistema de gestión.
- ✓ Para el mantenimiento del Sistema de Gestión es importante realizar una programación anual de auditorías internas en la cual se programa todos los procesos de implementación.

El Plan de implementación de la ISO/IEC 27032 es un aspecto clave en cualquier organización que desea alinear sus objetivos y principios de seguridad a la normativa internacional de referencia. El principal objetivo es sentar las bases del proceso de mejora continua en materia de seguridad de la información financiera, permitiendo a las organizaciones conocer el estado de la misma y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales. El proyecto

plantea el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información).

Se abordarán aspectos de la norma en la estructura, así como lineamientos, fases y su contenido, pero con el fin de trascender y ser más aplicativo y apegado a la realidad del caso práctico o empresa en cuestión, se adaptan algunos aspectos teniendo en cuenta las variables de la investigación, rubro de la empresa y aspectos legales de la regulación local.

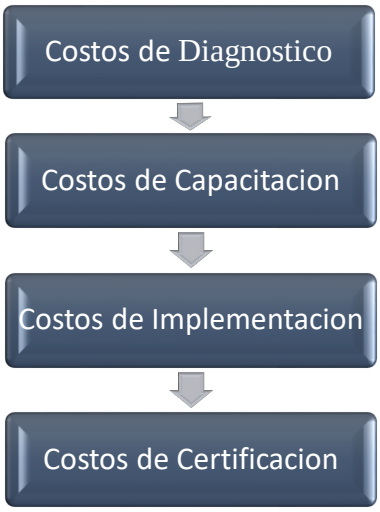
En este sentido, en torno a la investigación se busca realizar la implementación del SGSI con base a la investigación previa realizada en el capítulo 2 mediante el uso de la información recabada, así como también algunos aspectos a retomar de la empresa tomada como ejemplo para nuestra investigación, teniendo en cuenta que se imposibilita el uso de información, nombres, aspectos legales de la empresa, entre otros; por tanto se hará uso de información ficticia en cuanto a nombres, información, aspectos de diferente índole a fin de salvaguardar el perfil y evitar cualquier inconveniente.

Luego de tener finalizado el SGSI el principal objeto del manual o guía en la fase de ejecución, debido a la naturaleza de nuestro tema de investigación enfocada a la empresa de estudio, no se realizará la implementación, ya que nuestro objetivo consiste en crear la estructura y conformación de un sistema de gestión de seguridad de la información, siendo esta última fase responsabilidad de la empresa realizar la ejecución, y los cambios o adaptaciones que consideren para que se obtengan los resultados esperados, teniendo en cuenta que un sistema de gestión no es cerrado ni

finalizado, sino que va teniendo transformaciones de procesos, medidas y técnicas de evaluación a los controles que van a componerlo.

Plan de recursos para implementación del SGSI

Se inicia con los costos del proyecto los cuales son los recursos necesarios para la implementación del sistema de gestión según detalle;



- Costos de Diagnostico

Se debe de iniciar con una evaluación de las condicione en las que se encuentra la empresa con base a la implementación del sistema de gestión de seguridad de la información financiera. Cabe mencionar que este diagnóstico lo elaboró el grupo investigador, el cual se presenta en el capítulo II y por lo cual esta parte no presentara ningún costo monetario.

- Costos de Capacitación

Incluye los costos en lo que se incurrirá para brindar al personal una adecuada capacitación, dado que es importante que tanto la alta dirección como el resto del personal de la empresa conozcan todo lo relacionado con los elementos del sistema, para ello se deben de realizar ciertas capacitaciones que los incorpore de lleno a trabajar bajo el sistema. Por tanto, se elabora un detalle de los cursos en los que se incurrirá para la implementación del sistema de gestión.

Las Capacitaciones se dividen de la siguiente manera:

N.º	**TÍTULO DEL CURSO**
1	Sensibilización sobre las Normas ISO 27032
2	Definición General
3	Implementación del Sistema de Gestión en la seguridad de la información

A continuación, se presenta el contenido temático de cada uno de los cursos a impartir.

