UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“PROPUESTA DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA EL COMERCIO ELECTRÓNICO DE LAS PYMES DEL PARQUE INDUSTRIAL DE VILLA EL SALVADOR”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

ESPINOZA CUSQUISIBAN, GREGORIO DUBERLI

Villa El Salvador

2020

DEDICATORIA

A mis padres, Gregorio y María, y a mis hermanas, por sus ejemplos y apoyo incondicional para seguir superándome día a día, ellos son un pilar fundamental para seguir adelante

AGRADECIMIENTO

Agradezco a Dios por permitir darme la oportunidad de compartir este logro con mis queridos padres.

Agradezco a mi alma máter, Universidad Nacional Tecnológica de Lima Sur (UNTELS), quien me abrió las puertas para desarrollarme profesionalmente.

Al Ing. Hernán Ochoa Carbajal, mi asesor, por su guía y apoyo en brindarme las pautas necesarias para la elaboración de este trabajo de investigación.

A mis docentes universitarios, quienes han contribuido a través de sus conocimientos en mi formación profesional.

A mi querida familia, por su paciencia y apoyo motivacional para seguir adelante a pesar de los momentos difíciles.

A mi hermana Gaby, quien a pesar de sus tareas diarias, me ha ayudado en dedicarme y enfocarme en mi proyecto.

A todas las personas que de alguna u otra manera han o están en mi vida, de los cuales guardo sus consejos, enseñanzas y ánimos.

ÍNDICE

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

El presente trabajo de Investigación se realizó con la finalidad de optimizar la seguridad de la Información de las PYMES del Parque Industrial de Villa El Salvador vinculados al comercio electrónico, tomando como base a la Norma ISO/IEC 27001.

En estos últimos años, la información ya se considera como uno de los activos más valiosos en una empresa independientemente del tamaño de ésta; así mismo, el comercio electrónico ha tomado un papel importante sobre todo en los últimos meses, a tal punto que dicho tipo de comercio se vuelve más vulnerable a ataques informáticos. Actualmente, en su mayoría, muchas de la PYMES del Parque Industrial de Villa El Salvador no cuentan con un adecuado manejo y control de su información para sus diferentes procesos de comercio electrónico, por lo que aquí se propone un Plan de Seguridad de la Información aplicando los criterios de la Norma ISO/IEC 27001, buscando de esta manera obtener los controles mínimos que garanticen un comercio electrónico seguro y confiable para el cliente y empresa, logrando así un beneficio mutuo.

INTRODUCCIÓN

El presente trabajo de investigación, consiste en proponer un Plan de Seguridad de la Información, tomando como base el uso de la norma ISO/IEC 27001, para el comercio electrónico de las PYMES ubicadas en el Parque Industrial de Villa el Salvador, el cual actualmente concentra diferentes pequeñas y medianas empresas que poco a poco van creciendo económicamente en sectores de producción tales como carpintería, metal mecánica, confecciones, calzado, artesanía, construcción, entre otros, siendo así considerado como una zona productiva importante de Lima Sur y un eje primordial en la generación de empleo.

La seguridad en las empresas ya no se encuentra limitada a la protección de dinero, bienes y personas, la realidad actual exige la protección de un recurso más llamado Información. Toda organización necesita y depende de la información y la tecnología para el desarrollo seguro de sus diferentes procesos.

El interés de la presente investigación surge a raíz de la coyuntura atravesada por el Covid-19 y el crecimiento de compras vía online en los últimos meses, haciendo necesario adoptar medidas de seguridad que permitan que las PYMES del Parque Industrial del Villa El Salvador realicen un comercio electrónico de calidad en relación con una seguridad eficiente, esto basado principalmente en los 3 principios fundamentales de la Seguridad de la Información, los cuales son: Confidencialidad, Integridad y Disponibilidad.

Para el desarrollo del presente proyecto de investigación, se ha tomado en cuenta los siguientes capítulos:

En el Capítulo I, se elabora el Marco Teórico, en el que se plantea las bases teóricas y definiciones de términos básicos relacionadas a un Sistema de Gestión de Seguridad de la Información, ISO/IEC 270001 y el comercio electrónico, el cual permite tener una base para el desarrollo de la investigación.

En el Capítulo II, el cual comprende el desarrollo en sí del proyecto de investigación, la metodología y herramienta utilizada, así como la consolidación en la solución del problema y los resultados esperados.

OBJETIVOS

a. Objetivo General.

Proponer un Plan de Seguridad de la Información basado en la norma ISO/IEC 27001 para optimizar la confidencialidad, integridad y disponibilidad de la información en el comercio electrónico de las PYMES del Parque Industrial de Villa el Salvador.

b. Objetivos Específicos.

- Identificar y clasificar los activos de Información de las PYMES del Parque Industrial de Villa el Salvador.

- Identificar y evaluar los riesgos asociados a la seguridad de la Información en las PYMES del Parque Industrial de Villa el Salvador.

- Determinar las principales políticas de seguridad de la Información basado en la norma ISO/IEC 27001 para las PYMES del Parque Industrial de Villa el Salvador.

CAPÍTULO I: MARCO TEÓRICO

1.1 Bases Teóricas

1.1.1 Antecedentes

A continuación, se mencionan una serie de trabajos de investigación que se encuentran relacionados con el presente trabajo.

- "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA Y AUDITORÍA, APLICANDO LA NORMA ISO/IEC 27001", presentado por la Bachiller Tola Franco Diana Elizabeth (Guayaquil, 2015), en la cual pretende dar una adecuada solución de seguridad a la empresa A&CGroup, dedicada a la consultoría y auditoría. Esto se hace una necesidad debido a que A&CGroup trabaja con información de estados financieros de diversos clientes, por lo que es necesario un correcto uso y manejo de dicha información, para así asegurar una protección adecuada. Se mencionó conceptos claves tal como, la metodología PDCA (Plan-Do-Check-Act), importante para planificar la calidad de un servicio o producto durante su ciclo de vida. Tola (2015) llega a la conclusión que, los Sistemas de Gestión de Seguridad de la Información basado en la norma ISO 27001, están referidos en la prevención, por lo que es importante la identificación de los riesgos en que se encuentran o exponen los activos.

- "ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UNA APLICACIÓN WEB QUE PERMITA GESTIONAR EL CUMPLIMIENTO DE LOS REQUISITOS Y CONTROLES DE UNA AUDITORÍA ISO 27001 BASADA EN LA NORMA TÉCNICA ECUATORIANA INEN-ISO/IEC 27001:2011", presentado por Gálvez Zambrano Frank Moisés (Guayaquil 2015); en el que pretende gestionar eficientemente el cumplimiento de los requisitos y controles de la norma ISO 27001:2011, debido a una escasez de software de auditoría para dicha norma. El aplicativo permite realizar un seguimiento de una auditoría informática bajo

los lineamientos establecidos en la mencionada norma. Gálvez (2015) llega a concluir que, el cumplimiento y seguimiento de una auditoría informática basada en la Norma ISO 27001:2011, se puede automatizar mediante el uso de una herramienta informática que cumpla con los requisitos mínimos de seguridad y acceso.

- "ISO 27001 PARA PYMES", presentado por Parra Giraldo Angela María (Medellín, 2014), en la cual propone brindar un método de implementación de la ISO 27001 para las diferentes PYMES, brindando además propuestas de controles y procedimientos de seguridad de la información a modo de estrategias preventivas. Parra (2014) concluye en que las medidas de seguridad implantadas en una empresa deben ser complementadas con políticas y procedimientos para que de esta manera se consolide la seguridad de la información.

- "GUÍA DE IMPLEMENTACIÓN DE LA SEGURIDAD BASADO EN LA NORMA ISO/IEC 27001, PARA APOYAR LA SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS DE LA COMISARÍA DEL NORTE P.N.P EN LA CIUDAD DE CHICLAYO", presentado por Alcántara Flores Julio César (Chiclayo 2015); en el que elabora una guía que sirva de base para aumentar el nivel de seguridad de la información mediante la determinación de las deficiencias o debilidades en cuanto a la seguridad de la información. Alcántara (2015) llega a la conclusión que, mediante el uso de la Guía se logró minimizar los riesgos de los activos de la institución policial, y que las políticas de seguridad fueron determinantes para incrementar el nivel de seguridad.

- "DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN ALINEADO A LA NORMA ISO/IEC 27001: CASO UNIVERSIDAD NACIONAL DE MOQUEGUA", presentado por Coaguila Mamani Maribel Estela (Moquegua 2020); mediante el cual propone un plan que permita fortalecer los sistemas informáticos con que cuenta la institución en estudio, esto mediante la aplicación

de un modelo de Gestión de Riesgos. Coaguila (2020) concluye que, debido a su versatilidad, la norma ISO/IEC 27001 resulta muy compatible en relación a la realidad actual de la Universidad que fue objeto de investigación.

- "MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE TI PARA PYMES DEL SECTOR COMERCIAL QUE DEPENDEN DE PROVEEDORES CRÍTICOS", presentado por Flores Huamani Vladimir y Chavez Rios Manuel (Lima 2020); quienes desarrollan un modelo en el cual se plantea un conjunto de controles y planes que permitan disminuir los niveles de impacto en las Tecnologías de Información ante los posibles riesgos de seguridad que se puedan presentar en relación con los proveedores de las Pymes. Flores y Chavez (2020) llegan a determinar la efectividad del modelo respecto a la gestión del riesgo y seguridad de las Tecnologías de Información, además que puede servir como base para una Gestión de Riesgos de los Sistemas de Información.

1.1.2 Normas ISO

Son documentos que especifican requisitos que se pueden utilizar en diferentes organizaciones para garantizar que los productos o servicios que brindan cumplan sus objetivos (ISOTools Excellence, 2015).

- **Objetivos de la Norma ISO**

La función de la norma ISO se basa en mejorar la eficiencia de los procesos de la empresa, establecer un sistema de gestión de calidad reconocido mundialmente y promover intercambios y negociaciones internacionales, como base para el desarrollo empresarial. Asimismo, la finalidad de crear estas certificaciones es implementarlas en empresas de todos los tamaños y ámbitos: estándares de calidad, medio ambiente, riesgo, salud y seguridad, formación, innovación, tecnología, entre otras (Nuño, 2018).

