PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE MANABI

CARRERA DE ADMINISTRACIÓN DE EMPRESAS

TEMA:

“GESTIÓN DE LA INFORMACIÓN DE LAS EMPRESAS CONSTRUCTORAS: CASO VENTAS FORTE S.A’’

PREVIO AL TÍTULO DE:

INGENIERO EN ADMINISTRACIÓN DE EMPRESAS

AUTOR:

EMMANUEL AGUSTÍN MOREJÓN LÓPEZ

DIRECTOR DEL TRABAJO DE TITULACIÓN:

MGTR. NEIL EDUARDO BRITO PARDO

DICIEMBRE, 2022

PORTOVIEJO - ECUADOR

Certificación

Mgtr. Neil Eduardo Brito Pardo

Tutor del Proyecto de Grado

Certifica:

En mi calidad de tutor del trabajo de integración curricular, certifico haber revisado el presente manuscrito de investigación, el mismo que se ajusta a las normas vigentes de la carrera de Ingeniería Administración de Empresas de la Pontificia Universidad Católica del Ecuador, Sede Manabí, cumpliendo la Normativa del Trabajo de Integración Curricular; en consecuencia, es apto para su presentación y sustentación.

……..….

Mgtr. Neil Eduardo Brito Pardo

Aprobación del Tribunal

El jurado examinador aprueba el presente trabajo de integración curricular en nombre de la Pontificia Universidad Católica del Ecuador, Sede Manabí.

(f)_____ (f)_____

(f)_____

Autoría

Éste manuscrito no contiene ningún tipo de material que ha sido aceptado para la obtención de un título universitario en otra institución, excepto en forma de información de soporte que ha sido debidamente citada en mi trabajo. Este trabajo es de total responsabilidad del autor, quien declara bajo juramento que ninguna sección de este trabajo de integración curricular infringe los derechos de autor de nadie.

……..……

Emmanuel Agustín Morejón López

C.I. 131176325

Declaración de Derechos de Autor

Autorizo a la Pontificia Universidad Católica del Ecuador a distribuir este manuscrito de investigación en medios físicos y electrónicos con el fin de promover la divulgación de mis resultados a la comunidad científica y a la sociedad en general. Adicionalmente autorizo el uso de los contenidos de esta investigación como bibliografía para fines académicos, por cualquier medio o procedimiento, citando como fuente de información al autor de este trabajo.

Fecha: …….

Firma: …….

Dedicatoria

Dedico este proyecto a Dios por su infinito amor y por haberme acompañado todo este tiempo en mi camino, dándome la fortaleza para culminar con éxito mi trabajo de titulación.

A mis padres, pilares fundamentales en mi vida, quienes me han apoyado de manera incondicional, depositando toda su confianza en los obstáculos que se me han presentado, como también, por darme la fuerza y consejos para lograr cumplir mis metas planteadas.

Emmanuel Agustín Morejón López

Agradecimientos

Agradezco a Dios, por ser guía en mi camino y por concederme salud y bendiciones, lo que me ha permitido llegar a la meta que es la finalización de mi trabajo de tesis.

A mis padres, Ing. Wilmer Morejón y Vielka López, quienes me han apoyado en todos los momentos difíciles de mi vida, y con su sabiduría y consejos me han orientado para superar cada obstáculo en mi vida personal y profesional.

Un agradecimiento especial a mi Tutor de Tesis, Mgtr. Neil Eduardo Brito Pardo, por la guía brindada, quien con su conocimiento, experiencia y motivación me ha permitido desarrollar y terminar con éxito mi proyecto de investigación.

Emmanuel Agustín Morejón López

Resumen

El presente estudio de tipo cualitativo y propositivo, describe un plan de gestión para salvaguardar la información y procedimientos dentro de la ejecución de los contratos civiles ejecutados en la empresa constructora Ventas Forte S.A. En relación al alcance, el trabajo es explicativo y exploratorio, ya que analiza los riesgos que ocasiona a la empresa la inseguridad con que se maneja la información. El proceso de investigación se desarrolló en Portoviejo desde septiembre 2021 a enero 2022. Para el estudio de campo se seleccionaron técnicas como recopilación de información localizada, verificación del problema y posibles soluciones aplicando el "Ciclo *Deming*", lo que sirvió para determinar mediante el análisis de estrategias, el tipo de infraestructura de organización, así como valoración de activos y evaluación de riesgos, permitiendo la implementación de un plan de tratamiento de riesgo y selección de acciones de control según la norma ISO 27001. Los resultados obtenidos del 9,09% de riesgo alto y el 54.54% de riesgo medio, han sido mitigados cambiando el estado de algunos activos a riesgo medio y a riesgo bajo. La empresa logra continuidad de negocios basados en planes de contingencia; la imagen de su organización mejora y su valor en el mercado asciende. La incorporación del sistema de seguridad ISO 27001 permite a esta empresa mejorar su infraestructura tecnológica y llevar un adecuado control en la manipulación de los equipos y herramientas informática, además que genera más confianza entre el cliente y la empresa, disminuyendo la amenaza de pérdida o robo de información.

Palabras clave: seguridad de la información, gestión, riesgos, activos, mitigación

Abstract

This qualitative research study described a data management plan to protect information and procedures when executing civil engineering work contracts at *Ventas Forte S.A.* Construction Company, in Portoviejo, by analyzing the risks that information security threats may cause to any company. Accordingly, this explanatory-exploratory research study was carried out from September 2021 through January 2022. In order to conduct field study, localized information, problem verification and possible solutions were collected by applying the "Deming Cycle" to make it possible to determine through strategic analysis, the type of organizational structure, asset valuation and risk assessment that help implement a risk treatment plan, as well as the selection of controls as per ISO 27001 standard. The findings reveal 9.09% high risk and 54.54% medium risk, which have been mitigated, changing the status of some assets to medium risk and low risk. This company achieves business continuity from contingency plans; it improves its organizational image; and it increases its market value. ISO 27001 information security management system implementation improves this company's technical infrastructure by generating adequate control when working with computer tools and equipment; building more customer trust; and reducing information security threats. In conclusion, the implementation of this policy management and application system does improve information security and effectiveness of documentary procedures.

Keywords: information security, management, risks, assets, mitigation

Tabla de Contenidos

Índice de Tablas

GESTIÓN DE LA INFORMACIÓN

GESTIÓN DE LA INFORMACIÓN

1. Introducción

Hoy en día tener una empresa sin un sistema de gestión de la información representa un riesgo para su estabilidad. Actualmente se pudo referir a varios modelos de sistemas de gestión dentro de una organización, siendo una de estas normativas la Organización Internacional de Normalización, siglas en inglés ISO, las cuales presentan varias ramas que permiten estar encaminados a la Calidad, Gestión Ambiental, Sanidad y Seguridad Alimentaria, Seguridad de la Información, entre otras alternativas específicas.

El riesgo de que una empresa pierda toda su información es un escenario que muchas veces se toma en cuenta cuando ya es muy tarde, esto suele suceder por las tareas diarias acumuladas y la rutina de trabajos. Sin embargo, es una situación que puede evitarse considerando que ahora es muy común que toda o la gran parte de la documentación se maneje de manera digital, existiendo riesgos de pérdida por error, hackeo, robo o bloqueo de información.

Dentro de una empresa constructora con interés de salvaguardar los documentos no solo de manera física sino digital, se referencia la normativa ISO 27001 para la Seguridad de la información la cual objeta mantener segura la confidencialidad, integridad y disponibilidad de la información, conocida como un SGSI. Fundamentado en la teoría de gestión de la calidad PDCA, por su estructura básica que consiste en: Planificar, Hacer, Verificar y Actuar. (Universidad Internacional de la Rioja, 2019).

De esta manera el presente proyecto propone una alternativa para el uso y gestión de una herramienta basada en las necesidades de salvaguardar la información de una entidad constructora; y a su vez crear un plan de sistema de gestión de información que permita optimizar los recursos y ejecutarlos de manera eficaz.

1.2 Antecedentes

La Sociedad Ventas Forte S.A nace como persona jurídica con fecha 24 de junio de 2010 en la ciudad de Guayaquil, Ecuador, siendo su principal actividad la construcción tanto para empresas públicas y privadas.