1. Sensibilización sobre las Norma ISO 27032

N.º	**Contenido**
1	Propósito y ámbito de aplicación de la Norma ISO
2	Elementos del sistema de gestión en base a la Norma ISO

2. Definición general de sistema de gestión de seguridad de la información

N.º	Contenido
1	Manual general del sistema de Gestión
2	Procedimientos del sistema de gestión
3	Planes y programas del sistema de Gestión
4	Metodología para la continuidad y contingencia del negocio

3. Implementación del Sistema de Gestión

N.º	Contenido
1	Evaluaciones del Proyecto
2	Actividades de implantación (Duración y responsabilidades)
3	Control de la implementación y cronograma de actividades

Cursos	**Cantidad de personas**	**Cantidad de contenido**	**Pago de consultor**	**Total, del costo del curso**
Sensibilización sobre las Normas ISO 27032 (2 Contenidos $ 100.00 C /P)	10	2	$ 100.00	$ 2 ,000.00
Definición General (4 contenidos $100.00C /P)	10	4	$ 100.00	$ 4,000.00
Implementación del Sistema de Gestión en la seguridad de la información (3 contenidos $100.00 C /P)	10	3	$ 100.00	$ 3,000.00
Total				$ 9,000.00

- **Partidas Contables de costo de capacitación.**

PARTIDA X1		Debe	Haber
GASTOS PAGADOS POR ANTICIPADO			
Capacitación al personal		$ 7,964.60	
CREDITO FISCAL IVA		$ 1,035.40	
CCF			
ACREEDORES LOCALES			$ 8,203.54
Otros Proveedores			
Ing. Roberto Guillen			
IMPUESTO POR PAGAR			$ 796.46
ISR a terceros			
V/ por facturación de contratación de servicios de capacitación del SGSI		**$ 9,000.00**	**$ 9,000.00**

*Nota: Gastos Pagados por Anticipados

Los Gastos Pagados por Anticipado, son gastos que se registraron como un activo y que deben ser usados dentro del término de un año o en un ciclo financiero a corto plazo.

Dentro de las NIIF y las NIC no se encuentra una sección que establezca directamente lo que son los gastos pagados por anticipado sin embargo se puede deducir los párrafos que dan referencia de estos.

Los gastos pagados por anticipado forman parte de los Activo ya que cumplen con el párrafo 2.17 de las NIIF el cual establece “los Activos son beneficios económicos futuros…” Al realizar el pago por anticipado a su vez la empresa tiene derecho a recibir el beneficio pagado anticipadamente y mediante se hace uso del beneficio recibido dicho beneficio se irá transformando en gasto y así será representado contablemente.

Clasificación

Los gastos pagados por anticipado se clasifican como:

Gastos pagados por anticipado consumibles en el periodo: Son aquellos gastos pagados por anticipado que se esperan utilizar en el ejercicio y por lo tanto se presentan en el activo corriente

Gastos pagados por anticipados consumibles en más de un periodo: Son aquellos gastos pagados por anticipado que se esperan utilizar en más de un ejercicio y por lo tanto parte de su saldo se presenta en el activo corriente y parte en el activo no corriente.

Algunos de los gastos pagados por anticipado son:

- Seguros pagados por anticipados
- Pagos de Publicidad por adelantado
- Útiles y papelería

Reconocimiento

Según el párrafo 2.27 de NIIF PYMES "El reconocimiento es el proceso de incorporación en los estados financieros de una partida que cumple la definición de un activo, y que los sig. Criterios:

a) Es probable que cualquier beneficio económico futuro asociado con la partida llegue a, o salga de la entidad; y

b) la partida tiene un costo o valor que pueda ser medido con fiabilidad.

Como bien se establece en este párrafo los gastos pagados por anticipados deben ser medidos con fiabilidad, sin embargo, no siempre se conoce cuál es el valor exacto de la partida y por lo tanto estos deben estimarse en ese casos y dicha estimación debe ser razonable (Párrafo2.30)

Partida X2		Debe	Haber
ACREEDORES LOCALES		$ 8,203.54	
Otros Proveedores			
Ing. Roberto Guillen			
BANCOS			$ 8,203.54
Banco Davivienda			
V/ Pago de servicios de capacitación de la implementación del SGSI		$ 8,203.54	$ 8,203.54

Partida X3		Debe	Haber
IMPUESTO POR PAGAR		$ 796.46	
ISR a terceros			
BANCOS			$ 796.46
Banco Davivienda			
V/ Pago de servicios de capacitación de la implementación del SGSI		$ 796.46	$ 796.46

La amortización de capacitación será implementada en los seis meses que durará la implementación del sistema de gestión.