El propósito de crear estándares ISO es proporcionar pautas, coordinación, simplificación y unificación de estándares para empresas y organizaciones para reducir costos y mejorar la efectividad, y estandarizar normas de productos y servicios para organizaciones internacionales (ISOTools Excellence, 2015).

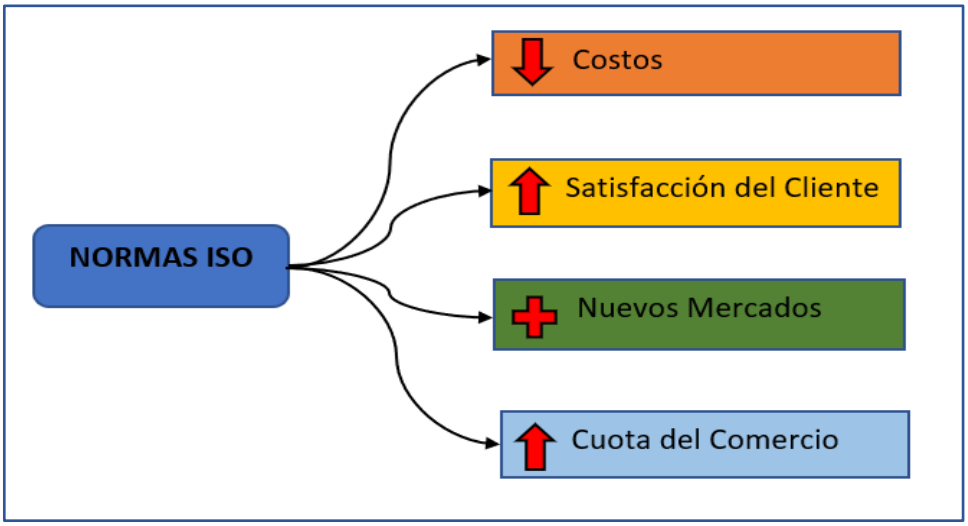

Figura 1: Ventajas de la Norma ISO

Fuente: Elaboración Propia

1.1.3 Familia ISO 27000

1.1.3.1 ISO 27000

La cual describe de manera general los estándares que componen la serie 27000, especificando el alcance y el propósito de la publicación de cada estándar. Recopila todas las definiciones de la serie 27000 y proporciona la base de por qué la implementación del SGSI es importante, da una introducción al sistema de gestión de seguridad de la información, establecimiento, seguimiento, mantenimiento y mejora de un SGSI (ISO27000, s.f.).

1.1.3.2 ISO 27001

Este es un estándar internacional que permite el aseguramiento, confidencialidad e integridad de los datos e información y los sistemas que

procesan esta información. La norma ISO 27001 permite además a las organizaciones evaluar los riesgos y aplicar las medidas de control necesarias para mitigar o eliminar los riesgos (ISOTools Excellence, 2014).

1.1.3.3 ISO 27002

Esta es una guía de buenas prácticas en la cual describe los objetivos de control y los controles recomendados desde una perspectiva de seguridad de la información. Como se describe en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de la ISO 27002: 2005 (ISO27000, s.f.).

Welivesecurity (2014) señala que a diferencia de la versión 2005, la versión 2013 de ISO 27001 ya no es una referencia normativa, por lo que su uso es opcional. Aunque todavía su uso se recomienda, ahora se puede consultar otras fuentes de información para aplicar controles de seguridad.

1.1.3.4 ISO 27003

Esta guía se centra en los aspectos clave necesarios para diseñar e implementar con éxito un SGSI de acuerdo con ISO / IEC 27001. Describe el proceso de especificación y diseño desde el concepto hasta el funcionamiento del plan de implementación, así como el proceso de obtención de la aprobación de la alta dirección para implementar el SGSI. La guía se originó a partir del Anexo B del estándar BS 7799-2 y una serie de documentos emitidos por BSI a lo largo de los años, así como recomendaciones y pautas de implementación (ISO27000, s.f.).

1.1.3.5 ISO 27004

La norma proporciona una guía que se centra en medir y evaluar los sistemas de gestión, los objetivos de control y la eficacia del control. Estos sistemas de gestión se utilizan para gestionar la seguridad de la información de acuerdo con los requisitos de ISO / IEC 27001. Esta función es muy útil cuando la

organización requiere el cumplimiento de la cláusula de evaluación del desempeño del SGSI (welivesecurity, 2014).

1.1.3.6 ISO 27005

Proporcionar pautas de gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en ISO / IEC 27001 y tiene como objetivo ayudar en la aplicación exitosa de la seguridad de la información basada en métodos de gestión de riesgos (ISO27000, s.f.).

1.1.3.7 ISO 27006

La cual especifica cuales son los requisitos para la acreditación de entidades de auditoría y certificación del sistema de gestión de seguridad de la información. En otras palabras, cuando se aplica al organismo de certificación ISO 27001, ayuda a explicar el estándar de acreditación de ISO / IEC 17021, pero no es un estándar de acreditación en sí mismo (ISO27000, s.f.).

1.1.3.8 ISO 27007

Esta norma proporciona una guía para realizar auditorías de SGSI y las competencias requeridas por los auditores. Está basado en ISO 19011, que es un estándar para cualquier tipo de auditoría de sistemas de gestión. Se trata de una referencia muy útil cuando es necesario cumplir con las cláusulas de auditoría interna de la ISO 27001 (welivesecurity, 2014).

1.1.3.9 ISO 27010

Consiste en compartir pautas de gestión de seguridad de la información entre organizaciones o departamentos. La ISO / IEC 27010 es aplicable al intercambio y difusión de diversas formas de información sensible entre la misma industria o departamento de mercado o departamento, incluidos los campos públicos y privados, nacionales e internacionales (ISO27000, s.f.).

1.1.4 Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI consiste en un conjunto de procedimientos, políticas y directrices, así como recursos y actividades relacionados que son administrados conjuntamente por una organización para proteger sus importantes activos de información. Desde la perspectiva de la norma internacional ISO / IEC 27001, el SGSI es un método sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización, y lograr así sus objetivos (ISO27000, s.f.).

- **Elementos clave de un SGSI**

  Según ISO27000 (s.f.), el Sistema de Gestión de Seguridad de la Información está basado en tres principios básicos que explicamos a continuación:

  - **Confidencialidad:** Según este principio, la información no se proporcionará ni divulgará a personas, entidades o procesos no autorizados.

  - **Integridad:** Está referida a mantener la exactitud e integridad de la información y sus métodos de procesamiento.

  - **Disponibilidad:** Las personas, entidades o procesos autorizados acceden y utilizan la información y sus sistemas de procesamiento cuando sea necesario.

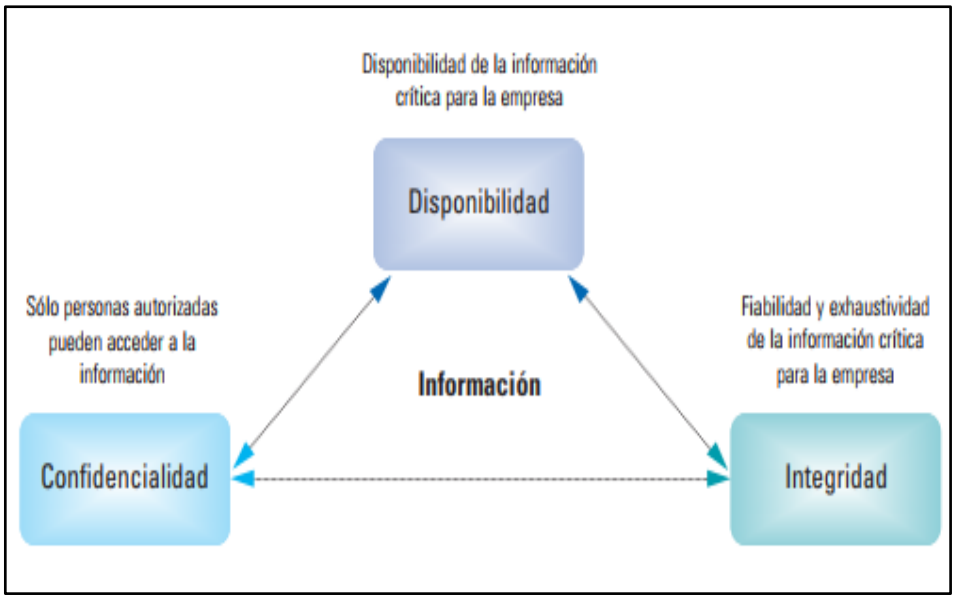

Figura 2: Elementos claves del SGSI

Fuente: tuv-sud.es

1.1.5 Metodologías de Gestión de Riesgos

1.1.5.1 Metodología Magerit

Es un método de análisis y gestión de riesgos desarrollado por el Consejo Superior de la Administración Electrónica Española, que proporciona un método sistemático que permite analizar los riesgos derivados de las tecnologías de la información y la comunicación, y así implementar medidas de control adecuadas las cuales puedan mitigar los riesgos. Para las empresas que comienzan con la gestión de la seguridad de la información, este método es muy útil porque permite enfocarse en los riesgos más críticos para la empresa, es decir, riesgos relacionados con los sistemas de información. (Gutiérrez, 2013).

1.1.5.2 Metodología Cramm

De acuerdo a Huerta (2012), es un método de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación británico, y que comprende 3 fases:

- Definir en forma general los objetivos de seguridad, incluida la definición del alcance, la identificación y evaluación de los activos tangibles e intangibles involucrados, y la determinación e identificación del valor de los datos en términos de impacto comercial.
- Realizar un análisis de riesgos determinando las amenazas que afectan al sistema y las vulnerabilidades explotadas por estas amenazas y finalmente el cálculo de los riesgos.
- Determinar y seleccionar las medidas de seguridad a aplicar en la entidad para obtener los riesgos restantes.

1.1.5.3 Metodología Octave

Es una metodología de evaluación y gestión de riesgos que permiten garantizar la seguridad del sistema informático. Utiliza una técnica de planificación y consultoría de estrategia en seguridad que se basa en el riesgo (Lara, 2014).

De acuerdo a Huerta (2012) esta metodología cuenta con 3 fases:

- Considerar la evaluación de la organización, estableciendo un perfil de activo-amenaza, recopilando los principales activos, amenazas y requisitos legales que pueden afectar al activo.
- Identificar las diferentes vulnerabilidades de estructura de TI.
- Desarrollar un plan de seguridad mediante un análisis de riesgos.