La constructora cuenta con personal administrativo y técnico especializado para el control y ejecución de obras civiles.

Debido a que la empresa Ventas Forte S.A. no amerita mayor espacio infraestructural por sus labores principalmente de carácter técnico en campo, sujetas a la realización de los trabajos objetos de sus contratos que difieren según el tipo de obra a ejecutar, la misma no necesita mayor espacio para albergar la información, más si es necesario manifestar que los equipos informáticos utilizados principalmente por el personal administrativo corresponde a equipos computacionales y dispositivos periféricos técnicos de alto valor por la necesidad de generar y almacenar grandes volúmenes de información y, adicionalmente, la seguridad de los datos es un factor predominante y de imperativo interés dentro de la empresa por los elevados costos y cuantías que pueden adquirir estos.

1.3 Objetivos

1.3.1 Objetivo General

- Desarrollar un plan de gestión para la seguridad de la información y la optimización de los recursos y procedimientos dentro de la ejecución de los contratos civiles ejecutados por la empresa constructora VENTAS FORTE S.A ubicada en la ciudad de Portoviejo

1.3.2 Objetivos Específicos

- Identificar y Valorizar los activos de información y la infraestructura tecnológica de la empresa Constructora Ventas Forte S.A., aplicando el modelo PDCA (*Plan, Do, Check, Act)* para el diagnóstico situacional, con la finalidad de evaluar los riesgos y evitar la materialización de amenazas.
- Determinar las políticas de seguridad basadas en la Norma ISO 27001.
- Evaluar un sistema de seguridad de información en la empresa Ventas Forte S.A. basados en las normas ISO 27001, para asegurar la continuidad de las operaciones y mejorar la calidad del servicio que brinda la empresa.
- Analizar la eficacia mediante un sistema de control a las mejoras continuas que se darán a través del desarrollo del sistema virtual (Plataforma web) durante el proceso de optimización en la empresa constructora Ventas Forte S.A.

1.4 Alcance

Este proyecto tiene como alcance generar un análisis sobre el rango de seguridad de la información de la empresa Ventas Forte S.A., basado en la evaluación de sus activos y herramientas informáticas, para posteriormente determinar los riesgos a los que se expongan frente al estándar ISO/IEC 27001:2013. Con base en estos resultados identificar los requerimientos y controles de seguridad más apropiados para la empresa acorde a las necesidades de la empresa; y, finalmente se establecerán la documentación y procedimientos requeridos como parte de la implementación de un Sistema de Gestión de Seguridad de la Información.

2. Materiales y Métodos

2.1 Materiales

La información y los datos son uno de los principales activos de las organizaciones. La protección de su seguridad y privacidad es una tarea fundamental para asegurar el correcto desarrollo del negocio, trasladando confianza a los stakeholders, clientes y usuarios. Cuanto mayor es el valor de la información y su privacidad, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada como consecuencia de una incidencia/brechas de seguridad/privacidad. (Seguridad y Privacidad de la información, 2021)

Para el desarrollo de este trabajo, fue utilizada la información proporcionada por la Empresa Ventas Forte S.A., tanto de sus clientes y trabajadores, como: contratos, fiscalización, planos,

pagos de nóminas, presupuesto, entre otros.

En la búsqueda de información se identificó los activos de la empresa Ventas Forte S.A, que incluían recursos inherentes con la gestión e intercambio de información, como vías de comunicación, hardware, documentación digital, software y manual e incluso de recursos humanos, a fin de realizar un análisis de riesgo informático.

Fue necesario el uso y aplicación de las ISO 27001. Norma internacional de la Organización Internacional de Normalización (ISO), que describe cómo gestionar la seguridad de la información en una empresa, con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal. (Dejan, 2021)

Figura 1. ***Sistema de Gestión de la Seguridad de la Información (SGSI).*** El gráfico representa los tres aspectos que garantiza la seguridad de la información de una empresa según ISO 27001. Adaptado de Lisot, Tu empresa de mantenimiento Informático y ciberseguridad, 2018, https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/#

GESTIÓN DE LA INFORMACIÓN

Con la implantación de la norma ISO 27001 en la empresa constructora Ventas Forte S.A. se plantearon los siguientes beneficios:

- Disminuir el impacto de los riesgos, ya que de materializarse las amenazas, estas pueden representar pérdidas de facturación, de oportunidades de negocio, de capital, sanciones legales, entre otros.
- Asegurar la constancia del negocio según el plan de contingencias.
- Mejorar la imagen de la organización e incrementar el valor comercial de la empresa.
- Aumentar el nivel de confianza de los proveedores, clientes, socios y accionistas.
- Mejorar el retorno de inversiones, al tener mejor criterio según los riesgos residuales aceptados y ahorro del tiempo, dinero debido a la reducción o supresión de actividades o inversiones de escasa o nula aplicabilidad.

Como material del estudio se utilizó el contexto de un Sistema de Gestión de Seguridad de la información (SGSI), que protege a la empresa contra amenazas que se presentan en su entorno y daños ocasionados por agentes externos o internos; siendo parte de la gestión global del riesgo en una empresa, por lo cual implementan políticas, aplican controles y procedimientos organizacionales y desarrollan o manejan aplicaciones de *software*. Hay aspectos que se aplican con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información.

En este contexto, (Seguridad de la Información, 2020) afirma que si los trabajadores de una empresa no participan en el Sistema de Gestión de Seguridad de la Información, se puede incrementar el riesgo que se produzca un incidente de seguridad que pueda generar

consecuencias, como: posibles pérdidas financieras, daños a la reputación de la empresa, reducción de la productividad, pérdida de oportunidad y competitividad en el mercado y penalizaciones económicas por incumplimiento de legislación vigente.

La implementación del Proceso de Gestión de Riesgos en la empresa Ventas Forte S.A, para valorar los riesgos de seguridad de información, con la aplicación de la metodología Margerit, permitirá que las autoridades tomen las decisiones correctas tomando en cuenta los riesgos derivados del uso de tecnologías de la información. (Margerit - versión 3.0, 2012)

La gestión de riesgo tiene como finalidad garantizar la seguridad de los datos, aplicar políticas previamente definidas en niveles de autorización de acceso e identificar las amenazas. Los Sistemas de Gestión de Seguridad de la información están fundamentadas en la certificación Internacional ISO/IEC 27001, el que presenta vulnerabilidades y riesgos informáticos.

Otra herramienta que se aplicó para la administración de información es el *software Amazon WorkDocs,* el cual es un servicio dirigido para empresas especialmente para el almacenamiento y uso compartido de la información digital. Completamente administrado bajo controles administrativos y funciones de comentarios que mejoran la productividad de los usuarios. Los archivos se almacenan en la nube de forma segura. Los archivos de sus usuarios solo están visibles para ellos y los colaboradores y espectadores designados. Otros miembros de la organización no tienen acceso a ningún otro archivo de usuario, salvo que se les haya concedido acceso específicamente. (AWS, 2021)

La implementación de la herramienta *Amazon WorkDocs* en la empresa Ventas Forte S.A., permitirá que el administrador del *software* pueda dar soporte a los clientes, compartir contenido, realizar comentarios enriquecedores y editar documentos de manera colaborativa. Cabe indicar, que los beneficios que tendrá la empresa constructora son la seguridad de información en la nube, colaboración eficiente en tiempo real, y reducción de costos a través del pago por las cuentas de usuarios activa y el almacenamiento que utilice.

2.2 Metodología

Esta investigación, de tipo exploratoria va a confrontar la teoría con la práctica. Según (SurveyMonkey, 2021) el método exploratorio se centra en el descubrimiento de ideas y percepciones en lugar de recopilar datos estadísticos precisos. Por este motivo, la investigación exploratoria es ideal como primer paso en un plan global de investigación. Se usa comúnmente para definir con mayor profundidad los problemas de una empresa, las áreas de crecimiento potencial, las medidas alternativas que se pueden tomar y para priorizar las áreas que requieren investigación estadística

En el contexto de la metodología, se utilizó la investigación de campo, debido a que es necesario acudir a la fuente del problema y observar, a través de la adquisición de información localizada, la verificación del problema y posibles soluciones mediante el plan que será aplicado y ejecutado de manera experimental con el fin de materializar los objetivos de la investigación. Como lo indica (Vallejo, 2002) en relación al diseño de investigación.