AMORTIZACION DE LA CAPACITACION DE IMPLEMENTACION DEL SGSI		
SALDO		**PERIODOS**
$ 9,000.00		**6**
	MENSUALIDAD	**$ 1,500.00 ***
MES	**CUOTA**	**SALDO**
jun-21	$ 1,500.00	$ 7,500.00
jul-21	$ 1,500.00	$ 6,000.00
ago-21	$ 1,500.00	$ 4,500.00
sep-21	$ 1,500.00	$ 3,000.00
oct-21	$ 1,500.00	$ 1,500.00
nov -21	$ 1,500.00	$ 0.00

Partida X4		Debe	Haber
GASTOS DE ADMINISTRACION			
Capacitaciones al Personal		$ 1,500.00	
GASTOS PAGADOS POR ANTICIPADO			$ 1,500.00
Capacitación al Personal			
		$ 1,500.00	$ 1,500.00
V/ Por provisión mensual amortizando de la implementación de sistema de gestión			

*Nota: La amortización se realizará de manera mensual hasta que se cumpla la implementación del sistema.

- Costos de la Documentación

Esto incluye el costo fijo de la documentación requerida para la implementación del sistema de gestión de seguridad de la información

Costo por copia $0.02

N.º	**TÍTULO DEL CURSO**	**N. de Copias**	
1	Sensibilización sobre las Normas ISO 27032	450	$ 9.00
2	Definición General del SGSI	540	$ 10.80
3	Implementación del Sistema de Gestión	675	$ 13.50
Total, Copias			$ 33.30

Cursos	Cantidad de personas	Cantidad / Doc.	Precio unitario	Total del costo
Anillado	10	1	$ 2.00	$20.00
Cartapacio	10	1	$5.00	$50.00
Separadores	10	1	$2.00	$20.00
Copias				$33.30
Total				$123.30

- **Partida de papelería**

PARTIDA X5		Debe	Haber
GASTOS DE ADMINISTRACIÓN			
Papelería y Útiles		$ 109.12	
CREDITO FISCAL IVA		$ 14.18	
CCF			
BANCOS			$ 123.30
Banco Davivienda			
V/ por costo de papelería en capacitación para implementación de sistema de gestión		$ 123.30	$ 123.30

- Costos de implementación

Estos son los costos de operación en los que incurrirá la empresa en la puesta en marcha del sistema de gestión de la seguridad de la información. Los costos de operación es la valoración monetaria de la suma de recursos destinados a la administración, operación y funcionamiento de una empresa, por lo tanto, es importante tomar en cuenta los costos en que se va a incurrir para mantener y administrar.

Los costos permanentes a los que se verá enfrentada la empresa serán los siguientes:

1) Asignación de personal nuevo

Se debe contar con una persona que sea la responsable directa de velar por el funcionamiento del sistema de gestión, para que sea quien representa a la alta dirección. El salario promedio para una persona que desempeña esta función es de $900.00 mensuales.

Perfil de personal a contratar.

Asistente de Seguridad	GRADO ACADÉMICO: graduado en Licenciatura en Administración de Empresas, Ingeniería Industrial o carreras afines al cargo o experiencia sobre armamento y personal de seguridad, trato y conducción de personal armado, Haber desempeñado cargos similares en seguridad: física, personal y de documentos por lo menos tres años.
	CONOCIMIENTOS ESPECIALES: Protección a personas importantes (PPI), Sistemas de recolección de información, planes de acción y de reacción, control y evaluación de sistemas de seguridad, así como también conocer sobre relaciones humanas, dominio de paquetes computacionales, en procesador de palabra y con énfasis en presentaciones.
	HABILIDADES ESPECIALES: Manejo de personal armado, manejo de armas, integración y coordinación de equipos de trabajo, toma de decisiones, propositivo y con capacidad de trabajar con metas de trabajo, con dominio de aplicaciones informáticos.
	ACTITUDES: Proactivo, capacidad de trabajar bajo presión, responsable, discreto y con disposición de trabajar fuera de la jornada laboral.

2) Papelería para emisión de informes

Este monto es establecido por la cantidad promedio de impresiones destinadas para la emisión de informes, se consideran $30.00 mensuales.

3) Atención a capacitación de personal

Las reuniones de comité se deben realizar una vez al mes para analizar los resultados obtenidos en los diferentes procesos, se consideran $25.00 mensuales.