1.1.5.4 Metodología Mehari

Es un método cuyo propósito es la de permitir el análisis directo e individual del riesgo descrito en diferentes situaciones, y así proporcionar un conjunto de herramientas diseñadas específicamente para la gestión de la seguridad a corto, medio y largo plazo (GlobalSUITE , s.f.).

1.1.6 Comercio Electrónico

Según Villagómez (2018) se entiende por Comercio Electrónico, al uso de cualquier medio electrónico para realizar transacciones comerciales, refiriéndose en la mayoría de los casos a la venta de productos a través de Internet, pero el término también incluye los mecanismos de compra. El comercio electrónico en algunos casos hace que el producto sea significativamente personalizado, especialmente cuando el sitio de comercio electrónico está vinculado al sistema de producción de la empresa; además, con respecto a los servicios y productos, el comercio electrónico le permite incluso reciba información de compra inmediatamente

Figura 3: E-commerce en el mundo (2018)

Fuente: Statista Digital Market Outlook

1.1.6.1. Tipos de Comercio Electrónico

Actualmente encontramos diversos tipos de comercio electrónico adaptables al mercado actual.

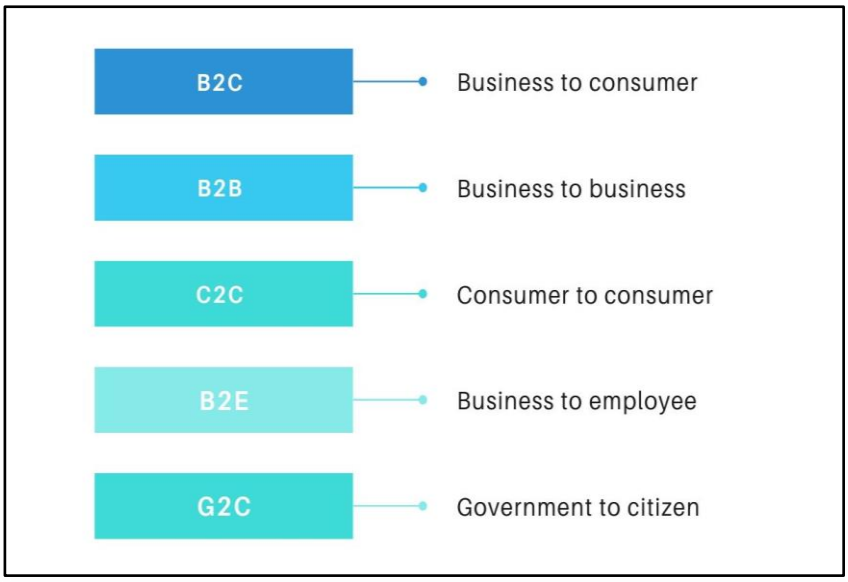

Figura 4: Modelos E-commerce

Fuente: Oberlo.com.pe

A continuación, de acuerdo a OK HOSTING (2016) tenemos los siguientes tipos de comercio electrónico:

a. Comercio Electrónico B2B.

Es la transmisión de datos relacionada con transacciones comerciales. Desde años, se ha utilizado para enviar documentos como facturas u órdenes de compra de forma electrónica, posteriormente, este tipo de negocio comenzó a incluir la compra de bienes y servicios a través de Internet y a través de servidores seguros. Estos servidores se encargan de cifrar los datos para proteger la información y proteger la seguridad de los propios consumidores, pues se utilizan mediante el uso de tarjetas de crédito o billeteras electrónicas. Realizar servicios de pago electrónico.

Figura 5: E-commerce B2B

Fuente: PromPerú

b. Comercio Electrónico B2C.

Es una o más estrategias desarrolladas y utilizadas por empresas comerciales para llegar directamente a los consumidores finales.

Figura 6: E-commerce B2C

Fuente: PromPerú

c. Comercio electrónico B2E.

Tipo de comercio que usa su propia red informática interna, mediante el cual no solo puede compartir información, sino que también se puede utilizar para otras funciones, por ejemplo, la empresa puede brindar novedades o incluso descuentos exclusivos para los empleados o personal de la red interna de la empresa. En definitiva, es el portal de una empresa y un portal para que los empleados de la misma empresa utilicen sus recursos.

Figura 7: E-commerce B2E

Fuente: humanlevel.com

d. Comercio Electrónico C2C.

Término que se utiliza para definir un modelo comercial de red, cuyo propósito es establecer una conexión comercial entre un usuario y otro usuario final, es decir es un negocio cuyo propósito es promover diversos productos y / o servicios entre particulares.

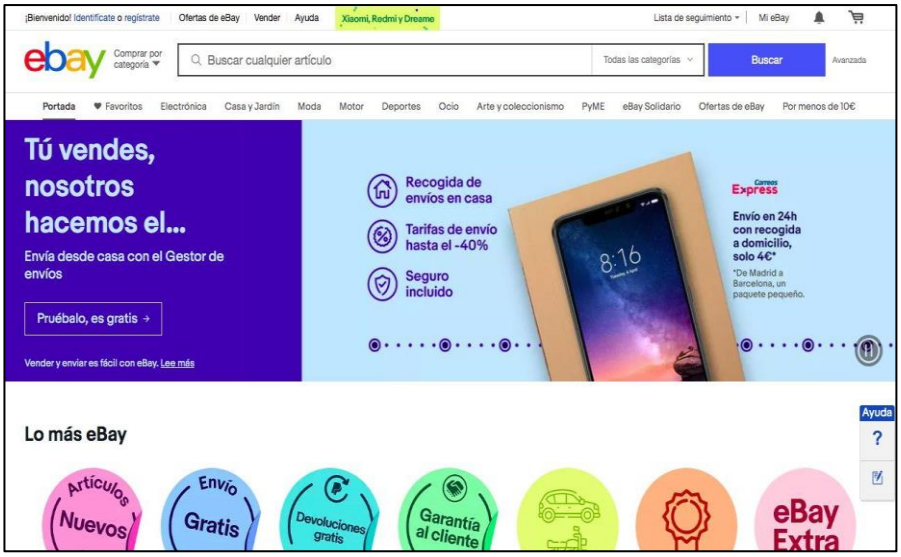

Figura 8: E-commerce C2C

Fuente: Oberlo.com.pe

e. Comercio Electrónico C2G.

Es responsable de permitir que los consumidores establezcan contacto con el gobierno, lo que permite un fácil intercambio de información a distancia entre los ciudadanos y la administración pública.

Figura 9: E-commerce C2G

Fuente: sat.com.pe

1.1.6.2 Comercio Electrónico en el Perú

En el 2019, el comercio electrónico en Perú movió $ 4 mil millones, teniendo un aumento del 31% y siendo una de las tasas de crecimiento más altas de la región. Aunque la escala del comercio electrónico en Perú es todavía pequeña en comparación con otros países de la región, ha tenido un gran salto. Como resultado, ha crecido casi 15 veces en la última década, de 276 millones de dólares en 2009 a 4 mil millones de dólares el año pasado.

Aunque en provincia ya se está desarrollando el comercio electrónico, el ritmo sigue siendo muy lento, teniendo así a la capital quien concentra la mayor cantidad de transacciones digitales, representando el 65%. Lima y Callao representaron el 55% y el 8% de las transacciones procesadas por Alignet, respectivamente. Arequipa y Trujillo juntas representan el 26% y los otros el 11% (Bravo, 2020).

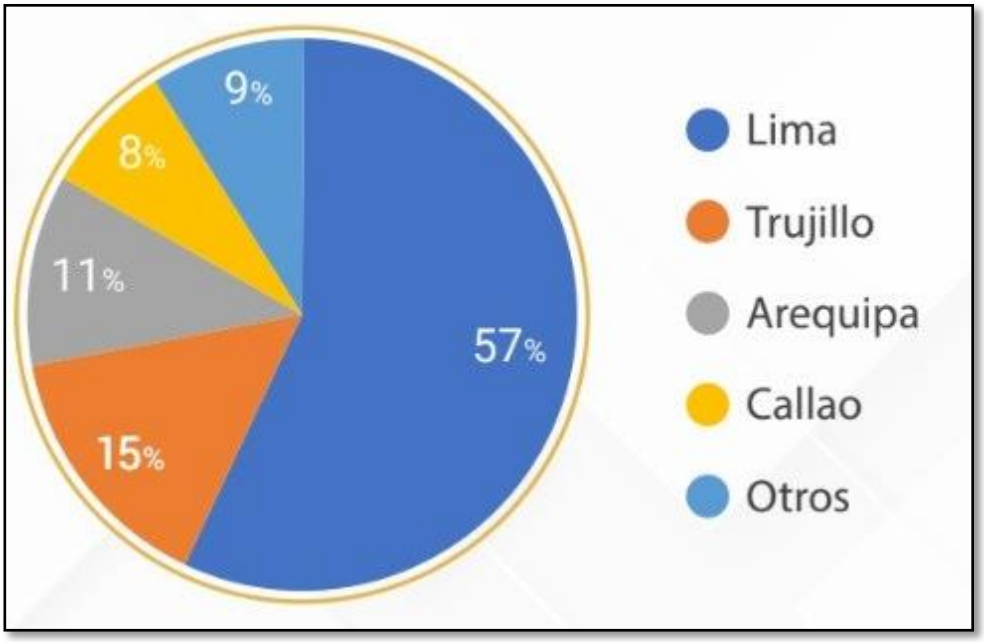

Figura 10: Distribución de Compradores Digitales

Fuente: BS Latam

1.2 Definición de Términos Básicos

- **Amenaza:** Cualquier evento que pueda provocar daño a la información.

- **Activo:** Todo aquello que tiene valor para una empresa.

- **Activo de la Información:** Cualquier información o elemento relacionado con el tratamiento de ésta que tenga valor para la entidad.

- **Hackeo:** Acción que realiza un Hacker, para este caso, persona que viola las seguridades de la información.

- **Información:** Conjunto de datos que se gestiona dentro de una organización.

- **ISO:** International Organization for Standarization (Organización Internacional de Normalización).

- **IEC:** International Electrotechnical Commission (Comisión Electrotécnica Internacional).

- **No Conformidad:** Es un incumplimiento de un requisito del sistema, sea este especificado o no. Se conoce como requisito una necesidad o expectativa establecida, generalmente explícita u obligatoria.