GESTIÓN DE LA INFORMACIÓN

Para la implementación de la norma ISO 27001, el cual tiene como enfoque la mejora continua, se utilizó la metodología PDCA (*Plan, Do, Check y Act*), por la experiencia de su uso en la implementación de esta norma, además, del enfoque a procesos que brinda, es la más utilizada por la ISO.

Según (Maurice, 2017), el circulo de Deming tiene como herramienta principal lograr la mejora continua en los procesos de las organizaciones reflejando un sistema de gestión.

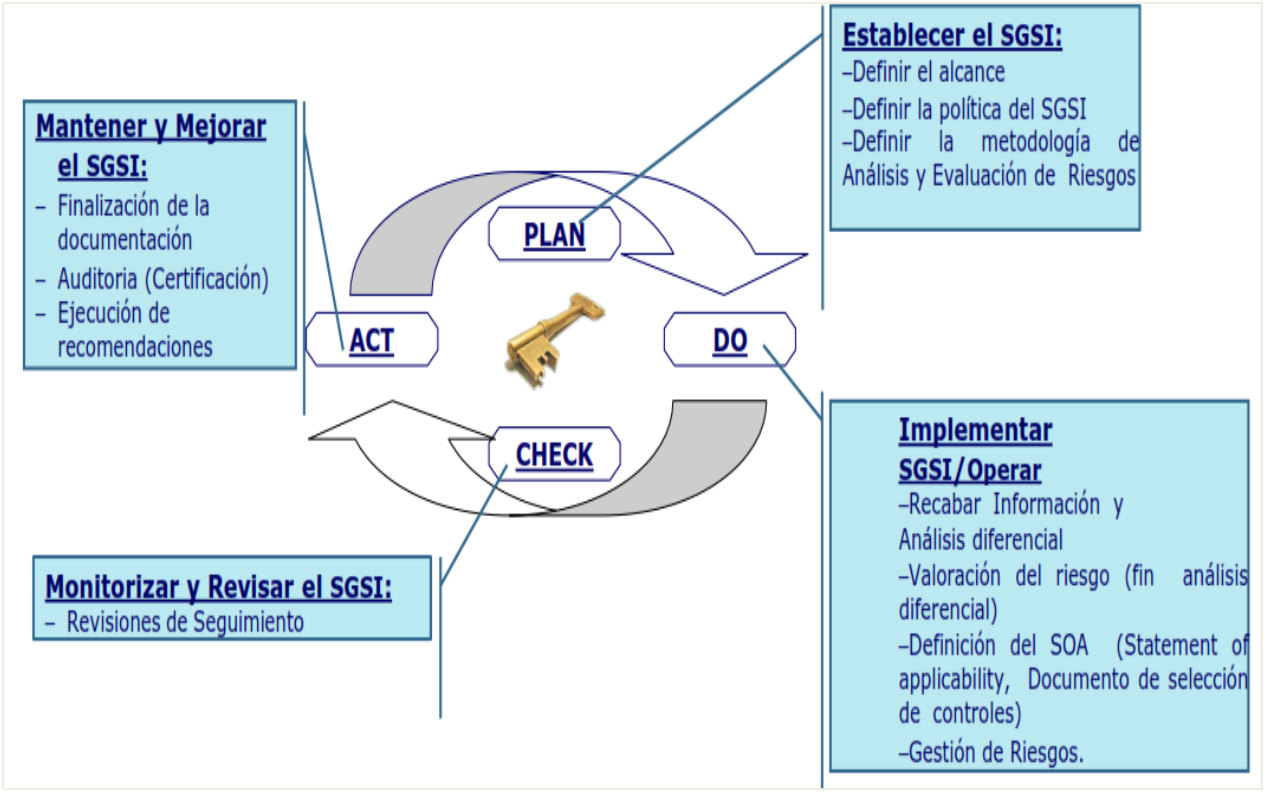

Figura 2. Modelo PDCA (Plan, Do, Check y Act) ISO 27001. El gráfico representa los niveles del modelo PDCA para la Implantación de un SGSI (Sistema de Gestión de la Seguridad de la Información). Adaptado de la Guía ISO 27001 (p. 13), por Brito N., PUCE.

2.2.1 Descripción de los pasos para el desarrollo e implementación del SGSI

Plan (Planificar)

- Obtención del soporte Directivo, existe el respaldo de la dirección Administrativa de la empresa.
- Alcance del SGSI, consiste en tomar en cuenta varias actividades como: características de los procesos de captura y procesamiento de datos y políticas del SGSI.
- Inventario de los Activos de la información, son los activos registrados en la empresa que incide en el impacto de los resultados obtenidos.
- Metodología de Gestión de Riesgos, se analiza el grado de exposición de riesgo que puede causar daños o perjuicios a los activos de la empresa. En esta etapa se considera la Metodología Margerit,
- Identificación de controles aplicables de la ISO 27001.

Do (Hacer)

Luego de identificar los riesgos, controles y activos de información, se procede con la implementación, como se detalla a continuación:

- Implementación del Plan de Tratamiento de riesgos, sirve para alcanzar los objetivos de control identificados anteriormente, mediante la asignación de recursos y responsabilidades en función de prioridades de seguridad de información.
- Implementación de Controles.
- Definición de un sistema de medición de efectividad de los controles.
- Gestión de las operaciones del SGSI.

Check (Revisar)

Esta fase sirve para analizar los resultados obtenidos luego de implementar los controles para el manejo de riesgo, lo que incluye:

- Revisión del cumplimiento
- Revisión periódica de la efectividad del SGSI
- Valoración Pre-Certificación
- Ejecución de auditorías internas periódicas del SGSI
- Registro de eventos de seguridad de información.

Act (Actuar)

En esta parte de harán correcciones o actualizaciones, según sea el caso:

- Actualización de los planes de seguridad en función de cambios y/o nuevos eventos.
- Implementación de mejoras, tomando en cuenta proyecciones de la realidad del entorno donde se desarrolla el proceso.
- Ejecución de medidas preventivas y/o correctivas para la seguridad de la información.
- Revisión de resultados sobre las mejoras implementadas.

3. Resultados

Los resultados de los análisis obtenidos en la presente investigación, tiene como importancia determinar que tanto contribuye un sistema de gestión basado en la Norma ISO 27001 en la seguridad de la información, y si influye o no dentro de las políticas de seguridad para salvaguardar la confidencialidad, integridad y disponibilidad del mismo.

GESTIÓN DE LA INFORMACIÓN

La empresa Ventas Forte S.A. cuenta con personal administrativo y técnico para la realización de las obras; dentro de su infraestructura cuenta con equipos informáticos y maquinarias para la construcción, y con relación a la información que maneja almacena información de los clientes y trabajadores.

En el análisis de riesgo, en primera instancia hay que determinar los activos de la empresa, su interrelación y valor, en el sentido de qué perjuicio supondría su degradación. Así mismo, se debe determinar a qué amenazas están expuestos aquellos activos; estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza, y estimar el riesgo.

En el caso de la empresa Ventas Forte S.A, para el levantamiento de la información, se identifica los activos que almacena información y los servicios que presta, lo que corresponde a los equipos informáticos utilizados en las diferentes áreas, tales como: Gerencia General, Administración, Financiero y Talento Humano.

Tabla 1

Activos de Equipos Informáticos de la empresa Ventas Forte S.A.

#	ID - ACTIVO	Tipo de Activo	Nombre del activo	CARGO	DEPARTAMENTO
1	VF1	Hardware	IPAD PRO 2020	Gerente	Gerencia General
2	VF2	Hardware	LAPTOP ASU ROG Strix G15 2021	Jefe Financiero	Financiero
3	VF3	Hardware	IPAD PRO 2020	Jefe Administrativo	Administrativo
4	VF4	Hardware	LAPTOP ASU ROG Strix G15 2021	Jefe de Tal.Humano	Recursos Humanos
5	VF5	Hardware	LAPTOP ASU ROG	Secretaria	Gerencia General

6	VF6	Hardware	Strix G15 2021 LEXMARK	Impresora	Gerencia General
7	VF7	Software	AMAZON WORKDOCS	Amazon Web Services	Administrativo

Nota. Los activos considerados corresponden a los equipos y herramientas informáticas con los que cuenta la empresa Ventas Forte S.A.