Descripción	**Costo Mensual**	**Costo semestral**
Personal Nuevo	$ 918.75	$ 5,512.50
Papelería	$ 30.00	$ 180.00
Atención a capacitación de personal	$ 25.00	$ 150.00
Total		$ 5,842.50

*Nota: estos costos son mensuales y para efectos de inversión inicial se consideran seis meses, en los cuales estará a prueba el sistema de gestión previo a la auditoria de certificación.

Partidas Contables de costo de implementación.

- Pago de pago de asistente de seguridad

PARTIDA X6		Debe	Haber
GASTOS DE ADMINISTRACION		$ 700.00	
Salarios a empleados			
RETENCIONES LABORALES			$ 105.05
ISSS	$ 21.00		
Cuota AFP	$ 50.75		
ISR	$ 33.30		
BANCOS			$ 594.95
Banco Davivienda			
Pago de salario correspondiente al mes de junio de 2021		$ 700.00	$ 700.00

PARTIDA X7		Debe	Haber
GASTOS DE ADMINISTRACION			
Aporte patronal empleados		$ 113.75	
ISSS	$ 52.50		
AFP	$ 54.25		
INSAFORD	$ 7.00		
Cuentas por pagar			$ 113.75
Beneficios a empleados			
ISSS	$ 52.50		
AFP	$ 54.25		
INSAFORD	$ 7.00		
Reconocimiento de aporte patronal correspondiente al mes de junio de 2021		$ 113.75	$ 113.75

PARTIDA X8		Debe	Haber
GASTOS DE ADMINISTRACION			
Vacación		$ 105.00	
Aguinaldo			
Indemnización			
Cuentas por pagar			$ 105.00
Beneficios a empleados			
Vacación	$ 17.50		
Aguinaldo	$ 29.17		
Indemnización	$ 58.33		$ -
Pago de salario correspondiente al mes de junio de 2021		$ 105.00	$ 105.00

*Nota: El monto se prorratea en seis meses de junio a noviembre de 2021

- Pago de papelería para ser utilizada en informes y reunión de comité

PARTIDA X9		Debe	Haber
GASTOS DE ADMINISTRACION			
Papelería y Útiles		$ 26.55	
Atención por reuniones de Personal		$ 22.12	
CREDITO FISCAL IVA		$ 6.33	
CCF			
BANCOS LOCALES			$ 55.00
Banco Davivienda			
V/ Por costos para verificación de pruebas al SGSI previo a certificación		$ 55.00	$ 55.00

- Costos de certificación

En este apartado se incluye el costo de la auditoría de segunda parte y la auditoría de certificación.

1) Auditoría externa

Esta auditoría será realizada por un consultor externo a la empresa. Costo $900.00.

PARTIDA X10		Debe	Haber
GASTOS DE ADMINISTRACION			
Honorarios		$ 797.00	
CREDITO FISCAL IVA		$ 103.61	
CCF			
-			
BANCOS LOCALES			$ 820.91
Banco Davivienda			
IMPUESTO POR PAGAR			$ 79.70
ISR a terceros			
V/ Pago de honorarios profesionales para auditoria de sistemas informáticos previo a certificación		$ 900.61	$ 900.61

2) Auditoria de certificación:

Para determinar el costo de la auditoria de certificación la cual asciende a $ 1,500.00

PARTIDA X11		Debe	Haber
GASTOS DE ADMINISTRACION			
Certificación		$ 1,327.43	
ISO 27037			
CREDITO FISCAL IVA		$ 172.57	
CCF			
BANCOS LOCALES			$ 1,500.00
Banco Davivienda			
V/ Pago de certificación ISO 27032		$ 1,500.00	$ 1,500.00

- Costos totales de proyecto.

Descripción	Costo Total
Costo Diagnostico	$ -
Costo de Capacitación	$ 9,000.00
Costo de Papelería	$ 123.30
Costo de Implementación	$ 5,842.50
Costo de verificación	$ 2,400.00
Total	$ 17,365.80

CONCLUSIONES

Como resultado de la investigación realizada se concluye lo siguiente:

- Es necesario la implementación del sistema de gestión basado en la ISO 27032, para el establecimiento de políticas y procedimientos para un mejor control en la transferencia de la información en la modalidad teletrabajo.

- La implementación del sistema de gestión de seguridad de la información debe ir acompañado del compromiso de la empresa y sus trabajadores para obtener resultados notables y lograr el mejoramiento continuo de los controles implementados.