- **PyME:** Es el acrónimo de pequeñas y medianas empresas, son empresas que cuentan con no más de 250 trabajadores en total y una facturación moderada, no poseen un gran tamaño ni mucho menos una enorme facturación, con un número limitado de trabajadores y que no disponen de los grandes recursos de las empresas de mayor tamaño.

- **Riesgo:** Probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema Informático, causando un impacto en la empresa.

- **Seguridad de Información:** Conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza.

- **Seguridad Física:** Protección del sistema ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, entre otros.

- **Seguridad Lógica:** Protección de la información en su propio medio, mediante el enmascaramiento de esta usando técnicas de criptografía.

- **Sistema de Gestión de la Seguridad Informática (SGSI):** Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.

- **Spam:** Mensaje no solicitado, habitualmente de tipo publicitario, enviado en forma masiva a través del correo electrónico, puede presentarse por programas de mensajería instantánea o por teléfono celular.

- **Vulnerabilidad:** Cualquier debilidad que pueda permitir a las amenazas causar daño a los sistemas y por ende a la información.

CAPÍTULO II: METODOLOGÍA DE DESARROLLO

2.1 Delimitación Temporal y Espacial del Trabajo

2.1.1 Temporal

- Fecha Inicio: Agosto del 2020.
- Fecha Término: Febrero del 2021.

2.1.2 Espacial

La Propuesta de proyecto está hecha para el Parque Industrial de Villa El Salvador, el cual se encuentra ubicado a la altura de la intersección de Avenida Separadora Industrial con avenida El Sol en el distrito de Villa el Salvador.

Figura 11: Ubicación del Parque Industrial de Villa El Salvador

Fuente: Apemives

2.2 Determinación y Análisis del Problema

El Parque Industrial de Villa El Salvador es una de las zonas más importantes de Lima Sur, y es en donde se concentra diferentes tipos de empresas (micro, pequeña y mediana empresa) cuyo funcionamiento hace posible la creación de puestos de trabajo, desarrollo industrial y desarrollo económico a nivel local. EXITOSA (2020) señala que, “Los microempresarios tienen un rol protagónico en el Perú, ya que representan 95% del total de empresas (5.3MM), y sostienen al 77% de los empleos en el país”

De la misma manera, como es de conocimiento, la industria del comercio electrónico en Perú ha experimentado un crecimiento en esto últimos meses a raíz del Covid-19, haciendo así que este tipo de comercio tenga un ascenso considerable como medio de uso para la compra y venta de productos en el Parque Industrial de Villa el Salvador. La mayoría de las PYMES cuentan con teléfono celular, POS, computadora e internet como herramientas básicas para sus procesos de comercialización electrónica; sin embargo, es necesario contar con medidas de seguridad en el manejo de dichas herramientas, y así en consecuencia un adecuado manejo de la información.

2.2.1 Identificación del Proceso de Comercio Electrónico

Para determinar la problemática referente a la gestión de seguridad en el comercio electrónico de las PYMES del Parque Industrial de Villa el Salvador, es necesario conocer a groso modo el proceso de comercio electrónico de las mismas, para lo cual se ha dividido en dos procesos específicos:

a. En página web

El proceso al respecto que se da entre el cliente y la PyME es de la siguiente manera:

1. El cliente ingresa a la Página Web de la PYME para buscar un producto.
2. El cliente elige el producto deseado.

3. Se llena el carrito de compras con los productos elegidos.
4. Se calcula el valor total, considerando el costo del envío y los impuestos de ley.
5. El cliente, para realizar la compra, debe ingresar el usuario y la contraseña respectiva en caso ya se haya registrado anteriormente; de lo contrario, debe llenar un formulario de suscripción.
6. Cuando el cliente ha ingresado y enviado todos sus datos, mediante el sistema de pago, se concreta el fin de la transacción.

b. En redes sociales (WhatsApp, Facebook, Instagram)

En lo que respecta al comercio a través de redes sociales, se realiza de una forma más simplificada a comparación de una página web.

1. La PYME ofrece sus productos a través de la red social.
2. El Cliente, contacta directamente a la PYME y se negocia el precio con las características a detalle del producto de interés a través de la aplicación.
3. Si el Cliente llega a un acuerdo con la PYME, se acuerda la entrega del producto y la forma de pago del mismo, que por lo general es a contra entrega y en efectivo.

2.2.2 Puntos Sensibles de Seguridad

a. Copias de seguridad

Políticas de copias de seguridad, en la cual se establezcan los criterios necesarios para su realización tales como: almacenamiento, frecuencia, tipo de soporte, etc.

b. Contraseñas

Contraseñas seguras por parte de las PYMES, esto tanto por parte del propietario para el acceso a los datos que maneja, como en las exigidas a los clientes para su registro a la hora de acceder al comercio electrónico.

c. Almacenamiento de información sensible

Los datos que contienen información sensible, como los números de tarjetas de crédito, son vulnerables a falta de una adecuada protección de los mismos.

2.3 Modelo de Solución Propuesto

Para el desarrollo del presente proyecto de investigación se tomará y aplicará la metodología de Evaluación y Análisis de Riesgos de los diferentes activos comunes en las PYMES del Parque Industrial de Villa el Salvador, basada en la norma ISO/IEC 27001, de esta manera permitirá realizar un diagnóstico de seguridad por cada activo y poder tomar las medias de control necesarias.

2.3.1 Evaluación y Análisis de los Riesgos

Se consideran 4 pasos importantes a seguir en lo que respecta a la Gestión de Seguridad de la Información para las PYMES del Parque Industrial de Villa el Salvador.

Figura 12: Pasos para la Evaluación y Análisis de Riesgos

Fuente: Elaboración Propia

Para un mejor enfoque referentes a las evaluaciones, se tomará en cuenta la combinación de las escalas cualitativa y cuantitativa

- Escala Cuantitativa: En la cual se usa una escala de valores numéricos.
- Escala Cualitativa: En la cual se usa una escala de clasificación para describir el grado o magnitud de valor.

2.3.1.1 Identificación de Activos de Información

De acuerdo a los procesos establecidos en el comercio electrónico de la PYME, se identifican a los activos tangibles e intangibles agrupados en base al tipo de Activo relacionados con dichos procesos.

Tabla 1
Activos de una PYME

Tipo de Activo	Activo
Documentación	Documentos que contienen información relacionado al negocio y la PYME
Hardware	Equipos de comunicación y computación, medios de almacenamiento
Software	Software de aplicación, software de sistema, antivirus, página web, correo electrónico
Humano	Personal

Fuente: Elaboración Propia

Consultar el Anexo A para una mejor visualización y detalle de los Activos de Información identificados.

2.3.1.2 Valoración de Activos de Información

Para la valoración cuantitativa de los activos identificados, se tomará en cuenta los criterios de la seguridad de Información: Confidencialidad (C), Integridad (I) y Disponibilidad (D), los cuales irán desde una valoración 1 clasificado como “Baja”, hasta una valoración de 3 clasificado como “Alta”, siendo el valor final la suma de valores de los tres criterios de Seguridad tal como se muestra en el Anexo B.

Para determinar el grado de valor final del activo, se utilizará los criterios de valoración según lo indicado en la Tabla 2, y así de esta manera determinar el grado de importancia que tiene para la PYME.

Tabla 2
Criterios de Valoración de Activos

Valor	Criterio	Descripción
1 - 3	Bajo	Cuando su inactividad tiene un efecto casi irrelevante
4 - 6	Medio	Cuando su inactividad tiene un efecto de cuidado
7 - 9	Alto	Cuando su inactividad tiene un efecto grave

Fuente: Elaboración Propia

2.3.1.3 Clasificación y Valoración de Riesgos

Una vez identificado y valorado a los activos de Información, se procederá a valorar los riesgos identificados de aquellos activos categorizados con valor “Alto”. Para ello se determinará la Probabilidad que el riesgo ocurra y el Impacto o Severidad del mismo y de esta manera elaborar una matriz de calor.

a. Probabilidad de Ocurrencia: Indicativo de que tan probable es que el riesgo llegue a ocurrir.

Tabla 3
Valorización de Probabilidad de Ocurrencia del Riesgo

Valor	Criterio	Descripción
1	Poco probable	Riesgo cuya frecuencia de ocurrencia es muy baja
2	Medianamente Probable	Riesgo medianamente frecuente de ocurrir
3	Probable	Riesgo con frecuencia de ocurrencia alta
4	Muy Probable	Riesgo cuya frecuencia de ocurrencia es muy alta

Fuente: Elaboración Propia

b. Impacto o Severidad: Se refiere al grado de afectación del riesgo.

Tabla 4
Valorización de Impacto del Riesgo

Valor	Criterio	Descripción
1	Muy Bajo	Información afectada aceptable
2	Bajo	Información afectada de poco impacto
3	Alto	Información afectada de importancia
4	Muy Alto	Información afectada muy grave

Fuente: Elaboración Propia

c. Matriz de calor: Matriz de medición del riesgo que se elabora relacionando la Probabilidad con el Impacto del riesgo. Ver Figura 13 y 14.

Probabilidad de Ocurrencia		Impacto			
		Muy Bajo	Bajo	Alto	Muy Alto
		1	2	3	4
Poco Probable	4	4	8	12	16
Medianamente Probable	3	3	6	9	12
Probable	2	2	4	6	8
Muy Probable	1	1	2	3	4

Figura 13: Matriz de Calor del Riesgo

Fuente: Elaboración Propia

RIESGO	VALOR
Alto	11 a 16
Medio	4 a 10
Bajo	1 a 3

Figura 14: Criterio de Valoración del Riesgo

Fuente: Elaboración Propia

2.3.1.4 Mapa de calor de Riesgos

Se procederá a elaborar el Mapa de calor de Riesgos respectivo, identificando los Riesgos por cada activo, y así obtener el nivel de Riesgo asociado.

El Mapa de calor de riesgos obtenido se encuentra desarrollado en el Anexo C.

2.3.2 Propuesta de Políticas de Seguridad

Esta propuesta tiene como objetivo proteger los activos utilizados en el comercio electrónico de la PYME frente a amenazas (internas o externas y/o deliberadas o accidentales), ya que ayudarán a minimizar los riesgos identificados, y de esta manera asegurar el cumplimiento de la confidencialidad,

la integridad y la disponibilidad de la información. Las Políticas de Seguridad deben ser divulgadas y acatadas por todo el personal de la PYME.