Los equipos informáticos descritos en la Tabla 1 se clasifican de acuerdo a las tareas que realizan en las diferentes áreas de la empresa Ventas Forte S.A.

3.1 Valoración de los activos / Ponderación de la criticidad de activos

La valoración se puede ver desde la perspectiva de la necesidad de proteger, pues cuanto más valioso es un activo, mayor nivel de protección se requiere en la dimensión de seguridad. El fin de tener segura la información es poder cumplir los objetivos planteados por la empresa, implementando un sistema que resguarde lo más importante que es la información, considerando los riesgos relativos a las TIC de la organización, a los clientes, y a la administración.

La valoración se considera a las características propias de un activo para darle valor a las consecuencias de una amenaza, basados en:

- Disponibilidad. La información debe estar siempre accesible para aquellos que estén autorizados.
- Integridad. La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.

GESTIÓN DE LA INFORMACIÓN

- Confidencialidad. La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.

Esta valoración está determinada en 5 dimensiones: 5 - muy alto, 4 - alto, 3 - medio, 2 - bajo y 1 – nulo, y por cada escala se consideran varios criterios.

Tabla 2

Escala de Valores / Criterios de Valor

Valor		Escala de valores		Criterios de Valor
5	Muy alto	Afectación muy alta a la empresa	DO	Daño en la operación del negocio
			DSE	Daño en los sistemas de la empresa
			DI	Daño en la información guardada en la base de datos
4	Alto	Afectación alta a la empresa	DS	Daño en un sector/área específicamente
			FCR	Falla en cumplir un reglamento de Ley
			FAP	Falla en la atención al público
3	Medio	Afectación media a la empresa	ON	En ocasiones afecta la operatividad del negocio
			IMC	Impacto medio en las comunicaciones
2	Bajo	Afectación baja a la empresa	PTI	Problemas en el trabajo de un individuo
			IMO	Impacto mínimo en la operación la empresa
1	Nulo	La empresa no sufre afectación	NOA	No afecta la seguridad de los datos.

Nota. Esta tabla muestra las características del activo como consecuencia de una amenaza en la seguridad de la información, basado en varios criterios de acuerdo a la escala de valoración.

GESTIÓN DE LA INFORMACIÓN

Una vez identificado los niveles de amenaza de los equipos informáticos de la Empresa Ventas Forte mediante la aplicación de criterios por cada escala correspondiente a la disponibilidad, integridad y confidencialidad de la información, se calcula el promedio siendo este el resultado de la ponderación asignada a cada activo, ver tabla 3.

Tabla 3

Valoración de Activos de los equipos informáticos de la Empresa Ventas Forte S.A

	ID – activo	Nombre del activo	Disponibilidad		Integridad		Confidencialidad		Valor Total
			Valor	Crit.	Val.	Crit.	Val.	Crit.	
1	VF1	IPAD PRO 2020	2	PTI	3	ON	2	PTI	2,33
2	VF2	LAPTOP ASU ROG Strix G15 2021	3	ON	3	IMC	2	PTI	2,67
3	VF3	IPAD PRO 2020	2	PTI	3	ON	2	PTI	2,33
4	VF4	LAPTOP ASU ROG Strix G15 2021	3	ON	3	IMC	2	PTI	2,67
5	VF5	LAPTOP ASU ROG Strix G15 2021	3	ON	3	IMC	2	PTI	2,67
6	VF6	LEXMARK T656	2	IMO	1	NOA	1	NOA	1,33
7	VF7	AMAZON WORKDOCS	5	DO	5	DI	4	FCR	4,67

Nota. A cada equipo informático de la Empresa Ventas Forte S.A. se calcula el valor promedio como resultado del impacto a la posible afectación conforme a la escala y criterio determinados en la tabla 2.

3.2 Identificación de amenazas y vulnerabilidades.

La vulnerabilidad se refiere a la exposición directa a un riesgo dentro del área de sistemas, debido a la inseguridad que sufren las conexiones entre los equipos, mientras que, la amenaza se

considera a un posible evento que pudiera presentar o ocurrir, atentando contra las partes de un sistema ya sea físico o digital, en lo que se refiere a la integridad, disponibilidad, confidencialidad y autenticidad de la información.

Se Identifican todas las amenazas y vulnerabilidades inherentes a la información que maneja la empresa Ventas Forte S.A., utilizando una metodología de evaluación de riesgos previamente seleccionada. También se analiza el nivel de impacto y riesgo que implican estas vulnerabilidades y los controles para su mitigación. Por lo tanto, se deben crear acciones para prevenir las vulnerabilidades y amenazas acorde a la importancia del nivel de inversión. En la tabla 4, se agrupan los activos de los equipos informáticos de la siguiente manera: Ipad, laptop, impresora y Aplicación Software *Amazon WorkDocs*.

Tabla 4

Amenazas y Vulnerabilidad de los activos de la Empresa Ventas Forte S.A.

	AMENAZAS	**VULNERABILIDAD**
Activo	**Descripción**	**Descripción**
IPAD, LAPTOP, IMPRESORA	Terremoto	Falta de protección antisísmica
	Incendio	Falla en los sistemas contra incendios
	Falla Física	Falla / falta de mantenimiento preventivo
	Falla Eléctrica	Falla en los sistemas de los UPS o Generadores Eléctricos
	Temperatura	Falla en el Acondicionamiento adecuado de temperatura
	Robo	Falla / falta de control antirrobo
AMAZON WORKDOCS	Administración del Sistema	Falta de capacitación al Administrador de la plataforma
	Usuarios	Falta de capacitación a los usuarios sobre la herramienta
	No detección de errores en el sistema (monitoreo)	Error de monitoreo de la herramienta

	Ingreso erróneo de información	Falta de conocimiento de la herramienta
	Caídas en el sistema (falla en los servicios	Fallas en la actualización del sistema

Nota. Detalle de los tipos de amenazas y vulnerabilidad de los activos equipos informáticos identificados en la empresa Ventas Forte S.A.

3.3 Análisis e identificación de impacto.

El impacto es la diferencia entre las estimaciones del estado de seguridad del activo antes y después de materializar las amenazas. El activo de información según la norma ISO 27001 es la consecuencia de la materialización de una amenaza.

A continuación, se analiza el impacto en la empresa Ventas Forte S.A. de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de los activos de información, evaluando de forma realista la probabilidad de ocurrencia en relación a las amenazas y vulnerabilidades.

- Existe una fragmentación de información de los trabajos de la empresa que derivan en deficiencias en la optimización de recurso temporal y humano, principalmente en el proceso de generación de planillas de avances de trabajos, fase fundamental para la adquisición de los recursos de la empresa.
- Se presenta un alto y constante riesgo de sufrir multas e incluso de generar incumplimientos contractuales al no proveer la información solicitada por parte de los entes de control en los tiempos establecidos para este efecto debido a la desincronización departamental.

GESTIÓN DE LA INFORMACIÓN

- Resulta evidente una carencia de organización por parte del personal responsable de la información que impide la correcta unificación de la información necesaria para los fines de la empresa constructora.

Por lo anterior es necesario la optimización la gestión administrativa a través de la generación de un plan dentro de la empresa, implementando estrategias de las tecnologías de la información para erradicar la fragmentación de información y con esto evitar la falta de eficiencia que infiere directa y principalmente en incumplimientos contractuales y consecuencias que conllevan desde multas pecuniarias hasta la rescisión de sus contratos.

Tabla 5

Consecuencias del Impacto

Código	Descripción
I1	Pérdidas materiales
I2	Pérdidas económicas
I3	Responsabilidad legal
I4	Daños a personas
I5	Incumple obligaciones fiscales
I6	Pérdida de información (activo)

Nota. Esta tabla muestra las posibles consecuencias ante un hecho que suscita con relación a la seguridad de la información.

La tabla número 6 determina las consecuencias del impacto por cada tipo de amenaza y la afectación en los intereses de la empresa Ventas Forte S.A., considerando el tipo de activo de los equipos informáticos y la amenaza relacionada.

Tabla 6

Consecuencias del Impacto por tipo de amenaza a los Activos Informáticos de la empresa Ventas Forte S.A.