- La aplicación de guías presentadas en esta investigación permitirá a la empresa identificar el estado en el que se encuentra a nivel de *ciberseguridad* e implementar los controles sobre los puntos clave de la empresa tomando como base lo planteado en esta investigación.

RECOMENDACIONES

De acuerdo a conclusiones anteriores se recomienda:

- Poner en práctica los mecanismos establecidos para verificar si los controles que se están llevando a cabo son eficientes.

- Hacer partícipe al mayor número de empleados en la implementación para que el uso del sistema de gestión de seguridad de la información sea de manera habitual.

- Establecer un seguimiento constante del sistema de seguridad de la información la cual puede ser realizada en forma periódica según lo determine la empresa.

BIBLIOGRAFIA

- Consultoría para la implementación de un marco de *ciberseguridad* ISO/IEC 27032. (2018). *Auditors, Internet Security*.

- Gómez. (2018).
- 5 Beneficios de implementar un sistema de gestión de seguridad de la información. (2019).
- (2019). *Fintech.* San Salvador.
- La importancia de la seguridad informática en tu empresa. (2019).
- Politicas de seguridad informática. (2019).
- Ataque de día cero. (2020). *Wikipedia*.
- Diferencias entre seguridad informática y SI . (2020). *Seguridad Atlas LTDA*.
- Seguridad de la Información. (2020). *WIKIPEDIA* .
- Teletrabajo: una historia llena de desafíos. (2020).
- Asamblea Legislativa, d. (16 de 02 de 2005). Decreto Legislativo No 611. *Codigo de trabajo*. Publicado en el Diario Oficial No 55 Tomo 366, 18 de marzo de 2005.
- AUDITORS, I. S. (s.f.). *isecauditors.* Obtenido de https://www.isecauditors.com/consultoria-csf-iso-27032
- Castro, A. R. (2011). Riesgo tecnológico y su impacto para las organizaciones Parte 1.
- Deloitte. (2019). Las preocupaciones del CISO. *El estado de la ciberseguridad en el 2019*. file:///C:/Users/Admon03/Desktop/Deloitte-ES-informe%20CISOS-ciberseguridad.pdf.
- Excellence, I. T. (2020). Seguridad informática o seguridad de la información.
- ISO TOOLS. (20 de 08 de 2017). 4 opciones de mitigación en el tratamiento de riesgos según ISO 27001. *PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA*. https://www.isotools.org/2017/08/20/4-opciones-mitigacion-tratamiento-riesgos-segun-iso-27001/.
- Las normas ISO, & Importancia y Beneficios . (28 de 09 de 2016). Las normas ISO : Importancia y Beneficios. *Daruma*. https://www.darumasoftware.com/gestion-calidad/las-normas-iso-importancia-beneficios/.
- Ltd., M. (s.f.). *https://es.malwarebytes.com/phishing/*. Obtenido de Suplantación de identidad (phishing): https://es.malwarebytes.com/phishing/
- Maria Camilo Arevalo. (20 de 12 de 2019). ISO 27032, el estándar enfocado en ciberseguridad. https://www.riesgoscero.com/blog/iso-27032-el-estandar-enfocado-en-ciberseguridad.
- Negocios. (2019). Las empresas de consumo con las más afectadas por ciberataques. *elsalvador.com*.
- netasystemsoficial. (02 de 07 de 2019). *Fases de la ciberseguridad ante una amenaza*. Obtenido de https://netasystems.home.blog/2019/07/02/fases-de-la-ciberseguridad-ante-una-amenaza/
- Normalización, O. S. (2019). Seguridad de la Información.
- Normas ISO. (s.f.). ISO 27001 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. https://www.normas-iso.com/iso-27001/.

- Organizacion Internacional de Normalizacion. (20 de 04 de 2019). Seguridad de la información, ciberseguridad y protección de la privacidad. *1/SC27, ISO/IEC JTC*. https://www.iso.org/committee/45306.html.
- OSTEC. (30 de 12 de 2016). ISO 27002: Buenas prácticas para gestión de la seguridad de la información. https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi.

ANEXOS

GUIA 1

UNIVERSIDAD DE EL SALVADOR

FACULTAD E CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Guía de preguntas dirigido al Contador General de Empresa de Pinturas S.A. de C.V.

OBJETIVO: Obtener información por parte del Contador General de la empresa, respecto a la importancia de desarrollar un Sistema Gestión de Seguridad de la Información con el involucramiento del profesional de la contaduría que contribuya en la calidad de información de la empresa.