Las Políticas de Seguridad de la Información a considerar son:

2.3.2.1 Política de Activos de Información

Mediante el cual se busca evitar riesgos de los activos de información y que puedan ocasionar complicaciones en el comercio electrónico de la PYME.
Entre las acciones a tomar en cuenta se tienen:

- Determinar procedimientos para el manejo de la información.
- Establecer responsabilidades sobre los activos, quienes se encargarán de controlar el acceso a los mismos.
- Controlar el mantenimiento preventivo del equipamiento informático asegurando su disponibilidad e integridad.

2.3.2.2 Política de Control de Acceso

Por medio del cual se busca impedir el acceso no autorizado a la Información.
Entre las acciones a tomar en cuenta se tienen:

- La autenticación de todos los usuarios.
- Eliminar la cuenta de acceso de los usuarios que ya no pertenecen a la PYME.
- Se deben seleccionar contraseñas robustas que permitan una mayor seguridad de acceso.
- Toda información catalogada como confidencial se de manejar de una forma tal que no se vea afectada su integridad.

2.3.2.3 Política del Personal

Cuyo propósito es la de reducir los riesgos provenientes de un error humano definiendo mecanismos que lleven al uso adecuado de los activos.

Entre las acciones a tomar en cuenta se tienen:

- Los colaboradores deben mantener la integridad de sus credenciales a fin de evitar accesos no autorizados.
- Las credenciales son personales y privadas, por lo que no se debe divulgar y/o compartir con personas ajenas al área.
- Ante cualquier evidencia de vulnerabilidad de las credenciales, se debe informar al responsable inmediato.
- Los colaboradores deberán firmar un Compromiso de Confidencialidad respecto al manejo de la información.

2.3.2.4 Política de Seguridad Física

Mediante el cual se busca impedir accesos no autorizados, daños e interferencia a las instalaciones, protegiendo de esta manera tanto el recurso como la información crítica de la misma.

Entre las acciones a tomar en cuenta se tienen:

- Los colaboradores deben contar con una identificación que les permita su ingreso a las instalaciones.
- Implementar perímetros de seguridad que permitan proteger áreas que contienen información sensible.

2.3.2.5 Política de Redes

Por los cuales se busca guardar y mantener los datos transmitidos a través de la red, minimizando así el riesgo de acceso incorrecto y tratando de proporcionar un flujo de datos seguro.

Entre las acciones a tomar en cuenta se tienen:

- La configuración de enrutadores, firewall, entre otros dispositivos de red, deben ser documentados.
- Toda información que se transmita por red pública, debe ser encriptada

2.3.2.6 Política de Correo Electrónico

Cuya finalidad es garantizar la privacidad de los correos electrónicos, el correcto uso de los mismos.

Entre las acciones a tomar en cuenta se tienen:

- Todos los mensajes de correo electrónico que contengan información confidencial, deben ser encriptados antes de ser transmitidos.
- Evitar abrir correos de dudoso origen.
- Evitar acceder y transmitir mensajes tipo spam.

2.3.2.7 Política del Comercio Electrónico

Estas políticas permitirán evitar la divulgación de información confidencial y fraude, en las transacciones a través de la página web o las redes sociales.

Entre las acciones a tomar en cuenta se tienen:

- La información referente a la forma de compra, tales como tarjetas y números de cuentas, debe estar encriptada y almacenada en dispositivos a los que se pueda acceder solo personal autorizado.
- Las transacciones de comercio realizadas a través del sitio web de la PYME, deben registrarse y archivarse máximo un mes luego de la transacción.
- Definir procedimientos de entrega de productos, reembolso de dinero y devoluciones de productos.

2.3.2.8 Política de Internet

Mediante el cual se busca establecer medidas para minimizar el riesgo generado por el acceso a Internet.

Entre las acciones a tomar en cuenta se tienen:

- Utilizar la red de internet solo para fines relacionados con la PYME y su comercio electrónico, evitando el acceso a páginas y/o aplicaciones ajenas al trabajo.
- Evitar el acceso a archivos o enlaces sospechosos.

2.3.2.9 Política de Backup

Nos van a permitir proporcionar directrices que permitan mantener la disponibilidad de la información a personal autorizado cuando sea necesario, así mismo permitirá tener un respaldo ante la pérdida de la información.

Entre las acciones a tomar en cuenta se tienen:

- Establecer mecanismo y procedimientos para realizar los respaldos de información.
- Establecer mecanismo y procedimientos para realizar la recuperación de la información.
- Los respaldos de información se deben de realizar periódicamente por el encargado de sistemas.
- El personal responsable de la copia de seguridad debe definir los procedimientos adecuados para eliminar de forma segura los soportes de información.

2.4 Resultados

Como producto de la implementación del Plan de Seguridad de la Información, se elaboró el mapa de calor de riesgos y se definieron las diferentes propuestas de Política de Seguridad, los cuales permitieron definir, en base a la norma ISO/IEC 27001, los controles de seguridad importantes y necesarios. Dichos controles permitirán a las PYMES del Parque Industrial de Villa el Salvador, minimizar los riesgos asociados a cada activo, y optimizar los procesos relacionados con el comercio electrónico de dichas PYMES.

En el Anexo D, se puede observar los diferentes Controles de Seguridad necesarios para cada riesgo.

2.5 Planificación del Proyecto

2.5.1 Alcance

La propuesta del Plan de Seguridad de la Información para las PYMES del Parque Industrial de Villa el Salvador, abarca a las áreas de Compra-Venta, Administrativa e Informática, las cuales están involucradas directamente con el comercio electrónico.

2.5.2 Cronograma

Se ha estimado un tiempo total de 7 meses en el desarrollo del presente Plan de Seguridad. Ver Anexo E.

2.5.3 Análisis Costo Beneficio

2.5.3.1 Costo del Proyecto

Tomando en cuenta los Costos tanto de la Elaboración del Plan e Implementación de los Controles de Seguridad propuesto, se han elaborado los siguientes Presupuestos tentativos.

a. Costo de Elaboración del Plan de Seguridad

En la Tabla 5 se tiene el Costo a incurrir solamente en la elaboración del Plan de Seguridad, es decir sin tomar en cuenta la Implementación de Controles.

Tabla 5
Costo de Elaboración del Plan de Seguridad

Descripción	Unidad de medida	Costo Unitario	Cantidad (Ud. Medida)	Costo Total (S/.)
Encargado del Proyecto	Mes	2500.00	5	12500.00
Computadora Portátil	Unidad	2000.00	1	2000.00
Impresora	Unidad	492.00	1	492.00
Cartucho de Tinta	Unidad	65.00	3	195.00
Lapiceros	Unidad	1.00	7	7.00
Paquetes de hojas bond	Unidad	10.00	3	30.00
Servicio de internet	Mes	136.00	7	952.00
TOTAL				**16176.00**

Fuente: Elaboración Propia

b. Costo de Implementación de los Controles del Plan de Seguridad

Según el Anexo F, se tiene un cuadro con el Costo Bruto de Implementación por cada control establecido; sin embargo, se puede observar que existen controles cuyo tratamiento y/o cláusula ISO/IEC27001 relacionada, se aplican a más de un activo analizado. Por lo mismo y para una mejor determinación y entendimiento del costo de la implementación de los controles, se ha establecido en la Tabla 6 el Costo Neto de dichos controles.

Tabla 6
Costo de Implementación de Controles

Descripción	Unidad de medida	Costo Unitario	Cantidad (Ud. Medida)	Costo Total (S/.)
Alta Dirección (Representante)	Mes	3500.00	1	3500.00
Encargado del Proyecto	Mes	2500.00	2	5000.00
Encargado de Redes	Mes	2000.00	2	4000.00
Encargado de Mantenimiento	Mes	1500.00	2	3000.00
Capacitación	Mes	500.00	1	500.00
Computadora Portátil	Unidad	2000.00	1	2000.00
Computadora de Escritorio	Unidad	2000.00	2	4000.00
Licencia Office 365	Año	180.00	1	180.00
Licencia Antivirus	Año	200.00	1	200.00
Disco Duro Externo	Unidad	250.00	2	500.00
Conectores RJ45	Unidad	0.50	10	5.00
Cable UTP	Metros	1.00	15	15.00
Canaleta	Unidad	10.00	8	80.00
Roseta RJ45	Unidad	7.50	3	22.50
Mueble de Oficina con llave	Unidad	250.00	2	500.00
Archivador con llave	Unidad	400.00	2	800.00
Lector de huella digital	Unidad	1000.00	2	2000.00
TOTAL				**26302.50**

Fuente: Elaboración Propia

2.5.3.2 Beneficio del Proyecto

Considerando los riesgos de mayor valor obtenido en el mapa de Calor, se ha elaborado un supuesto Ahorro y/o Beneficio a obtener con la Implementación del presente Plan de Seguridad. Cabe señalar que los datos registrados en la Tabla 7, se ha elaborado tomando en cuenta incidentes ocurridos una vez al año.

Tabla 7
Beneficio Aproximado del Proyecto

Descripción	Beneficio (S/.)
Pérdida de información en los activos físicos	15000.00
Borrado de información accidental	10000.00
Falla en los activos físicos	25000.00
TOTAL	**50000.00**

Fuente: Elaboración Propia

2.5.3.3 Viabilidad del Proyecto

Obtenido el Costo y Beneficio del Proyecto, se realiza calcula la relación Beneficio/Costo tal como se indica en la Tabla 8. Así pues, al ser B/C > 1 se considera aceptable y viable el Proyecto propuesto.

Tabla 8
Viabilidad del Proyecto

Descripción	Total (S/.)
Beneficio Total	50000.00
Costo Total (Elaboración+Implementación)	42478.50
Relación B/C	**1.18**

Fuente: Elaboración Propia

CONCLUSIONES

- La identificación de los procesos relacionado con el comercio electrónico, permite determinar los puntos sensibles donde la seguridad de la información es vulnerable.

- Mediante la identificación y valoración de los Activos tomando en cuenta los criterios de Confidencialidad, Integridad y Disponibilidad, se logró determinar aquellos activos de mayor importancia y atención.