Activo	Código	Descripción Amenaza	Impacto	Disponibilidad	Integridad	Confidencialidad
IPAD, LAPTOP, IMPRESORA	APC1	Terremoto	I1, I2, I4	X		
	APC2	Incendio	I1, I2, I4	X		
	APC3	Falla Física	I1, I2	X		
	APC4	Falla Eléctrica	I1, I2	X		
	APC5	Temperatura	I1, I2, I4	X		
	APC6	Robo	I1, I2, I3, I4	X		X
AMAZON WORKDOCS	AWD1	Administración del Sistema	I2, I3, I4	X	X	X
	AWD2	Usuarios	I1, I2, I5, I6	X		
	AWD3	No detección de errores en el sistema (monitoreo)	I1, I2	X		
	AWD4	Ingreso erróneo de información	I2, I4, I6		X	
	AWD5	Caídas en el sistema (falla en los servicios	I2, I5	X		

Nota. Esta tabla muestra el impacto y su afectación en la seguridad de la información considerando el tipo de activo informáticos de la empresa Ventas Forte S.A y la amenaza relacionada.

3.4 Análisis y Evaluación del Riesgo

La evaluación del riesgo es un proceso de comparación de los riesgos estimados contra un criterio de riesgo calculado dado para determinar la importancia del riesgo en todos los activos de la empresa, para encontrar medidas preventivas para la seguridad de la información.

GESTIÓN DE LA INFORMACIÓN

Luego de identificar los riesgos a los que están expuestos los activos de la empresa Ventas Forte S.A. a través de un análisis completo entre vulnerabilidades, amenazas y el impacto, se considera una metodología de análisis de riesgo cualitativo que consiste en utilizar una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales (baja, media y alta) y la probabilidad de esas consecuencias. Cabe indicar, que se necesita tener como dato la frecuencia que puede suceder las amenazas y asignar un valor al impacto ocasionado, lo que servirá para el análisis y evaluación de riesgo.

Tabla 7.

Formas de Frecuencia ante una amenaza

Código	Frecuencia
5	Siempre
4	Casi siempre
3	A veces
2	Pocas veces
1	Casi nunca

Nota. Esta tabla muestra la frecuencia que puede suceder una amenaza.

Tabla 8.

Nivel de Impacto ante una amenaza.

Código	Nivel de impacto
5	Muy alto
4	Alto
3	Medio
2	Bajo
1	Muy bajo

Nota. La tabla muestra un valor de acuerdo al nivel de impacto ante una amenaza a los activos de la empresa Ventas Forte S.A.

Tabla 9

Nivel de Riesgo

Código	Descripción
1-5	El riesgo es Bajo
6-15	El riesgo es Medio
16-27	El riesgo es Alto

Nota. El nivel de riesgo aplica la siguiente fórmula Nivel de riesgo = VA (CID) * Nivel de amenaza * Nivel de vulnerabilidad

Tabla 10.

Matriz de análisis y evaluación del Riesgo

Activo	Código	Descripción	Frecuencia	Impacto	Valor del riesgo
IPAD, LAPTOP, IMPRESORA	APC1	Terremoto	1	5	5
	APC2	Incendio	1	5	5
	APC3	Falla Física	2	5	10
	APC4	Falla Eléctrica	2	5	10
	APC5	Temperatura	2	5	8
	APC6	Robo	1	5	5
AMAZON WORKDOCS	AWD1	Administración del Sistema	1	5	5
	AWD2	Usuarios	3	4	12
	AWD3	No detección de errores en el sistema (monitoreo)	4	5	20
	AWD4	Ingreso erróneo de información	3	4	12
	AWD5	Caídas en el sistema (falla en los servicios	2	5	10

Nota. Valoración de riesgo de los Activos informáticos de la empresa Ventas Forte S.A.

La tabla 10 determina el valor de riesgo por los activos informáticos, siendo los de mayor ponderación en los equipos Ipad, Laptop e Impresora, ante las amenazas Falla física, falla

eléctrica y temperatura, la frecuencia 2 (pocas veces), el nivel de impacto es 5 (muy alto) y el valor de riesgo 10, lo que significa que el riesgo es medio. Y, con relación a la herramienta Amazon WorkDocs, la amenaza de mayor ponderación es la "No detección de errores en el sistema (monitoreo)", cuya frecuencia se determina 4 (casi siempre), el nivel de impacto 5 (muy alto) y el valor del riesgo 20, lo que significa que el riesgo es muy alto.

3.5 Análisis e implementación del plan de tratamiento de riesgo

El tratamiento de los riesgos es tomar decisiones frente a los diferentes riesgos existentes en la empresa. Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo.

Dentro de los procesos de gestión del riesgo de la seguridad de la información, existen cuatro opciones disponibles para el tratamiento del riesgo: Reducción del riesgo, Aceptación del riesgo, Evitación del riesgo y Transferencia del riesgo.

Reducción del riesgo. - Tiene por objetivo reducir el nivel del riesgo para a su vez reducir el impacto y la probabilidad de ocurrencia de daños sobre los activos de información de la empresa.

Aceptación del riesgo.- Debido a los costos de implementación para mitigar el impacto cuando el riesgo se presente, algunas empresas deciden no invertir en planes de tratamiento de riesgos y deciden asumir las consecuencias del impacto cuando se presente el riesgo.

Evitar el riesgo.- Se debe evitar la actividad o la acción que da origen al riesgo particular. Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riego, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad.

Transferencia del riesgo.- El riesgo se debe transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular dependiendo de la evaluación del riesgo.

Tabla 11

Plan de Tratamiento de Riesgo de la empresa Ventas Forte S.A.

Activo	AMENAZA		VULNERABILIDAD	Valor del riesgo	Riesgos mitigados
	Código	Descripción	Descripción		
IPAD, LAPTOP, IMPRESORA	APC3	Falla Física	Falla / falta de mantenimiento preventivo	10	5
	APC4	Falla Eléctrica	Falla en los sistemas de los UPS o Generadores Eléctricos	10	5
AMAZON WORKDOCS	AWD2	Usuarios	Falta de capacitación a los usuarios sobre la herramienta	12	4
	AWD3	No detección de errores en el sistema monitoreo	Error de monitoreo de la herramienta	20	10
	AWD4	Ingreso erróneo de información	Falta de conocimiento de la herramienta	12	8
	AWD5	Caídas en el sistema (falla en los servicios	Fallas en la actualización del sistema	10	5

Nota. Esta Tabla muestra la Valoración de riesgo elevada de los activos informáticos de la empresa Ventas Forte S. A., los cuales deben ser mitigados.

3.6 Análisis y selección de los controles del estándar ISO 27001

La ISO 27001 o Sistema de gestión de la seguridad de la información, es un marco de políticas y procedimientos que incluye todos los controles legales, físicos y técnicos que forman parte de los procesos de gestión de riesgos de información de una empresa. Esta norma cuenta con un total de 114 controles de seguridad, divididos en 14 secciones, como se detalla a continuación:

- Políticas de seguridad de la información: A. 5.
- Organización de la seguridad de la información: A.6.
- Seguridad de los recursos humanos: A. 7.
- Gestión de Activos: A.8.
- Controles de acceso: A.9.
- Criptografía – Cifrado y gestión de claves: A.10.
- Seguridad física y ambiental: A.11.
- Seguridad operacional: A.12.
- Seguridad de las comunicaciones: A.13.
- Adquisición, desarrollo y mantenimiento del sistema: A.14.
- Gestión de incidentes de seguridad de la información A.16.
- Cumplimiento: A.18.

En base al resultado de la gestión de riesgos de la empresa Ventas Forte S.A., se ha seleccionado los controles aplicables para garantizar la seguridad de la información.