1.En el área de contabilidad, ¿Los procesos contables de información financiera los llevan de forma sistematizada?

2. ¿Existe un administrador del sistema y cuáles son sus funciones?

3. ¿Existe un manual del usuario para dicho sistema?

4. ¿Qué conocimientos tiene sobre la seguridad de la información en la entidad?

5. ¿De la siguiente lista de controles relacionados al respaldo de la información, mencione cuáles son los controles aplicados en la entidad:

- USB
- Disco duro externo
- Respaldo en línea (Nube)

- Otros

6. ¿Cuál es la importancia de la seguridad de la información en la empresa?

7. ¿Según la situación que se vivió en el país con respecto a la cuarentena por causa del COVID-19 su empresa adoptó la modalidad del Teletrabajo?

8. ¿La empresa brindó el equipo necesario al personal para implementar la modalidad Teletrabajo?

9. ¿Qué tipo de control utiliza para la trasmisión de la información como reportes, informes, memorándum entre otros en la modalidad Teletrabajo?

10. ¿Los programas que utilizan en la empresa para almacenar datos, cumplen con las características de seguridad? (Explique las características)

11. ¿Dentro de la empresa existe un manual o política de seguridad de información?

12. ¿Qué podría decir acerca de los sistemas de gestión de la seguridad de la información?

13. ¿Ha recibido capacitaciones relacionadas a los sistemas de gestión de la seguridad de la información? ¿Si recibe con qué frecuencia?

14. ¿Considera importante la implementación de un sistema de gestión de seguridad de la información? ¿Por qué?

GUIA 2

UNIVERSIDAD DE EL SALVADOR

FACULTAD E CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Cuestionario dirigido al área de Soporte TI, Soyapango, San Salvador

OBJETIVO: Obtener información por parte del área de informática de la empresa, respecto a la importancia de desarrollar un Sistema Gestión de Seguridad de la Información con el involucramiento del profesional de la contaduría que contribuya en la calidad de información financiera de la empresa.

1. ¿Quién es responsable de instalar y mantener el software de seguridad en las computadoras?

- Empleados
- Administrador de Sistemas
- Personal de TI

2. ¿En qué lugar se almacena la información del sistema?

3. ¿La empresa cuenta con servidores, de ser así de qué tipo son?

4. ¿Se realizan mantenimientos preventivos y correctivos y con qué frecuencia?

5. ¿De qué forma se extrae la información de las computadoras?

6. ¿Qué tan seguro son sus controles ante el robo o alteración indebida de la información valiosa de la empresa?

7. ¿Describa si existe una parametrización de usuarios para cada empleado del área contable?

8. ¿Tiene software antivirus y otros escudos instalados en las computadoras?

9. ¿Con qué frecuencia actualizas un software antivirus?

10 ¿Realiza copia de seguridad de datos?

11. De la siguiente lista de controles relacionados al respaldo de la información, mencione cuáles son los controles aplicados en la entidad:

Opción
Respaldo en línea (nube)
Utilización de disco duro externo exclusivo para back-ups
Utilización de un disco duro interno (computadoras con uso múltiple)
Almacenaje físico interno
Contratación de servicio de almacenaje externo
Realización de respaldos completos
Realización de respaldos diferenciales
Realización de respaldos incrementales

12. ¿Cuentan con un sistema con un sistema de Gestión para la seguridad de la información?

13. ¿Considera necesario la implementación de un sistema de gestión para la seguridad de la información en la modalidad del teletrabajo?

GUIA 3

UNIVERSIDAD DE EL SALVADOR

FACULTAD E CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

Guía de preguntas dirigido al Gerente o Contralor de Empresa de Pintura S.A. de C.V.

OBJETIVO: Obtener información por parte del General o Contralor de la empresa, respecto a la importancia de desarrollar un Sistema Gestión de Seguridad de la Información con el involucramiento del profesional de la contaduría que contribuya en la calidad de información de la empresa.

1. ¿Se había implementado con anterioridad el teletrabajo en la empresa?

2. ¿Qué áreas o departamentos utilizó el teletrabajo durante la situación de cuarentena?

3. ¿Qué medidas o controles implementó como gerente para el seguimiento de actividades de los empleados en Teletrabajo?

4. ¿Considera que las redes sociales o plataformas de videollamadas son canales ideales y seguros para la trasmisión y asignación de tareas para el cumplimiento del trabajo diario?

5. ¿Cuentan con políticas o manual de la *ciberseguridad* y cómo se aplica a la seguridad de la información?

6. ¿Qué tan preparada esta la empresa ante un hackeo, robo o alteración de información confidencial?

7. ¿Poseen alguna certificación local o internacional que asegure la integridad, disponibilidad y confiabilidad de la información de la empresa?

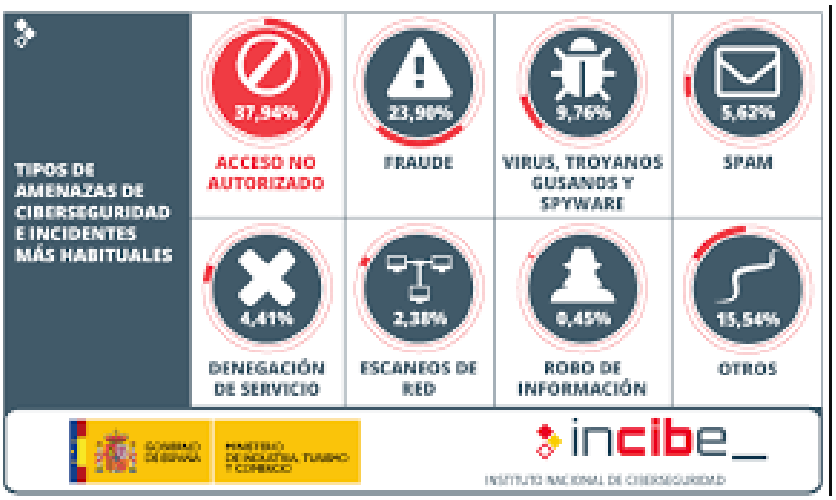
8. ¿La inversión en una certificación de seguridad de la información es costosa, así como la creación de SGSI, estima conveniente el desarrollo de alguna de estas 2 modalidades?

9. ¿Considera que sería indicado la creación e implementación de un sistema de gestión de seguridad de la información para la empresa?

Figura 4 ***Ciberseguridad de la empresa***

Fuente: (Ciberseguridad de la empresa , 2017)

Figura *5 Tipos de Amenazas de Ciberseguridad*



Fuente: (Tipos de Amenazas de Ciberseguridad e incidentes mas habituales, 2017)

Figura 6: ***Implementación de Sistema de Gestión basado en ISO 27032***

Fuente: Elaboración propia

Figura 7 ***Planilla de salario de asistente de seguridad, aporte patronal y beneficios a empleado correspondiente al periodo de junio a noviembre de 2021.***

PLANILLA DE SUELDOS
PLANILLA DE SALARIO CORREPONDIENTE AL MES JUNIO DE 2021
Valores Expresados en Dólares Estadounidenses

					DIAS	RETENCIONES Y DESCUENTOS				APORTES PATRONALES					
	NOMBRE	CARGO	SUELDO ACTUAL	TOTAL DEVENGADO	LAB.	ISSS	AFP	RENTA	OTROS	ISSS	AFP	ISSS	TOTAL RETENCION Y DESC.	NETO A RECIBIR	TOTAL GASTO
						3%	7.25%			7.50%	7.75%	1.00%			
1	Personal Nuevo	Asistente de Seguridad	$ 700.00	$ 700.00	30	$ 21.00	$ 50.75	$ 33.30	$ -	$ 52.50	$ 54.25	$ 7.00	$ 105.05	$ 594.96	**$ 806.75**
	Planilla SGSI	----------	**$ 700.00**	**$ 700.00**		**$ 21.00**	**$ 50.75**	**$ 33.30**	**$ -**	**$ 52.50**	**$ 54.25**	**$ 7.00**	**$ 105.05**	**$ 594.96**	**$ 806.75**

	NOMBRE	CARGO	SUELDO ACTUAL	VACACION PROPORCIONAL	AGUINALDO PROPORCIONAL	INDEMNIZACIONPROPORCIONAL
1	Personal Nuevo	Asistente de Seguridad	$ 700.00	$ 105.00	$ 175.00	$ 350.00
	Planilla SGSI	----------	**$ 700.00**	**$ 105.00**	**$ 175.00**	**$ 350.00**

*Nota:

- Monto de vacación calculado en base a ley
- Monto de Aguinaldo en base a ley
- Monto de Indemnización en base a ley