- El Mapa de Calor desarrollado, permite identificar y evaluar a los riesgos de mayor criticidad, ayudando de esta manera a generar los controles específicos que permitan minimizar los riesgos.

- Las políticas de Seguridad propuestas y los controles definidos, son esenciales para garantizar un plan de seguridad de la Información eficiente ya que permiten o ayudan a los colaboradores involucrados a tener un manejo adecuado de los Activos.

- El desarrollo de un Plan de Seguridad de la Información tomando como base a la Norma ISO/IEC 27001, genera un factor de confianza y seguridad para las PYMES dentro de su proceso de comercio electrónico, además que sirve como base para una futura certificación ISO 27001.

RECOMENDACIONES

- Revisar el Plan de Seguridad periódicamente a fin de actualizar los Activos de Información iniciales, los Riesgos y controles de seguridad de acuerdo a la realidad actual.

- Capacitación constante a los colaboradores en temas de seguridad y comercio electrónico, ya que permite una mayor formación y toma de conciencia acerca de la importancia de la seguridad de la Información en este proceso.

- Compromiso integral por todos los miembros de la PYME en cuanto al desarrollo del Plan de Seguridad, a fin de cumplir los controles de seguridad determinados.

- Realizar un seguimiento de los Controles implementados a fin de mantener los niveles de riesgos estables.

- Tener claro que el plan de seguridad de la información debe ser manejado con responsabilidad y buscando siempre cumplir objetivos que agreguen valor a la PYME.

REFERENCIAS BIBLIOGRÁFICAS

Alcántara, J. (2015). Guía de Implementación de la Seguridad basado en la Norma ISO/IEC 27001, para apoyar la Seguridad en los Sistemas Informáticos de la Comisaría del Norte P.N.P en la Ciudad de Chiclayo. *(Tesis de Grado).* Universidad Católica Santo Toribio de Mogrovejo, Chiclayo.

Bravo, F. (23 de Agosto de 2020). *Comercio electrónico Perú: La Guía más completa del mercado*. Obtenido de ECOMERCE NEWS: https://www.ecommercenews.pe/ecommerce-insights/2020/crecimiento-del-comercio-electronico-en-peru.html

Coaguila, M. (2020). Diseño de un Plan de Gestión de Seguridad de Información alineado a la Norma ISO/IEC 27001: Caso Universidad Nacional de Moquegua. *(Tesis de Grado).* Universidad José Carlos Mariátegui, Moquegua.

EXITOSA. (30 de Abril de 2020). *El comercio electrónico podría crecer un 200% y convertirse en motor de la reactivación económica*. Obtenido de EXITOSA: https://exitosanoticias.pe/v1/el-comercio-electronico-podria-crecer-un-200-y-convertirse-en-motor-de-la-reactivacion-economica/

Flores, V., & Chavez, M. (2020). Modelo de Gestión de Riesgos de Seguridad de TI para pymes del sector comercial que dependen de proveedores críticos. *(Tesis de Grado).* Universidad Peruana de Ciencias Aplicadas, Lima.

Gálvez, F. (2015). Análisis, Diseño e Implementación de una Aplicación Web que permita gestionar el cumplimiento de los Requisitos y Controles de una Auditoría ISO 27001 basada en la Norma Técnica Ecuatoriana INEN-ISO/IEC 27001:2011. *(Tesis de Grado).* Universidad Politécnica Salesiana, Guayaquil.

GlobalSUITE . (s.f.). *Métodos de evaluación de riesgos: Mehari, Ebios, Octave*. Obtenido de GlobalSUITE: https://www.globalsuitesolutions.com/es/metodos-de-evaluacion-de-

riesgos/#:~:text=MEHARI%20integra%20cuestionarios%20de%20controles,y%20en%20dominios%20de%20seguridad.

Gutiérrez, C. (14 de Mayo de 2013). *MAGERIT: metodología práctica para gestionar riesgos*. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Huerta, A. (30 de Marzo de 2012). *Introducción al análisis de riesgos – Metodologías (I)*. Obtenido de SecurityArtWork: https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/#:~:text=CRAMM%20es%20la%20metodolog%C3%ADa%20de,versi%C3%B3n%20vigente%20es%20la%205.2.

Huerta, A. (2 de Abril de 2012). *Introducción al análisis de riesgos – Metodologías (II)*. Obtenido de SecurityArtWork: https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/#:~:text=OCTAVE%20es%20una%20metodolog%C3%ADa%20de,y%20Disponibilidad%2C%20esta%20metodolog%C3%ADa%20se

ISO27000. (s.f.). *Serie "27000"*. Obtenido de ISO27000: https://www.iso27000.es/iso27000.html

ISO27000. (s.f.). *SGSI*. Obtenido de ISO27000: https://www.iso27000.es/sgsi.html

ISOTools Excellence. (13 de Agosto de 2014). *¿Qué es la ISO 27001?* Obtenido de ISOTools Excellence: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISOTools Excellence. (19 de Marzo de 2015). *¿Qué son las normas ISO y cuál es su finalidad?* Obtenido de ISOTools Excellence: https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

ISOTools Excellence. (19 de Marzo de 2015). *Definición de las Normas ISO*. Obtenido de ISOTools Excellence: https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

Lara, C. (16 de Marzo de 2014). *Metodología de Evaluación de Riesgos Informáticos*. Obtenido de Blogger: http://metodologiaoctave.blogspot.com/2014/03/metodologia-octave.html

Nuño, P. (19 de Febrero de 2018). *¿Para qué sirven las Normas ISO?* Obtenido de Emprende Pyme: https://www.emprendepyme.net/para-que-sirven-las-normas-iso.html

OK HOSTING. (2016). *El Comercio electrónico*. Obtenido de OK HOSTING: https://okhosting.com/blog/el-comercio-electronico/

Parra, A. (2014). ISO 27001 para PYMES. *(Trabajo Fin de Máster).* Universidad Internacional de la Rioja, Medellín.

Tola, D. (2015). Implementación de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría y Auditoría, aplicando la Norma ISO/IEC 27001. *(Tesis de Grado).* Escuela Superior Politécnica del Litoral, Guayaquil.

Villagómez, C. (18 de Enero de 2018). *Introducción al Comercio Electrónico ('e-commerce')*. Obtenido de CCM: https://es.ccm.net/contents/201-introduccion-al-comercio-electronico-e-commerce

welivesecurity. (10 de Setiembre de 2014). *Estándares de Seguridad ISO 27000: ¿Qué hay de nuevo?* Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2014/09/10/estandares-seguridad-iso-27000-nuevo/

ANEXOS

Anexo A. Inventario de Activos de Información

N°	Activo	Tipo de Activo
1	Comprobantes de Compra y Venta	Documentación
2	Cotizaciones	
3	Lista de proveedores	
4	Planilla de colaboradores	
5	Computadora de escritorio	Hardware
6	Teléfono (fijo, celular)	
7	Impresora (Multifuncional)	
8	Cableado ethernet	
9	Router	
10	Disco Duro externo	
11	Microsoft Windows 10	Software
12	Microsoft Office 2016	
13	Antivirus	
14	Correo electrónico (Outlook)	
15	Página Web	
16	Firewall de Windows	
17	Red Wifi	
18	Administrador	Humano
19	Encargado de venta	
20	Encargado sistemas	

Anexo B. Valoración de los Activos de Información

N°	Activo	Valoración Parcial			Valor Final
		C	I	D	
1	Comprobantes de Compra y Venta	2	3	2	7
2	Cotizaciones	2	3	1	6
3	Lista de proveedores	2	3	1	6
4	Planilla de colaboradores	3	3	1	7
5	Computadora de escritorio	3	3	3	9
6	Teléfono (fijo, celular)	1	2	3	7
7	Impresora (Multifuncional)	1	2	2	5
8	Cableado ethernet	2	3	3	8
9	Router	2	3	3	8
10	Disco Duro externo	3	3	2	8
11	Microsoft Windows	1	3	3	7
12	Microsoft Office	1	2	3	6
13	Antivirus	3	3	3	9
14	Correo electrónico	2	3	3	8
15	Página Web y redes sociales	2	2	3	7
16	Firewall de Windows	1	3	3	7
17	Red Wifi	3	3	3	9
18	Administrador	1	3	2	6
19	Encargado de venta	1	3	2	6
20	Encargado sistemas	1	3	3	7

Anexo C. Mapa de Calor de Riesgos

Activo de Información	Identificación del Riesgo	Evaluación del Riesgo		
		Probabilidad	Impacto	Nivel de Riesgo
Comprobantes de Compra y Venta	Pérdida del documento por controles mínimos de acceso	3	3	**9-Medio**
Planilla de colaboradores	Mal uso de la información por falta de control de acceso y almacenamiento	2	3	**6-Medio**
Computadora de escritorio	Sustracción de la información y/o equipo por falta de políticas de control de acceso	4	4	**16-Alto**
	Falla del equipo por falta de mantenimiento	3	3	**9-Medio**
	Pérdida de la información contenida por falta de políticas de copias de seguridad	3	4	**12-Alto**
Cableado ethernet	Saturación de información entre equipos de red por una mala instalación del cableado interno	1	2	**2-Bajo**
	Interceptación de la información debido a una mala gestión de instalación	1	4	**4-Medio**
	Falla de conexión a internet por una mala instalación del cableado interno	2	4	**8-Medio**
Router	Acceso no autorizado debido a contraseñas débiles	1	4	**4-Medio**

	Filtración de información por configuraciones deficientes	1	4	**4-Medio**
	Falla en la transmisión de señal por falta de mantenimiento	3	3	**9-Medio**
Disco Duro externo	Pérdida o robo del dispositivo por inadecuado almacenamiento	3	4	**12-Alto**
	Deterioro del dispositivo por inadecuado uso	1	3	**3-Bajo**
	Pérdida de data debido a una falta de manejo de backups	2	3	**6-Medio**
Microsoft Windows	Mal funcionamiento del sistema debido a licencia no autorizada	1	3	**3-Bajo**
	Falla de acceso al sistema por mal uso	1	4	**4-Medio**
Antivirus	Falla en su diagnóstico por licencia no autorizada y/o caducada	4	4	**16-Alto**
	Ingreso de virus por mal uso del software	2	3	**6-Medio**
Correo electrónico	Filtración de correos confidenciales debido a un acceso no autorizado	1	4	**4-Medio**
	Acceso denegado debido a una mala gestión de contraseñas	3	2	**6-Medio**
Página Web y redes sociales	Filtración del código fuente debido a un acceso no autorizado	2	4	**8-Medio**