Tabla 12

Análisis y Selección de Controles de la Norma ISO 27001

PLAN DE TRATAMIENTO DE RIESGO				
Activo	**AMENAZA**		**VULNERABILIDAD**	**Control Seleccionado**
	Código	**Descripción**	**Descripción**	
IPAD, LAPTOP, IMPRESORA	APC3	Falla Física	Falla / falta de mantenimiento preventivo	8. Gestión de Activos 11.2 Seguridad de los equipos
	APC4	Falla Eléctrica	Falla en los sistemas de los UPS o Generadores Eléctricos	8. Gestión de Activos 11.2 Seguridad de los equipos 17.1 Continuidad de la seguridad de la información.
AMAZON WORKOCS	AWD2	Usuarios	Falta de capacitación a los usuarios sobre la herramienta	8.1.3 Uso aceptable de los Activos 11.2 Seguridad de los equipos
	AWD3	No detección de errores en el sistema (monitoreo)	Error de monitoreo de la herramienta	11.2 Seguridad de los equipos
	AWD4	Ingreso erróneo de información	Falta de conocimiento de la herramienta	8.1.3 Uso aceptable de los Activos 11.2 Seguridad de los equipos
	AWD5	Caídas en el sistema (falla en los servicios	Fallas en la actualización del sistema	11.2 Seguridad de los equipos

Nota. De acuerdo a la amenaza y vulnerabilidad de los activos con mayor ponderación de riesgo, se selecciona los controles de seguridad de la Norma ISO 27001 en base al resultado de la gestión de riesgo.

3.7 Desarrollo e implementación del Sistema de Gestión de Seguridad de la información

De acuerdo a la Guía Nro. 8 del Modelo de Seguridad y Privacidad de la información, (MINTIC, 2013) con derechos reservados por parte del Ministerio de Tecnología de la Información y las Comunicaciones, y considerando el trabajo de investigación (Huayamave, 2017) se detallan los controles seleccionados, lo que corresponde al componente de Planificación:

A.8. Control Gestión de Activos

A.8.1. Responsabilidad por los activos. Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

La empresa Ventas Forte S.A. debe tener claramente registrado los tipos de activos con los que cuenta y de ser posible un avaluó, con la finalidad de agilitar la recuperación en el caso de alguna pérdida en la información.

A.8.1.3. Uso aceptable de los Activos. Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

Los usuarios que utilizan y manejan los activos de la empresa Ventas Forte S.A., sean estos equipos o sistemas informáticos quieren capacitación permanente y retroalimentación.

A.11. Seguridad física y del entorno

A.11.2. Equipos. Objetivo: Prevenir la pérdida, daño o robo o compromiso de activos, y la interrupción de las operaciones de la organización.

La empresa Ventas Forte S.A. debe proteger sus equipos contra todo tipo de amenaza, sean estos de tipo físico o ambiental, con la finalidad de minimizar accesos no autorizados y la mala manipulación del activo (equipo), que puedan conllevar al daño o sustracción del activo, por lo tanto, se debe contar con planes de emergencia ante cualquier eventualidad que se presente.

A.17. Aspectos de seguridad de la información de la gestión de continuidad de negocio.

A.17.1 Continuidad de seguridad de la información. Objetivo: Incluir en los sistemas de gestión de la continuidad de negocio de la organización seguridad de la información.

La empresa Ventas Forte S.A. deberá tener una plan de contingencia o emergente en el caso de falla en los controles, y que ya no puedan cumplir con sus objetivos para los que fueron implementados. Se debe garantizar con controles de seguridad de la información operativa ante cualquier eventualidad o desastre natural.

El plan de contingencia y recuperación ante imprevistos debe ser revisado periódicamente, ya que puede presentarse algún cambio dentro de los procesos que maneja la empresa.

Tabla 14

Plan de Acción en base a los controles seleccionados en el Plan de Tratamiento de Riesgo.

Activo	AMENAZA		VULNERABIL	Control Seleccionado	Plan de Acción
	Código	Descripc.	Descripción		
IPAD, LAPTOP, IMPRESORA	APC3	Falla Física	Falla / falta de mantenimiento preventivo	8. Gestión de Activos 11.2 Seguridad de los equipos	Tener actualizado el inventario de equipos. Planificar los mantenimientos preventivos periódicos.
	APC4	Falla Eléctrica	Falla en los sistemas de los UPS o Generadores Eléctricos	8. Gestión de Activos 11.2 Seguridad de los equipos 17.1 Continuidad de la seguridad de la información.	Realizar el plan de continuidad para saber qué medidas tomar en el caso que se presente un evento o suceso de este tipo, contar con suministro eléctrico alterno, equipos UPS y demás.
AMAZON WORKDOCS	AWD 2	Usuarios	Falta de capacitación a los usuarios sobre la herramienta WorKDocs.	8.1.3 Uso aceptable de los Activos 11.2 Seguridad de los equipos	Impartir capacitación sobre la plataforma que utiliza la constructora Ventas Forte S.A. a todos el personal nuevo y firmar acta de responsabilidad entre el trabajador nuevo y la empresa sobre el uso de los sistemas (activos).
	AWD 3	No detección de errores en el sistema (monitoreo)	Error de monitoreo de la herramienta	11.2 Seguridad de los equipos	Capacitación a personal y usuarios sobre el monitoreo de aplicaciones y estado de los servicios. Establecer el plan de acción ante eventos o sucesos que se presenten.
	AWD 4	Ingreso erróneo de información	Falta de conocimiento de la herramienta	8.1.3 Uso aceptable de los Activos 11.2 Seguridad de los equipos	Impartir capacitación sobre los sistemas que utiliza la constructora Ventas Forte S.A. a todo el personal nuevo y firmar acta de responsabilidad entre el trabajador nuevo y la empresa sobre el uso del sistema.
	AWD 5	Caídas en el sistema (falla en los servicios	Fallas en la actualización del sistema	11.2 Seguridad de los equipos	Plan de contingencia. Tener un plan de recuperación y continuidad del negocio para minimizar el impacto por la caída del servicio.

Nota. Se detalla el plan de contingencia en base a los controles de seguridad seleccionados en el Plan de Tratamiento de Riesgo.

3.8 Desarrollo de la política de seguridad informática

El recurso más importante de una empresa es la información, por lo tanto, debe estar protegido mediante la creación de varias políticas de seguridad para proveer los elementos claves de seguridad ya mencionados: Integridad, disponibilidad, Confidencialidad, Autenticidad y Trazabilidad, para:

- Garantizar la confidencialidad de los datos gestionados en los diferentes procesos de la empresa.
- Garantizar la disponibilidad de servicios ofrecidos a clientes, de igual manera a los servicios y procesos internos de la empresa.
- Garantizar el funcionamiento de servicios en lapsos de tiempo cortos, tras ocurrir situaciones de emergencia.
- Prevenir que la información sea modificada sin ninguna autorización.
- Concientizar y brindar formación permanente sobre seguridad de la información.

La política de seguridad está formada de normas, reglamentos y protocolos a seguir de acuerdo con los objetivos, requisitos del negocio y leyes previamente establecidos, donde se determinan las medidas para salvaguardar la información de amenazas, permitiendo la continuidad del negocio, minimizar los posibles daños y maximizar el rendimiento de las herramientas empleadas para proteger la información.

GESTIÓN DE LA INFORMACIÓN

La política de Seguridad tiene dos propósitos centrales: Informar a todos los usuarios sobre las obligaciones que deben asumir respecto a la seguridad asociada a los recursos de tecnologías de información y dar las guías para actuar ante posibles amenazas y problemas presentados (Cevallos, 2011).

Objetivo de la Política.- Se debe elaborar un documento claro sobre las políticas establecida para garantizar el correcto manejo de los activos de la empresa Ventas Forte S.A. y correcta difusión de las políticas para que sean de conocimiento de todo el personal de la empresa.

Documento de Política de Seguridad de la Información.- Es un documento que se debe de cumplir obligatoriamente por parte de todos los empleados de la empresa y debe estar difundido por el personal de talento humano para que todos conozcan de las políticas de la empresa en lo referente a gestión de activos. El no cumplir con estas políticas puede traer consigo pérdidas monetarias para la empresa y el no cumplimiento de sus objetivos. Dentro del documento se debe especificar lo siguiente:

- Objetivos de la organización, el alcance y una descripción de la seguridad de la información
- Valoración y manejo de los riesgos existentes así como detallar los objetivos de los controles.
- Una descripción de las políticas y normas de conformidad más importantes para la organización.

Revisión de la Política de Seguridad de la información. La revisión de la política de seguridad de la información debe ser efectuada con frecuencia o en tiempos planificados, para ello se debe señalar los cambios más significativos a la primera evaluación de los riesgos presentes en activos de la organización.