	Robo y alteración de información por falta de controles de acceso	3	4	**12-Alto**
	Modificación del código fuente debido a un mal uso del sistema	2	3	**6-Medio**
Firewall de Windows	Ingreso de códigos maliciosos debido a un manejo inadecuado del software	2	3	**6-Medio**
	Modificación en la configuración debido a un manejo inadecuado del software	2	4	**8-Medio**
Red Wifi	Filtración de información relevante debido al uso de wi fi públicos	3	4	**12-Alto**
	Acceso no autorizado debido a una débil seguridad de acceso	2	4	**8-Medio**
Encargado sistemas	Falla en la seguridad por falta de capacitación y actualización de conocimientos	3	4	**12-Alto**
	Robo de información debido a influencias negativas	1	4	**4-Medio**

Anexo D. Controles de Seguridad de la Información

Activo de Información	Riesgo	Nivel de Riesgo	Controles	
			Clausula ISO/IEC 27001	Tratamiento
Comprobantes de Compra y Venta	Pérdida del documento por controles mínimos de acceso	9-Medio	A.11.1.3 Seguridad de instalaciones	Prevenir e impedir el acceso no autorizado a ambientes o instalaciones
Planilla de colaboradores	Mal uso de la información por falta de control de acceso y almacenamiento	6-Medio	A.11.1.3 Seguridad de instalaciones	Prevenir e impedir el acceso no autorizado a ambientes o instalaciones
Computadora de escritorio	Sustracción de la información y/o equipo por falta de políticas de control de acceso	16-Alto	A.9.1.1 Políticas de control de acceso A.9.4.1. Restricción de acceso a información A.11.1.3 Seguridad de instalaciones A.11.2.1 Protección de equipos	Implementar medidas que impidan el acceso no autorizado tanto a las instalaciones u ambientes como a la información digital
	Falla del equipo por falta de mantenimiento	9-Medio	A.11.2.4 Mantenimiento de equipos	Realizar mantenimiento programado a fin de evitar fallas en el equipo
	Pérdida de la información contenida por falta de políticas de copias de seguridad	12-Alto	A.12.3.1. Copias de respaldo de la información.	Implementar Políticas de backup
Cableado ethernet	Saturación de información entre equipos de red por una mala instalación del cableado interno	2-Bajo	A.11.2.3. Seguridad del cableado	Implementar políticas de redes a fin de evitar interceptaciones, interferencias o daños a la información.
	Interceptación de la información debido a una mala gestión de instalación	4-Medio	A.11.2.3. Seguridad del cableado A.13.1.1. Controles de redes.	Implementar políticas de redes a fin de evitar interceptaciones, interferencias o daños a la información.

	Falla de conexión a internet por una mala instalación del cableado interno	**8-Medio**	A.11.2.3. Seguridad del cableado	Implementar políticas de redes a fin de evitar interceptaciones, interferencias o daños a la información.
Router	Acceso no autorizado debido a contraseñas débiles	**4-Medio**	A.9.1.2. Acceso a redes y a servicios en red	Implementar políticas de redes que permitan un acceso autorizado
	Filtración de información por configuraciones deficientes	**4-Medio**	A.11.2.3. Seguridad del cableado A.13.1.1. Controles de redes.	Implementar políticas de redes a fin de evitar interceptaciones, interferencias o daños a la información.
	Falla en la transmisión de señal por falta de mantenimiento	**9-Medio**	A.11.2.2. Servicios Públicos de soporte A.11.2.4 Mantenimiento de equipos	Establecer políticas de seguridad física y un mantenimiento programado a fin de evitar interrupciones por fallas en el equipo
Disco Duro externo	Pérdida o robo del dispositivo por inadecuado almacenamiento	**12-Alto**	A.11.1.3 Seguridad de instalaciones	Implementar medidas que impidan el acceso no autorizado instalaciones u ambientes
	Deterioro del dispositivo por inadecuado uso	**3-Bajo**	A.8.1.3. Uso Aceptable de los Activos A.11.2.4 Mantenimiento de equipos	Realizar mantenimiento periódico a fin de evitar fallas en el dispositivo
	Pérdida de data debido a una falta de manejo de backups	**6-Medio**	A.12.3.1. Copias de respaldo de la información.	Implementar Políticas de backup
Microsoft Windows	Mal funcionamiento del sistema debido a licencia no autorizada	**3-Bajo**	A.14.2.9. Pruebas de aceptación de sistemas	Realizar pruebas de funcionamiento del software
	Falla de acceso al sistema por mal uso	**4-Medio**	A.9.1.1 Políticas de control de acceso A.8.1.3. Uso Aceptable de los Activos	Establecer medidas de acceso autorizado y reglas para un adecuado uso del sistema
Antivirus	Falla en su diagnóstico por licencia no autorizada y/o caducada	**16-Alto**	A.14.2.9. Pruebas de aceptación de sistemas	Realizar pruebas de funcionamiento del software
	Ingreso de virus por mal uso del software	**6-Medio**	A.9.1.1 Políticas de control de acceso A.8.1.3. Uso Aceptable de los Activos A.12.2.1. Controles contra códigos maliciosos	Establecer medidas de acceso autorizado y reglas para un adecuado uso del sistema

Correo electrónico	Filtración de correos confidenciales debido a un acceso no autorizado	**4-Medio**	A.9.1.1 Políticas de control de acceso A.13.2.3. Mensajes electrónicos	Implementar políticas de control de acceso y de seguridad en la transmisión de información a través del correo electrónico
	Acceso denegado debido a una mala gestión de contraseñas	**6-Medio**	A.7.1.2. Términos y condiciones del empleo	Establecer responsabilidades en el manejo idóneo del rol asignado
Página Web y redes sociales	Filtración del código fuente debido a un acceso no autorizado	**8-Medio**	A.9.1.1 Políticas de control de acceso	Implementar políticas de control de acceso
	Robo y alteración de información por falta de controles de acceso	**12-Alto**	A.9.1.1 Políticas de control de acceso	Implementar políticas de control de acceso
	Modificación del código fuente debido a un mal uso del sistema	**6-Medio**	A.9.1.1 Políticas de control de acceso A.8.1.3. Uso Aceptable de los Activos A.12.2.1. Controles contra códigos maliciosos	Establecer medidas de acceso autorizado y reglas para un adecuado uso del sistema
Firewall de Windows	Ingreso de códigos maliciosos debido a un manejo inadecuado del software	**6-Medio**	A.8.1.3. Uso Aceptable de los Activos A.12.2.1. Controles contra códigos maliciosos	Establecer reglas para un adecuado uso del sistema
	Modificación en la configuración debido a un manejo inadecuado del software	**8-Medio**	A.7.1.2. Términos y condiciones del empleo	Establecer responsabilidades en el manejo idóneo del rol asignado
Red Wifi	Filtración de información relevante debido al uso de wifi públicos	**12-Alto**	A.9.4.2. Procedimiento de Conexión Segura	Implementar políticas de redes que permitan realizar conexiones seguras
	Acceso no autorizado debido a una débil seguridad de acceso	**8-Medio**	A.9.1.2. Acceso a redes y a servicios en red	Implementar políticas de redes que permitan un acceso autorizado
Encargado sistemas	Falla en la seguridad por falta de capacitación y actualización de conocimientos	**12-Alto**	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información	Implementar Políticas de Personal que permitan al colaborador compromiso con la seguridad de la información
	Robo de información debido a influencias negativas	**4-Medio**	A.7.1.2. Términos y condiciones del empleo A.7.2.3. Proceso disciplinario.	Establecer responsabilidades en el manejo correcto de la información

Anexo E. Cronograma del Proyecto

Actividad	Agosto				Setiembre				Octubre				Noviembre				Diciembre				Enero				Febrero				Total semanas
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
1. Diagnosticar los procesos operacionales del comercio elctronico de la PYME	x	x																											2
2.Determinar los puntos sensibles de seguridad			x																										1
3. Identificar los Activos Principales de Información				x																									1
4. Valorizar los Activos				x																									1
5. Identificar los Riesgos principales de seguridad					x	x																							2
6. Elaborar una Matriz de calor de Riesgos							x	x																					2
7. Diagnosticar los Riesgos									x	x																			2
8. Determinar las Políticas de Seguridad											x	x	x																3
9. Determinar los Controles de Seguridad														x	x	x													3
10. Implementación del Plan																	x	x	x	x	x	x	x	x					8
11. Seguimiento y Control del Plan de Seguridad	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	28

Anexo F. Costo Bruto de los Controles de Seguridad a Implementar

Activo de Información	Controles		Costo	
	Clausula ISO/IEC 27001	Tratamiento	Descripción del costo	Valor (S/.)
Comprobantes de Compra y Venta	A.11.1.3 Seguridad de instalaciones	Prevenir e impedir el acceso no autorizado a ambientes o instalaciones	Instalación de un lector de huella digital y de mueble de oficina seguro	1400.00
Planilla de colaboradores	A.11.1.3 Seguridad de instalaciones	Prevenir e impedir el acceso no autorizado a ambientes o instalaciones	Instalación de un lector de huella digital y de mueble de oficina seguro	1400.00
Computadora de escritorio	A.9.1.1 Políticas de control de acceso A.9.4.1. Restricción de acceso a información A.11.1.3 Seguridad de instalaciones A.11.2.1 Protección de equipos	Implementar medidas que impidan el acceso no autorizado tanto a las instalaciones u ambientes como a la información digital	Instalación de un lector de huella digital y claves de acceso seguro	1200.00
	A.11.2.4 Mantenimiento de equipos	Realizar mantenimiento programado a fin de evitar fallas en el equipo	Diagnósticos y reparaciones de equipos	3000.00
	A.12.3.1. Copias de respaldo de la información.	Implementar Políticas de backup	Copias periódicas en la PC y unidad externa	700.00
Cableado ethernet	A.11.2.3. Seguridad del cableado	Implementar políticas de redes a fin de evitar interceptaciones interferencias o daños a la información.	Diagnósticos y reparaciones de los equipos de red	2000.00

	A.11.2.3. Seguridad del cableado A.13.1.1. Controles de redes.	Implementar políticas de redes a fin de evitar interceptaciones interferencias o daños a la información.	Instalaciones seguras de cableado y equipo de red	2250.00
	A.11.2.3. Seguridad del cableado	Implementar políticas de redes a fin de evitar interceptaciones interferencias o daños a la información.	Instalaciones seguras de cableado y equipo de red	2250.00
Router	A.9.1.2. Acceso a redes y a servicios en red	Implementar políticas de redes que permitan un acceso autorizado	Creación de accesos seguros	2000.00
	A.11.2.3. Seguridad del cableado A.13.1.1. Controles de redes.	Implementar políticas de redes a fin de evitar interceptaciones interferencias o daños a la información.	Instalaciones seguras de cableado y equipo de red	2000.00
	A.11.2.2. Servicios Públicos de soporte A.11.2.4 Mantenimiento de equipos	Establecer políticas de seguridad física y un mantenimiento programado a fin de evitar interrupciones por fallas en el equipo	Diagnósticos y reparaciones de equipos	2000.00
Disco Duro externo	A.11.1.3 Seguridad de instalaciones	Implementar medidas que impidan el acceso no autorizado a instalaciones u ambientes	Implementación de un lector de huella digital y de mueble de oficina seguro	1250.00
	A.8.1.3. Uso Aceptable de los Activos A.11.2.4 Mantenimiento de equipos	Realizar mantenimiento periódico a fin de evitar fallas en el dispositivo	Diagnósticos y reparaciones de equipos	2000.00
	A.12.3.1. Copias de respaldo de la información.	Implementar Políticas de backup	Copias periódicas en la PC y unidad externa	700.00
Microsoft Windows	A.14.2.9. Pruebas de aceptación de sistemas	Realizar pruebas de funcionamiento del software	Diagnósticos y reparaciones de equipos	2000.00
	A.9.1.1 Políticas de control de acceso A.8.1.3. Uso Aceptable de los Activos	Establecer medidas de acceso autorizado y reglas para un adecuado uso del sistema	Capacitación periódica	500.00
Antivirus	A.14.2.9. Pruebas de aceptación de sistemas	Realizar pruebas de funcionamiento del software	Instalación de antivirus con licencia original	600.00

	A.9.1.1 Políticas de control de acceso A.8.1.3. Uso Aceptable de los Activos A.12.2.1. Controles contra códigos maliciosos	Establecer medidas de acceso autorizado y reglas para un adecuado uso del sistema	Capacitación periódica	500.00
Correo electrónico	A.9.1.1 Políticas de control de acceso A.13.2.3. Mensajes electrónicos	Implementar políticas de control de acceso y de seguridad en la transmisión de información a través del correo electrónico	Capacitación periódica	500.00
	A.7.1.2. Términos y condiciones del empleo	Establecer responsabilidades en el manejo idóneo del rol asignado	Capacitación periódica	500.00
Página Web y redes sociales	A.9.1.1 Políticas de control de acceso	Implementar políticas de control de acceso	Creación de accesos seguros	2500.00
	A.9.1.1 Políticas de control de acceso	Implementar políticas de control de acceso	Creación de accesos seguros	2500.00
	A.9.1.1 Políticas de control de acceso A.8.1.3. Uso Aceptable de los Activos A.12.2.1. Controles contra códigos maliciosos	Establecer medidas de acceso autorizado y reglas para un adecuado uso del sistema	Capacitación periódica y creación de accesos seguros	500.00
Firewall de Windows	A.8.1.3. Uso Aceptable de los Activos A.12.2.1. Controles contra códigos maliciosos	Establecer reglas para un adecuado uso del sistema	Capacitación periódica y creación de accesos seguros	500.00
	A.7.1.2. Términos y condiciones del empleo	Establecer responsabilidades en el manejo idóneo del rol asignado	Capacitación periódica y creación de accesos seguros	500.00
Red Wiffi	A.9.4.2. Procedimiento de Conexión Segura	Implementar políticas de redes que permitan realizar conexiones seguras	Instalaciones seguras de cableado y equipo de red	2000.00
	A.9.1.2. Acceso a redes y a servicios en red	Implementar políticas de redes que permitan un acceso autorizado	Instalaciones seguras de cableado y equipo de red	2000.00
Encargado sistemas	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información	Implementar Políticas de Personal que permitan al colaborador compromiso con la seguridad de la información	Capacitación periódica	500.00

	A.7.1.2. Términos y condiciones del empleo A.7.2.3. Proceso disciplinario.	Establecer responsabilidades en el manejo correcto de la información	Charlas de concientización por parte de la Alta Dirección	1500.00
Costo Bruto Total				**41250.00**

Anexo G. Anexo A de la Norma ISO/IEC 27001:2013

ISO/IEC 27001:2013 -ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
A.5. POLÌTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.
	Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
	Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.
		A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.
		A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
		A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto.
	A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
	Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
	A.7.1. Antes de asumir el empleo.	A.7.1.1. Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.
	A.7.2. Durante la ejecución del empleo.	A.7.2.1. Responsabilidades de la Dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.
	Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
		A.7.2.3. Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
	A.7.3. Terminación y cambio de empleo.	A.7.3.1. Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
	Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	
	A.8.1. Responsabilidad por los Activos.	A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
	Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.
		A.8.1.3. Uso Aceptable de los Activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
		A.8.1.4. Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

A.8. GESTIÒN DE ACTIVOS.	A.8.2. Clasificación de la Información.	A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificacion no autorizada.
	Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organizacion.	A.8.2.2. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
		A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
	A.8.3. Manejo de medios de soporte.	A.8.3.1. Gestión de medios de Soporte Removibles. Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
	Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.	A.8.3.2. Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.
		A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
	A.9.1. Requisitos del Negocio para Control de Acceso.	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
	Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.2. Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
	A.9.2. Gestión de Acceso de Usuarios.	A.9.2.1. Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.
	Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	A.9.2.2. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
		A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
		A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestion formal.

A.9. CONTROL DE ACCESO.		A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.
		A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A.9.3. Responsabilidades de los usuarios.	A.9.3.1. Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
	Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.	
	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.1. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexion segura.
		A.9.4.3. Sistema de Gestión de Contraseñas. Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
		A.9.4.4. Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
		A.9.4.5. Control de Acceso a Códigos Fuente de Programas. Se debe restringir el acceso a códigos fuente de programas.
A.10. CRIPTOGRAFÍA	A.10.1. Controles Criptográficos.	A.10.1.1. Política sobre el uso de controles Criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.
	Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	A.10.1.2. Gestión de Claves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.

A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.1. Áreas Seguras.	A.11.1.1. Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
	Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.2. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
		A.11.1.3. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.
		A.11.1.4. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
		A.11.1.5. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
		A.11.1.6. Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
	A.11.2. Equipos.	A.11.2.1. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.
	Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.2. Servicios Públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.

		A.11.2.3. Seguridad del cableado. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.
		A.11.2.4. Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
		A.11.2.5. Retiro de Activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
		A.11.2.6. Seguridad de equipos y activos fuera del predio. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de
		A.11.2.7. Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o rehúso.
		A.11.2.8. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.
		A.11.2.9. Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.
	A.12.1. Procedimientos operacionales y responsabilidades.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.
	Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.2. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
		A.12.1.3. Gestión de Capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeno requendo del sistema.
		A.12.1.4. Separación de los ambientes de desarrollo, ensayo y operación. Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.
	A.12.2. Protección contra códigos maliciosos.	A.12.2.1. Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

A.12. SEGURIDAD DE LAS OPERACIONES.	Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	
	A.12.3. Copias de Respaldo.	A.12.3.1. Copias de respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
	Objetivo. Proteger contra la pérdida de datos.	
	A.12.4. Registro y Seguimiento.	A.12.4.1. Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.
	Objetivo. Registrar eventos y generar evidencia.	A.12.4.2. Protección de la información de registro. Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
		A.12.4.3. Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.
		A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
	A.12.5. Control de Software Operacional.	A.12.5.1. Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
	Objetivo. Asegurarse de la integridad de los sistemas operacionales.	
	A.12.6. Gestión de vulnerabilidad técnica.	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
	Objetivo. Prevenir el aprovechamiento de las vulnerabilidades tecnicas.	A.12.6.2. Restricciones sobre la instalación de Software. Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.
	A.12.7. Consideraciones sobre auditorías de sistemas de información.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
	Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.	

A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.1. Gestión de Seguridad de Redes.	A.13.1.1. Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
	Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.2. Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
		A.13.1.3. Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
	A.13.2. Transferencia de información.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.
	Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.2. Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
		A.13.2.3. Mensajes electrónicos. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.
		A.13.2.4. Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
	A.14.1. Requisitos de seguridad de los sistemas de información.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
	Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.	A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
		A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.
	A.14.2. Seguridad en los procesos de desarrollo y de soporte.	A.14.2.1. Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.

A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.2. Procedimiento de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización.
		A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.
		A.14.2.4. Restricciones sobre los cambios de paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
		A.14.2.5. Principios de construcción de sistemas de seguros. Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.
		A.14.2.6. Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
		A.14.2.7. Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.
		A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.
		A.14.2.9. Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.
	A.14.3. Datos de ensayo.	A.14.3.1. Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.
	Objetivo. Asegurar la protección de los datos usados para ensayos.	
	A.15.1. Seguridad de la información en las relaciones con los proveedores.	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
	Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

A.15. RELACIONES CON LOS PROVEEDORES.		A.15.1.3. Cadena de suministro de tecnología de información y comunicación. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
	A.15.2. Gestión de la prestación de servicios de proveedores.	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
	Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	A.15.2.2. Gestión de cambios a los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
	Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.	A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.
		A.16.1.3. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
		A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
		A.16.1.5. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
		A.16.1.7. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
	A.17.1. Continuidad de seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.

A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organizacion.	A.17.1.2. Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los validos y eficaces durante situaciones adversas.
	A.17.2. Redundancia	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
	Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.	
A.18. CUMPLIMIENTO.	A.18.1. Cumplimiento de requisitos legales y contractuales.	A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.
	Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.2. Derechos de Propiedad Intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.
		A.18.1.3. Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
		A.18.1.4. Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.

		A.18.1.5. Reglamentación de Controles Criptográficos. Se deben usar controles criptograficos, en cumplimiento de todos los acuerdos
	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
	Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.	A.18.2.2. Cumplimiento con las políticas y normas de seguridad. Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.
		A.18.2.3. Revisión del Cumplimiento Técnico. Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.