Política de Seguridad de la Información

Cláusula 1

Creación de un Comité conformado por Gerente, Talento Humano y Jefes de Área, el cual se reunirá para la compra y adquisición de activos tecnológicos, Estandarización de equipos de Tecnología de la Información, aplicaciones y sistemas.

Entre las responsabilidades del Comité, se encuentra la correcta utilización y funcionamiento de los activos de información, plan de mejora continua sobre los tipos de riesgos observados, preparación de estrategias y controlar la calidad del servicio brindado. Como también, mantener el inventario general de los activos actualizado, cumplir y hacer cumplir las políticas establecidas para el uso de los activos e implementar acciones correctivas y sanciones correspondientes a las personas que no acaten las políticas.

Cláusula 2.

Se deben definir claramente las responsabilidades de protección de los activos y servicios. Las personas con responsabilidades de seguridad son las encargadas de verificar la correcta ejecución de las tareas asignadas y supervisara todas las políticas implementadas y establecidas por el Comité.

GESTIÓN DE LA INFORMACIÓN

Inventario de los activos de cómputo

Cláusula 3.

Elaborar un formato el cual se encuentre aprobado por el Comité, donde conste el inventario general de todos los activos, y asignación de custodio y funciones que se realizan con ese activo.

Sobre las instalaciones físicas de los activos de cómputo (equipos)

Cláusula 4

Los equipos de cómputo deben constar con instalaciones eléctricas y puntos de redes identificadas y en correcto funcionamiento. La persona responsable debe firmar un acta de entrega del activo y en donde se valide la firma de responsabilidad. El uso de regletas, extensiones u otros elementos de corrientes queda totalmente prohibido. Se debe realizar un control semestral sobre los puestos de trabajo y los equipos instalados al personal que labora en la empresa.

Funcionamiento de los equipos de cómputo

Cláusula 5

El Jefe Administrativo debe revisar que los activos de cómputo se utilicen de manera correcta y en las condiciones adecuadas establecidas por el proveedor.

Cláusula 6

Evitar el consumo de alimentos y bebidas en los espacios establecidos para los equipos de cómputo.

GESTIÓN DE LA INFORMACIÓN

Cláusula 7

Prohibir el ingreso de equipos particulares a las áreas de la empresa, como también, prohibir la instalación de programas y aplicativos no autorizados.

Cláusula 8

Implementar software de antivirus actualizado a los equipos de cómputo de la empresa. Asignar a quien corresponda el monitoreo del estado de la aplicación en los equipos instalados.

Elementos de seguridad y del entorno

Cláusula 9

La empresa debe garantizar el adecuado uso de los equipos de computación, por ejemplo: ambiente climatizado de acuerdo a las necesidades de las áreas, rutas de escape por área, equipos y señalización contra incendio, sistemas de fuentes de energía para dotar a los equipos en caso de algún suceso, contar con políticas y procedimientos definidos por cualquier eventualidad que pueda suceder en la empresa.

Mantenimiento preventivo y correctivo

Cláusula 10

Desarrollar un plan de mantenimiento preventivo a los equipos de cómputo, donde se encuentre establecida la frecuencia de esta actividad, el personal responsable y definir el procedimiento sobre los mantenimientos correctivos que se presenten en la empresa.

GESTIÓN DE LA INFORMACIÓN

Correcto uso de los Activos

Cláusula 11

Los activos de la empresa deben estar accesible solo por personal autorizado y ser utilizados de acuerdo con las funciones asignadas para lo que fueron instaladas.

Internet y redes internas

Cláusula 12

La empresa debe establ**cer** normas relacionadas con el correcto uso de los recursos informáticos existentes que aseguren la integridad de los sistemas, equipos y la confidencialidad de la información, resultado de las operaciones que realiza la empresa. E implementar políticas de seguridad lógica y equipos como firewall, IPS (proveedor de servicio de internet), equipos de filtrado web e email y equipos perimetrales.

Cláusula 13

Desarrollar un plan de contingencia antes desastres, asegurar los activos de la empresa mediante póliza de seguros. Elaborar procedimientos para que la empresa pueda seguir funcionando desde un sitio alterno en el caso de desastres.

Copias de seguridad de los datos

Cláusula 14

Los empleados y autoridades deben custodiar convenientemente sus cuentas de usuarios y contraseñas, no revelarán o transferirán a terceros (personas o navegadores que permitan el recordatorio automático de contraseñas), más bien serán responsables directos de toda la

actividad relacionada con el uso indebido de sus cuentas de usuario asignadas. Así mismo, se prohíbe el envío por correo de forma interna o externa, de información confidencial que comprometa los intereses de la empresa.

Cláusula 15

El responsable de la administración de la herramienta WorkDocs respetará la privacidad de los usuarios, no divulgará información acerca de las cuentas de usuario o del uso que haga del servicio a menos que sea requerido para cumplir con procedimientos legales.

Los usuarios deberán depurar (borrar) de sus bandejas de correo personal y departamental los correos innecesarios, con la finalidad de precautelar la disponibilidad de espacio de almacenamiento otorgado a cada cuenta y de los equipos servidores.

El envío o recepción de archivos concerniente a la empresa Ventas Forte, debe realizarse a través del servicio la Herramienta WorkDocs, para garantizar el principio de confidencialidad y no repudio.

3.9 Análisis de Resultados del Sistema de gestión de seguridad de la información

La implantación de la norma ISO 27001 en una empresa, tiene como finalidad reducir sus riesgos y evitar posibles incidentes de seguridad. Sin embargo, hay que considerar que existen situaciones que son imposibles evitar, ya que no es posible proteger los activos de la información al 100%, por lo que es necesario disponer de un Plan de Continuidad, mismo que

tiene como objetivo impedir que la actividad de la empresa se interrumpa y, si no puede evitarse, que el tiempo de inactividad sea el mínimo imposible.

Para garantizar la continuidad de los sistemas de información, las políticas creadas deben ser socializadas por el personal responsable, para que sean cumplidas a cabalidad y crear acuerdos de compromiso entre la empresa y los trabajadores.

3.9.1 Dar a conocer la política de seguridad

Las políticas de seguridad deben ser comunicadas y difundidas al personal que labora en la empresa, como también, al personal externo que mantiene negociaciones

La capacitación a los empleados de la empresa Ventas Forte S.A. es una actividad imprescindible para que comprendan y apliquen las políticas dentro de sus funciones y establecer un plan de capacitación continuo con la finalidad de reforzar las dudas referentes a las políticas.

3.10. Evaluar si fueron mitigados los riesgos

Se realizó análisis de los riesgos mitigados.

Tabla 15.

Riesgos Mitigados

PLAN DE TRATAMIENTO DE RIESGO						Riesgos Mitigados		
Activo	**Código**	**Descripción**	**Frecuencia**	**Impacto**	**Valor del Riesgo**	**Frecuencia**	**Impacto**	**Riesgos mitigados**
IPAD, LAPTOP, IMPRESORA	APC3	Falla Física	2	5	10	1	5	5
	APC4	Falla Eléctrica	2	5	10	1	5	5
AMAZON WORKDOCS	AWD2	Usuarios	3	4	12	1	4	4
	AWD3	No detección de errores en el sistema (monitoreo)	4	5	20	2	5	10
	AWD4	Ingreso erróneo de información	3	4	12	2	4	8
	AWD5	Caídas en el sistema (falla en los servicios	2	5	10	1	5	5

Nota. Evaluación si los riesgos mitigados

Tabla 16.

Plan de Tratamiento de Riesgo Mitigados

PLAN DE TRATAMIENTO DE RIESGO					
Activo	**AMENAZA**		**VULNERABILIDAD**	**Valor del Riesgo**	**Riesgos mitigados**
	Código	**Descripción**	**Frecuencia**		
IPAD, LAPTOP, IMPRESORA	APC3	Falla Física	Falla / falta de mantenimiento preventivo	10	5
	APC4	Falla Eléctrica	Falla en los sistemas de los UPS o Generadores Eléctricos	10	5
AMAZON WORKDOCS	AWD2	Usuarios	Falta de capacitación a los usuarios sobre la	12	4

		herramienta		
AWD3	No detección de errores en el sistema (monitoreo)	Error de monitoreo de la herramienta	20	10
AWD4	Ingreso erróneo de información	Falta de conocimiento de la herramienta	12	8
AWD5	Caídas en el sistema (falla en los servicios	Fallas en la actualización del sistema	10	5

Nota. Plan de tratamiento de riesgos mitigados.

4. Discusión

Los resultados obtenidos en el análisis de la presente investigación fueron utilizados para su comparación y evaluación de indicadores de riesgos antes y después de ser aplicado el sistema de gestión de la información para su seguridad basados en la norma ISO 27001. Sin embargo, Vega (2020), comenta que en base a la búsqueda de una evaluación exitosa y con impacto positivo esta debe incluir realización de actividades adicionales a la verificación y examinación técnica. Vega dentro de su estudio menciona 3 técnicas definidas por Baloch (2017), las cuales permitirían definir de manera más clara la técnica usada en el presente proyecto. Estas son: Técnicas de revisión, técnicas de identificación y técnicas de validación de vulnerabilidad. Para el presente proyecto se consideró como técnica utilizada la técnica de revisión, ya que, Baloch (2017) afirma que con "Se basa en la examinación con el fin de evaluar sistemas, aplicaciones, redes, políticas y procedimientos con el objetivo de descubrir vulnerabilidades."

En la evaluación de riesgo de los 11 activos analizados en la empresa Ventas Forte S.A. el 54.54% fueron considerados riesgo medio y un 9.09% de riesgo alto, el porcentaje restante no presenta riesgo. Una vez implementado el plan de tratamiento de riesgo y la aplicación de los

planes de acción de acuerdo con los controles seleccionados de la norma ISO 27001, los riesgos fueron mitigados basados en el cambio de estado de algunos activos, de pasar de riesgo medio a bajo riesgo. (Cáceres, 2027) ejecutó la implementación de un SGSI compuesto en 5 sistemas de tal manera de que se cumplieran 44 objetivos de control de los 144 del objetivo principal. En el caso de la empresa Ventas Forte S.A cumple progresivamente con la reducción del riesgo llegando a la conclusión que el sistema de gestión mejora la seguridad de la información y la eficacia en los procedimientos documentales.

Para que estos hallazgos sean aplicados por otras organizaciones o instituciones, la revisión de la política de seguridad de la información debe ser efectuada con frecuencia en periodos establecidos por una planificación estratégica previa, para ello, se debe señalar los cambios más significativos a la primera evaluación de los riesgos presentes en activos de la organización. Estos lineamientos pueden seguir el orden de las 15 cápsulas mencionadas respecto a las políticas de seguridad.

Como función fundamental de la empresa constructora le corresponde la parte operativa en la que requiere salvaguardar la seguridad de la información y determinar si influye notoriamente las políticas de seguridad en la mejora de la confidencialidad, integridad y disponibilidad.

Los resultados demuestran la importancia de la complementariedad de este plan de gestión, ya que atiende a una necesidad estratégica, esto se observa claramente en que se han mostrado resultados tanto cualitativos como cuantitativos en las secciones de gestión del tiempo y del costo incurrido.

5. Conclusiones

- El estado actual de seguridad de información no garantiza confianza en sus procesos y por medio del análisis de riesgos aplicando el modelo PDCA (*Plan, do, Check, Act*) se diagnosticó la necesidad de herramientas que bajo normativas permitan la administración digital de su documentación.
- La aplicación de las políticas de seguridad permiten salvaguardar la información de amenazas, como también, disminuir los posibles daños e incrementar el rendimiento de las herramientas utilizadas para proteger la información.
- Un plan para la seguridad de la información crea una mayor garantía para la organización y las empresas con las que se asocia en cada contrato. Los clientes obtienen más seguridad de su documentación y procesos, lo que conlleva a continuidad en los negocios, y un bajo nivel de impacto de las amenazas que se presenten.
- La incorporación de un sistema de seguridad bajo la normativa ISO 27001 permite a la empresa Ventas Forte S.A. mejorar la infraestructura tecnológica y llevar un adecuado control en la manipulación de los equipos y herramientas informática.
- El uso de una plataforma informática (*Amazon Workdocs*) permite controlar de manera compartida y sincronizada las funciones de cada archivo, verificando el acceso permitido solo a los usuarios activos.

6. Recomendaciones

- Determinar los responsables de los activos mediante acta, y que se lleve un control del uso correcto de los equipos y herramientas informáticas.
- Socializar las Políticas de seguridad de la información al personal de la empresa Ventas Forte S.A. para que tengan conocimiento de los procesos a seguir en el caso que se presenten amenazas.
- Escoger siempre una plataforma con proveedor que posea respaldo en el mercado. De esta manera se garantizará la seguridad y verificación del servicio.
- Adquirir equipos de buena calidad y actualizados en sus sistemas operativos y software, esta inversión asegurará un largo periodo de funcionamiento y evitará riesgos de que sin previo aviso se dañen los equipos.
- Actualizar frecuentemente el sistema de protección electrónica o copias de seguridad, ya sea por medio de un disco duro u otras plataformas que permiten guardar archivos en la nube.
- La formación y la capacitación a los empleados disminuiría los riesgos del bajo o nulo uso de la plataforma de seguridad que se haya contratado y a su vez aumenta la defensa contra a amenazas y perdidas de la información de la empresa.

7. Referencias Bibliográficas:

AWS. (2021). *¿Qué es Amazon WorkDocs?* Obtenido de https://docs.aws.amazon.com/es_es/workdocs/latest/adminguide/what_is.html

Baloch, R. (2017). *Ethical hacking and penetration testing guide. Auerbach*.

Cáceres, N. Y. (2027). *Sistema de Gestión de seguridad de la información para la Subsecretaría de Economía y Empresas de menor tamaño*. Obtenido de https://repositorio.uchile.cl/bitstream/handle/2250/147976/Sistema-de-gestion-de-seguridad-de-la-informacion-para-la-Subsecretaria-de-Economia-y-Empresas.pdf?sequence=1&isAllowed=y

Cevallos, P. (11 de 10 de 2011). *Políticas de Seguridad*. Obtenido de https://www.repositorio.utn.edu.ec

Dejan, K. (2021). *¿Qué es norma ISO 27001?* Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

Huayamave, R. (2017). implementación de un sistema de gestión de seguridad de la información (sgsi) aplicado a los activos de la empresa constructora Coetecorpza SA, basados en el estándar ISO 27002.

ISO 27001 en empresas constructoras. (30 de Mayo de 2014). Obtenido de https://www.pmg-ssi.com/2014/05/iso-27001-en-empresas-constructoras/

Margerit - versión 3.0. (octubre de 2012). Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Maurice, F. (2017). *Ciclo de Deming: ejemplos, etapas, importancia, ventajas y desventajas*. Obtenido de https://www.beetrack.com/es/blog/ciclo-de-deming-etapas-ejemplos

MINTIC. (2013). Seguridad y Privacidad de la info, rmación.

Morante, D. C. (2015). Gestión administrativa y su relación con el uso de las Tics de las pymes de la zona urbana del cantón Quevedo, año 2015. Quevedo-Ecuador: Universidad Técnica Estatal de Quevedo. Obtenido de https://repositorio.uteq.edu.ec/handle/43000/5097

Risco, E. (2021). Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín, 2021.

Rus Arias, E. (2021). Investigación Exploratoria. *Economipedia*. Obtenido de https://economipedia.com/definiciones/investigacion-exploratoria.html

Seguridad de la Información. (20 de octubre de 2020). Obtenido de https://www.pmg-ssi.com/2020/10/cuales-son-los-motivos-por-los-que-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Seguridad y Privacidad de la información. (2021). Obtenido de https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion

SurveyMonkey. (2021). *Los 3 tipos de investigación de encuestras y cuándo usarlos*. Obtenido de https://es.surveymonkey.com/mp/3-types-survey-research/

Universidad Internacional de la Rioja. (2019). ¿Qué es la certificación ISO 27001 y para que sirve? *UNIR REVISTA*.

Vallejo, M. (marzo de 2002). El diseño de investigación: una breve revisión metodológica. *Scielo, 72*(1). Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-99402002000100002

Vega, E. (arzo de 2020). *Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking*. Obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf