FACULTAD DE POSTGRADOS

PROYECTO CAPSTONE: DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA EMPRESA DEL SECTOR INDUSTRIAL

AUTORES

Luis Israel Pérez Chancusig
Cristian Andrés Quiñones Castro

AÑO

2022

FACULTAD DE POSGRADOS

PROYECTO CAPSTONE: DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA EMPRESA DEL SECTOR INDUSTRIAL

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de

MAGÍSTER EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Autores

Luis Israel Pérez Chancusig

Cristian Andrés Quiñones Castro

Año

2022

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.“

_____

Luis Israel Pérez Chancusig
1714900543

_____

Cristian Andrés Quiñones Castro
0802577916

AGRADECIMIENTOS

A Dios por ser siempre bueno conmigo, por Él mi vida ha sido bendecida hasta que sobre y abunde.

Agradezco a mi mami Alicia por estar siempre pendiente de nosotros.

DEDICATORIA

A mi amada esposa Patty, gracias por ser el amor que me impulsa a llegar más lejos.

A Sofy y Emiliano, por su alegría incondicional que llena de felicidad mi vida, los amo con todo mi ser.

AGRADECIMIENTOS

Agradezco en primer lugar a Dios por permitirme alcanzar una meta más en mi carrera profesional y personal. A toda mi familia en especial a mi esposa, e hijo y a mis padres por el apoyo brindado durante todo este tiempo.

DEDICATORIA

El presente trabajo de titulación va dedicado a mis padres y sobre todo a mi esposa e hijo, que son el pilar fundamental para el cumplimiento de mis metas y objetivos en la vida.

Doy gracias a Dios por permitirme formar una bella Familia junto a mi hermosa esposa Evelin, y agradezco que haya llegado a mi vida ese ser maravillosos que me dice “Papá” (mi hijo Leandro), eres mi motivación para seguir creciendo, los amo.

RESUMEN

En la actualidad los retos más importantes para una empresa son los temas relacionados con la seguridad de la información, la cual se necesita proteger y garantizar la disponibilidad, confidencial e integridad, es importante elaborar un estado de situación actual de la empresa, donde se pueda determinar sus puntos vulnerables, tipos de información que posee, clasificar su información, evaluar su criticidad, crear planes de acción y políticas que guíen al programa de Gestion de Seguridad de la Información.

La evaluación del estado actual en seguridad de la información de la empresa permitirá obtener la brecha entre el nivel adecuado y el actual para tener un punto de partida para iniciar con planes de acción. Para obtener el nivel adecuado se utilizará marcos de referencia como NIST, ISO 27000.

Para conocer el tipo de información crítica de la empresa es necesario la identificación y clasificación de los activos de información en base a criterios establecidos y reuniones con personal del negocio.

Una vez establecido el inventario de activos de información se requiere identificar al contenedor físico o lógico del mismo, catalogar en base a una herramienta de análisis su criticidad.

Establecer un análisis de las amenazas y vulnerabilidades propias de estos activos críticos de información para identificar el riesgo inherente, evaluar los controles existentes y elaborar los planes de acción que permitan llegar a un riesgo residual aceptable para la empresa.

Finalmente se desarrollará de políticas de alto nivel que permitan guiar el proceso a implementar.

ABSTRACT

Currently, the most important challenges for a company are issues related to information security, which needs to be protected and guaranteed availability, confidentiality, and integrity. It is important to prepare a current status of the company, where it can be determine your vulnerabilities, types of information you have, classify your information, assess its criticality, create action plans and policies that guide the Information Security Management Program.

The evaluation of the current state of information security in the company will allow obtaining the gap between the appropriate level and the current one in order to have a starting point to start with action plans. To obtain the appropriate level, reference frameworks such as NIST, ISO 27000.

In order to know the type of critical information of the company, it is necessary to identify and classify the information assets based on established criteria and meetings with business personnel.

Once the inventory of information assets has been established, it is necessary to identify its physical or logical container, to catalog its criticality based on an analysis tool.

Establish an analysis of the threats and vulnerabilities of these critical information assets to identify the inherent risk, evaluate the existing controls and develop action plans that allow reaching an acceptable residual risk for the company.

Finally, high-level policies will be developed to guide the process to be implemented.

Contenido

Introducción

Las tendencias del mercado actual y futuro en temas de seguridad y ciberseguridad obligan a las empresas a ser cada vez más competitivas, las organizaciones que deseen mantenerse vigentes deben considerar a la información como uno de sus activos más importantes y críticos, por tal motivo es necesario evaluar la implementación de un Sistema de Gestión de la Seguridad de la Información. (INCIBE, 2016)

De acuerdo a la Guía Básica de Seguridad IT para PYME, en el 2019, 43% de los ataques cibernéticos se dirigieron a pequeñas empresas, 40% de las pequeñas y medianas empresas experimentaron ocho horas o más debido a una vulnerabilidad cibernética, un tercio de los gastos generados por una vulneración de datos se producen más de un año después del incidente y alrededor del 22% de estos gastos se producen durante el segundo año, 69% de las organizaciones sufrieron una vulneración debido a una amenaza interna, a pesar de las medidas preventivas. (ESET, 2022)

En el caso de la empresa analizada, la alta dirección ha considerado que es de vital importancia para la organización la protección de su información, ya que en función ésta cumple un rol importante en el cumplimiento de los objetivos estratégicos empresariales. Por ello se ha considerado al Departamento de Tecnología como un área clave para iniciar los procesos y alcanzar su cumplimiento.

Manteniendo el contexto nacional, no existe negocio o empresa que no sea vulnerable a ataques cibernéticos, según el ranking de los sectores que han sido víctimas de ciberataques efectivos, el 20% de entidades públicas, 16% en las industrias de alimentos, 16% empresas de *retail* y el sector salud, seguros y financiero con el 12%. (ITAhora, 2022)

1. Antecedentes

En la empresa analizada la información proviene de muchas fuentes que son propias de cada estructura organizativa, área de proceso o producción, dicha información es ingresada en el actual software de gestión empresarial, para los procesos de analítica de datos se utiliza un módulo de BI (*Business Intelligence*), adicionalmente existen iniciativas donde cada área tiene inventariada la información y existe un responsable y custodio de la misma, tanto la información física y digital están almacenadas en repositorios de la empresa.

Se ha identificado que información de varias fuentes como las áreas de Mantenimiento, Producción, Inteligencia de Negocios, han desarrollado reportes propios utilizando herramientas como *Excel, Power BI, Visual Basic, Power Pivot*, etc. e inclusive ya tienen interacción con nubes privadas de analítica. La información de estos procesos no consta en la matriz de activos de información, tanto para su edición, protección y almacenamiento, respaldo, etc., al no estar inventariada está en riesgo de pérdida, filtración, corrupción, difusión con consecuencias aun no valoradas para la empresa en términos económicos, legales y de reputación de marca.

Adicionalmente se ha reportado eventos que podrían ser catalogados como ataques dirigidos mediante phishing utilizando cuentas de correo empresarial que buscan obtener información de la empresa o tener acceso a la red interna.

2. Objetivo

Diseñar el programa del Sistema de Gestión de Seguridad de la Información (SGSI) que permita alcanzar el objetivo de mantener la confidencialidad, disponibilidad, integridad, privacidad de los activos de información más importantes de la organización.

3. Objetivos específicos.

Evaluación de la postura actual en seguridad de la información de la empresa a través de las mejores prácticas establecidas por los marcos de referencia y normas aplicables a nivel internacional.

Identificación y clasificación de los activos de información.

Evaluación de los riesgos relacionados con los activos encontrados y catalogarlos por importancia y criticidad.

Establecimiento de controles para los riesgos detectados, revisión y evaluación del cumplimiento planteado, desarrollo de políticas de alto nivel.

4. Metodología

En el desarrollo del presente proyecto se utilizaron dos marcos de referencia para establecer el estado inicial en seguridad de la empresa, NIST e ISO 27001 los cuales se adaptan de mejor manera a la empresa y al desarrollo de un SGSI, con lo cual se busca identificar y mitigar los riesgos y vulnerabilidades, logrando disminuir el impacto y probabilidad de ocurrencia que pueda interrumpir las operaciones de la empresa causando afectaciones financieras graves.

Para determinar la vialidad de la creación del Programa del Sistema de Gestion de Seguridad de la Información se elaboró un Caso de Negocio donde se ha desarrollado un análisis del proyecto y su viabilidad identificando sus riesgos y la estimación de tiempo, esfuerzo y costo, el detalle se encuentra en el Anexo 1. Caso de negocio.

5. Alcance

Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) para satisfacer la necesidad de proteger la información de los procesos críticos de la empresa, con base en un programa de seguridad sostenible en el tiempo y que pueda mantener una mejora continua, considerando diferentes marcos de referencia de seguridad conocidos.

Para el desarrollo del programa se realizará en fases las cuales se detallan a continuación:

Fase 1. Evaluación del estado actual en seguridad de la información de la empresa.

Fase 2. Identificación y clasificación de los activos de información.

Fase 3. Inventario de activos de información.

Fase 4. Análisis de amenazas y vulnerabilidades para dos activos de información críticos.

Fase 5. Desarrollo de políticas de alto nivel.

6. Marco teórico

Los recursos utilizados para el desarrollo del proyecto se detallan a continuación:

6.1. Norma ISO 27001

Esta norma internacional se ha preparado para proporcionar los requisitos para el establecimiento, implementación mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de la seguridad de la información es una decisión estratégica para una organización. (UNE, 2017)

El uso del estándar ISO 27001 permite a los sistemas de gestión de seguridad de la información contar con evaluaciones de riesgo los mismos que permitirán la aplicación de controles los cuales son de vital importancia para erradicar o mitigar estos fallos en los sistemas de seguridad de las organizaciones. (UNE, 2017)

6.2. NIST

NIST (National Institute of Standards and Technology) el marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario. Le brinda a su negocio una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad. (Comercio, 2022)

6.3. MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es la metodología de análisis y gestión de riesgos elaborada considerando por una parte facilitar ítems de análisis centrándose en lo específico del sistema objeto del análisis y para homogeneizar los resultados del mismo con base en tipos de activos, dimensiones y criterios de valoración relacionados con las amenazas más frecuentes y sus salvaguardas. (Publicas, 2012)

7. Justificación y oportunidades.

La organización cuenta con un procedimiento que parcialmente permite identificar sus activos, las amenazas y vulnerabilidades para el tratamiento de riesgos de seguridad de la información.

Actualmente existen políticas y procedimientos que las áreas cumplen y que son auditados interna y externamente, los cuales aún no se encuentran documentados y clasificados en su totalidad.

La empresa requiere contar con un Programa de Seguridad que permita contar con políticas, procesos y procedimientos con el objetivo de proteger la información de los procesos críticos de la empresa.

El diseño e implementación de un SGSI permitirá identificar y clasificar los activos de información críticos de la organización, reducir y mitigar los riesgos a los cuales se encuentra expuesta la información, ante posibles ataques cibernéticos, *phishing*, *ransomware*, etc., que comprometan la seguridad de la misma.

Desarrollo del Proyecto

8. Fase 1. Evaluación de estado actual

La organización tiene implementado varios controles para proteger la información relacionada a todos sus procesos, con base en una autoevaluación interna en conjunto con los responsables de las áreas se ha establecido un nivel

de cumplimiento de los controles utilizando los marcos de referencia para buenas prácticas NIST e ISO/IEC27001.

Para el análisis se utiliza una matriz con las cinco funciones principales de NIST: Identificar, Proteger, Detectar, Responder, Recuperar, sus categorías y subcategorías en donde a cada una de ellas se aplican controles de ISO/IEC 27001.

8.1. Criterios de evaluación

El método utilizado es la valoración y calificación de los controles de cada subcategoría basado en el siguiente criterio:

N para un control que no ha sido implementado.

P para un control que parcialmente se cumple.

L para un control que tiene evidencia de cumplimiento.

F para un control que se cumple en su totalidad.

Tabla 1.

Métrica de Evaluación

Valor	Métricas de evaluación	Ponderación
N	No logrado	1
P	Parcialmente logrado	2
L	Logrado en gran parte	3
F	Totalmente logrado	4

Con base en la ponderación de los controles de cada subcategoría (1,2,3,4), se realizó un promedio el cual es comparado dentro de un rango definido según el criterio establecido en la Tabla 1, donde 4 es el nivel ideal al cual la organización aspira llegar y 1 el valor mínimo en el cual podría encontrarse.

Tabla 2.

Nivel de la situación actual de la organización

Nivel	Situación Actual	Rango
1	Existe una iniciativa de ejecución de actividades sin la asignación de un responsable, sin planificación, sin documentos controlados, sin métricas de cumplimiento y mejora continua.	1,00 <= 1,75
2	Existe un proceso de ejecución de actividades con la asignación de un responsable, sin planificación, sin documentos controlados, sin métricas de cumplimiento y mejora continua.	> 1,75 <= 2,50
3	Existe un proceso de ejecución de actividades con la asignación de un responsable, con planificación, sin documentos controlados, sin métricas de cumplimiento y mejora continua.	> 2,50 <= 3,25
4	Existe un proceso de ejecución de actividades con la asignación de un responsable, con planificación, con documentos controlados, con métricas de cumplimiento y mejora continua.	> 3,25 <= 4,00

El resultado del nivel de cumplimiento de los controles, sean estas iniciativas, actividades de mejora, procesos establecidos con una planificación, con un responsable asignado y que su cumplimiento se encuentre respaldado con documentos controlados, se detalla en su totalidad en el Anexo 2 Hoja Matriz_evaluacion_(NIST-ISO).

En la Figura 1 se muestra una captura de pantalla del archivo del que se obtuvo el promedio por cada subcategoría:

Función	Categoría	Medicion actual	Ponderacion Nivel Actual	Evaluacion	Justificacion	Nivel adecuado
IDENTIFICAR (DNI)	**Gestión de Activos (ID.AM)**:Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización lograr los objetivos comerciales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de la organización y la estrategia de riesgo de la organización.	L	3		Dentro de la organización cada área ha inventariado y priorizado según su criticidad y valor comercial a los dispositivos y sistemas físicos, las plataformas y aplicaciones de software involucrados en sus procesos, se ha mapeado la comunicación organizacional, los flujos de datos y se ha establecido roles y responsabilidades de seguridad cibernética para toda la fuerza laboral y las partes interesadas de terceros, no toda la información esta gestionada por el ERP.	
		L	3			
		L	3			
		L	3			
		L	3			
		L	3	3		4
		L	3			

Figura 1. Extracto del análisis de la Función Identificar

En la figura 2 se muestra el resumen del promedio obtenido por cada categoría con base en la ponderación descrita en la Tabla 2.

		Nivel actual	Nivel adecuado
IDENTIFICAR (DNI)	Gestión de Activos (ID.AM)	3	4
	Entorno empresarial (ID.BE)	3.38	4
	Gobernanza (ID.GV)	2.90	4
	Evaluación de riesgos (ID.RA):	3.25	4
	Estrategia de Gestión de Riesgos (ID.RM)	3.69	4
	Gestión de Riesgos de la Cadena de Suministro (ID.SC)	3.54	4
PROTEGER (PR)	Gestión de Identidad, Autenticación y Control de Acceso (PR.AC)	3.49	4
	Sensibilización y Formación (PR.AT):	3.00	4
	Seguridad de Datos (PR.DS)	3.16	4
	Procesos y Procedimientos de Protección de la Información (PR.IP)	2.98	4
	Mantenimiento (PR.MA)	3.86	4
	Tecnología de Protección (PR.PT)	3.24	4
DETECTAR (DE)	Anomalías y Eventos (DE.AE)	2.27	4
	Monitoreo Continuo de Seguridad (DE.CM)	2.69	4
	Procesos de detección (DE.DP)	2.56	4
RESPONDER (RS)	Planificación de Respuesta (RS.RP)	3.00	4
	Comunicaciones (RS.CO):	3.30	4
	Análisis (RS.AN)	2.78	4
	Mitigación (RS.MI)	3.00	4
	Mejoras (RS.IM):	2.33	4
RECUPERAR (RC)	Planificación de Recuperación (RC.RP)	3.00	4
	Mejoras (RC.IM)	3.17	4
	Comunicaciones (RC.CO):	3.00	4

Figura 2. Resumen del análisis

Los resultados se condensan en una tabla donde se observa que la empresa tiene oportunidad de mejora en las funciones Detectar y Responder que tienen

valores menores a 3 (Nivel 3 y Nivel 2) en relación a los criterios establecidos en la Tabla 2.

	Nivel Actual	Nivel adecuado
IDENTIFICAR (DNI)	3.29	4
PROTEGER (PR)	3.29	4
DETECTAR (DE)	2.51	4
RESPONDER (RS)	2.88	4
RECUPERAR (RC)	3.06	4

Figura 3. Resumen global de valoración

En la Figura 4 se muestra el resultado de cada categoría y como se encuentra en relación al nivel adecuado.

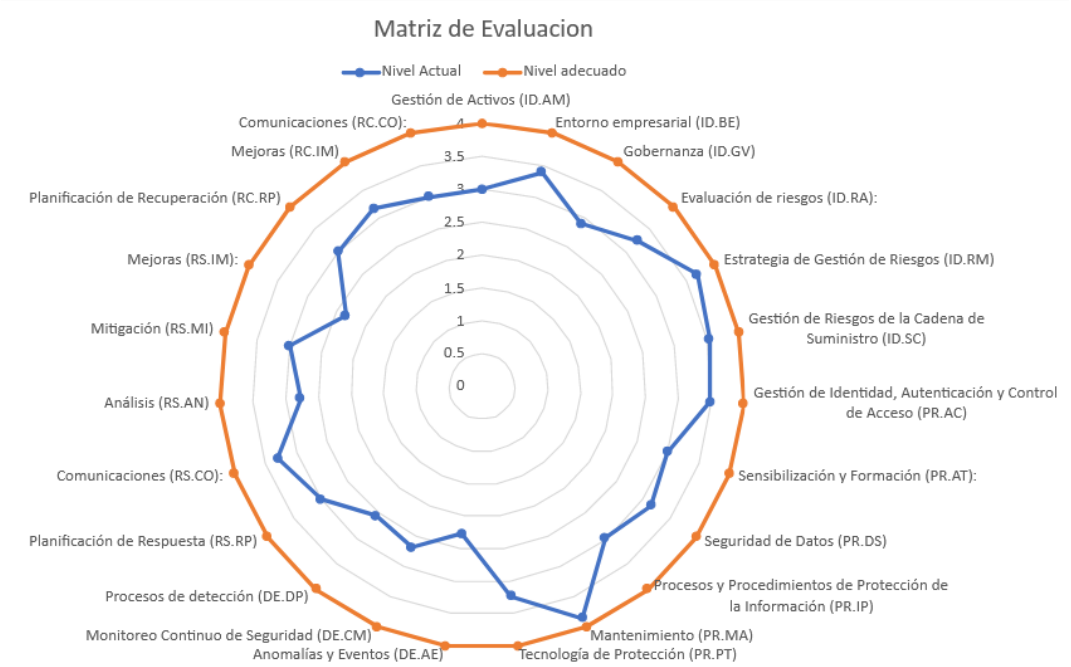

Figura 4. Resultado de valoración

En general se observa que las categorías que menor valor obtuvieron se encuentran en el Nivel 3 y son las siguientes:

- Anomalías y Eventos
- Monitoreo Continuo de Seguridad
- Procesos de detección
- Mejoras

En cambio, las categorías que mayor valor obtuvieron se encuentran en el Nivel 4 y son:

- Estrategia de Gestión de Riesgos
- Gestión de Riesgos de la cadena de suministro
- Mantenimiento

Con base en el resultado del análisis, la organización definirá en cuales categorías y/o subcategorías se priorizará la ejecución de los planes de acción considerando factores económicos, logísticos, regulatorios, de apetito de riesgo, etc.

En la Figura 5 se muestra un extracto de los análisis realizados donde se incluye planes de acción y responsables para los niveles más bajos obtenidos (Nivel 1 y Nivel 2), la información en detalle se encuentra desarrollada en el Anexo 2 Herramienta de Evaluación, Hoja: Resultados_Matriz_Evaluacion.

Función	Categoría	Medicion actual	Ponderacion Nivel Actual	Codigo	Planes de Accion	Responsable	Frecuencia
IDENTIFICAR (DNI)	**Gestión de Activos (ID.AM)**:Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización lograr los objetivos comerciales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de la organización y la estrategia de riesgo de la organización.	L	3	PL-AC-A.8.1.1	Identificar e inventariar la informacion y activos asociados a la informacion de la organizacion.	Gerente de Gestion de Activos	Anual
		L	3	PL-AC-A.8.1.2	Identificar y definir un propietario del activo de informacion	Gerente de Gestion de Activos	Anual
		L	3	PL-AC-A.8.1.1	Identificar e inventariar la informacion y activos asociados a la informacion de la organizacion.	Gerente de Gestion de Activos	Anual
		L	3	PL-AC-A.8.1.2	Identificar y definir un propietario del activo de informacion	Gerente de Gestion de Activos	Anual
					Implementar procedimientos para controlar la instalación del software en explotación, deteccion de código		

Figura 5. Controles y responsables para Niveles 1 y 2

8.2. Conclusión de la Evaluación de estado actual

La empresa tiene controles establecidos que acorde al criterio de evaluación tienen un nivel de cumplimiento 3 y 4, estos denotan la existencia de procesos ejecutados de manera dispersa según los encargados internos, es recomendable se implemente un Sistema de Gestión de la Seguridad de la Información SGSI para orquestar todos los esfuerzos realizados a fin de lograr niveles más altos de cumplimiento y seguridad para que dentro de la empresa se pueda llegar a la mejora continua.

Existen controles con Nivel 1 y 2 relacionados con la detección y monitoreo de amenazas lo cual representa una oportunidad de mejora, como parte de la implementación de un SGSI una de las sugerencias es la contratación en el corto plazo de un servicio de monitoreo de amenazas a través de un SOC.

9. Fase 2. Clasificación de la información

Para la organización la información que se genera utiliza y almacena en todos sus procesos es importante, independientemente si esta se encuentra en cualquier medio o área en específico, clasificarla es una de las tareas primordiales ya que esto ayudará a establecer cual es más crítica en relación a otra.

9.1. Tipología de impacto

Para clasificar la información se utilizará un modulador del tipo de impacto, el cual puede sufrir la organización con base en su giro de negocio y al grado de aceptación que se tenga de ellos. Se define para la organización el impacto como:

Aversión al impacto que es inaceptable.

Neutral al impacto que puede o no ser aceptado.

Agresivo al impacto que es aceptable.

Tabla 3.

Tipología de impacto.

MODULADOR DEL APETITO				
#	**Tipología de impacto (modulador)**	**AVERSION**	**NEUTRAL**	**AGRESIVO**
1	Pérdidas financieras	x		
2	Multas y sanciones de organismos de control		x	
3	Interrupción de operaciones parciales y/o totales	x		

4	Perdida/Degradación de imagen institucional	x		
5	Demandas judiciales, afectación legal		x	
6	Perdidas/ destrucción / afectación de bienes materiales		x	
7	Perdidas de vida / afectación de la salud de las personas	x		
8	Lucro cesante		x	
9	Observaciones de la auditoría interna y externa		x	
10	Afectación al clima laboral		x	x
11	Fuga o robo de información empresarial	x		
12	Desastres naturales	x		
13	Afectación a la comunidad	x		
14	Degradación de la calidad	x		

9.2. Apetito de riesgo de la organización

Es necesario definir en conjunto con la organización el apetito de riesgo que está dispuesta a aceptar, en este estudio se crea un instrumento en el cual se requiere identificar, cuantificar y detallar un nivel de perdida por cada impacto con base en categorizaciones desde la más baja “INSIGNIFICANTE” a la más alta “CATASTRÓFICA”, en la Figura 6 se muestra un extracto de la tabla donde se identificó con la organización los criterios para catalogar el apetito de riesgo del negocio.

	Niveles de impacto	CATASTROFICO	MAYOR	MODERADO
FINANCIERO	Perdidas financieras	> a 100.000,00 usd	50.00,00 < entre < 99.999,00 usd	hasta 49.000,00 usd
SANCIONES	Multas y sanciones de organismos de control		> a 100.000,00 usd	50.00,00 < entre < 99.999,00 usd
OPERACIÓN	Interrupcion de operaciones parciales y/o totales	2 Plantas de produccion	1 Planta de produccion	1 Sucursal
IMAGEN	Perdida o degradacion de la imagen institucional	Perdida de imagen con un grupo mayor de Distribuidores	Perdida de imagen con un grupo mayor de Clientes	Perdida de imagen con un grupo de la comunidad

Figura 6. Apetito de riesgo del negocio

9.3. Categorización de la información

La categorización de los tipos de información en función del impacto de la Confidencialidad, Integridad, Disponibilidad y Privacidad se utilizó para obtener la Criticidad de la información mediante relacionamiento entre ellas, los resultados basados en los criterios mencionados se encuentran en el Anexo 2 Herramienta de Evaluación, Hoja: Tipo_informacion, en la Figura 7 se muestra un extracto de la matriz utilizada en este análisis.

Num	Entidad/ Dominio	Tipo de informacion	Definicion del tipo de informacion	Propietario	Impacto Confidencialidad	Impacto Integridad	Impacto Disponibilidad	Impacto Privacidad	Calificacion de la Criticidad
1	Clientes	Personal	Nombres Completos, C.I., Género, Edad, Nacionalidad.	Asistente de ventas	MAYOR	MAYOR	MAYOR	MAYOR	MAYOR
2		Financiera	Informacion relacionada a su historial crediticio, patrimonio, pago de impuestos.	Asistente de ventas	MENOR	MENOR	MENOR	MENOR	MENOR
3		Legal	Record Policial, Información actualizada judicial(juicios).	Asistente de ventas	MENOR	MENOR	MENOR	MENOR	MENOR
4		Contacto	Numero de Teléfono, Correo Electrónico, Redes sociales.	Asistente de ventas	MODERADO	MODERADO	MODERADO	MODERADO	MODERADO

Figura 7. Categorización de los tipos de información

9.4. Conclusión Clasificación de la información

La organización puede identificar la criticidad de la información utilizando varios criterios como el impacto que puede llegar a tener si pierde dicha información, su importancia, su integridad, disponibilidad y privacidad, todos estos parámetros nos permiten clasificar la información mediante otros criterios: Secreta, Confidencial, Restringida, Uso Interno o Pública.

10. Fase 3. Identificación de activos críticos de información

Una vez que se obtuvo la Criticidad de la información de la organización, se debe definir en donde física o digitalmente se encuentra la información para identificar al activo critico que le contiene.

10.1. Modulador de niveles de impacto

Al igual que en los tipos de información, se requiere definir un modulador de niveles de impacto que permita calificar al activo que lo contiene para catalogarlo de acuerdo a los criterios a utilizar, a continuación en la Tabla 4 se lista las categorías:

Tabla 4.

Niveles de impacto para la evaluación activos

NIVELES DE IMPACTO	
1	INSIGNIFICANTE
2	MENOR
3	**MODERADO**
4	**MAYOR**
5	CATASTROFICO

10.2. Identificación de activos

Los activos a clasificar pueden ser físicos (hardware), lógicos (unidades de disco virtualizado), software (Programas, Aplicaciones), etc., cada uno de ellos puede contener varios tipos de información, un custodio o un responsable.

Con base en el modulador de niveles de impacto de la Tabla 4 se clasificará a los activos y sus elementos, el resultado se obtendrá relacionando el impacto entre cada uno de ellos obteniendo un resultado general para cada activo, este resultado esta categorizado desde lo más crítico “CATASTRÓFICO” hasta lo más bajo “INSIGNIFICANTE” en el Anexo 2 Herramienta de Evaluación, Hoja: Activos_Informacion, se muestra una captura de la matriz de clasificación utilizada en el análisis.

Num	Codificacion	Nombre del Activo	Nombre del tipo de informacio	Descripcion del tipo de informacion	Nivel de impacto	Custodio	Criticidad Activo
1	SIS-001	SISTEMA ERP	Informacion del cliente	Informacion comercial del cliente que contiene nombres completos, cedula, direccion, informacion de contacto, RUC, razon social,	MAYOR	Asistente de ventas	CATASTROFICO
			Informacion crediticia	Informacion relacionada con el ambito crediticio utilizada para generar cupos de credito interno.	MAYOR	Analista de credito	
			Informacion legal	Informacion legal de la organizacion, clientes, empleados, personal relacionado con la organizacion.	MAYOR	Asistente juridico	
			Informacion de estrategia comercial	Informacion registrada para toma de decisiones relacionadas a al estrategia comercial.	MAYOR	Gerente Comercial	
			Procesos logisticos	Informacion de procesos de logistica.	CATASTROFICO	Asistente de logistica	

Figura 8. Clasificación de los activos de información.

11. Conclusión de la Identificación de Activos críticos de la información.

Con base en la clasificación de los activos se identifica varios activos que tienen un resultado de “CATASTROFICO”, estos son los activos críticos de información y son los que contienen información de vital importancia para la organización y con base en el apetito de negocio su impacto es mayor, para el análisis de este proyecto se ha seleccionado dos de los activos considerados como críticos.

12. Fase 4. Análisis de amenazas y vulnerabilidades.

12.1. Análisis de amenazas y vulnerabilidades para activos críticos

Una vez identificado los activos críticos de información se realiza un análisis de amenazas y vulnerabilidades que permita identificar lo que se va a proteger, no necesariamente la organización dispone del presupuesto para proteger todos los activos, la inversión que sea autorizada debe ser justificada y basada en la severidad del riesgo que se encuentre como resultado de la evaluación.

Para el análisis se crea una matriz basada en la metodología de MAGERIT versión 3.0 donde se utiliza la taxonomía de evaluación, las amenazas y salvaguardas aplicables para identificar las vulnerabilidades del activo critico de información. (Publicas, 2012)

De acuerdo al alcance del proyecto, se ha seleccionado dos activos críticos para realizar el análisis:

- Servidor Core.
- Switch Core

12.2. Criterios de evaluación.

Para obtener una valoración se utilizará el criterio de severidad que tienen las vulnerabilidades asociadas al activo crítico, se considera la probabilidad de ocurrencia del evento descrito en la Tabla 5.

Tabla 5.

Probabilidad de Ocurrencia

	Cuantitativo	Cualitativo	Descripción
PROBABILIDAD	1	RARO	Una vez al año
	2	POCO PROBABLE	Dos veces al año
	3	POSIBLE	Tres veces al año
	4	PROBABLE	Una vez al mes
	5	CASI CERTEZA	Dos veces al mes

Para obtener el grado o nivel de severidad para la evaluación se realiza una matriz donde se clasifica en función de los dos parámetros, probabilidad versus impacto, la cual se muestra en la Tabla 6.

Tabla 6.

Matriz de severidad

PROBABILIDAD	CASI CERTEZA	MODERADO	MODERADO	ALTO	CATASTROFICO	CATASTROFICO
	PROBABLE	MODERADO	MODERADO	ALTO	ALTO	CATASTROFICO
	POSIBLE	BAJO	MODERADO	MODERADO	ALTO	CATASTROFICO
	POCO PROBABLE	BAJO	BAJO	MODERADO	ALTO	ALTO
	RARO	BAJO	BAJO	MODERADO	MODERADO	ALTO
		INSIGNIFICANTE	MENOR	MODERADO	**MAYOR**	CATASTRÓFICO

IMPACTO

La severidad es el producto entre la probabilidad de ocurrencia por el impacto que afecta al activo crítico, la valoración realizada es en función de los riesgos propios al giro de negocio de la empresa, en la Tabla 6 se muestra los criterios utilizados para su valoración.

Tabla 7.

Matriz de severidad

SEVERIDAD	
BAJO	Evento de riesgo que no implica pérdidas financieras, no se incurre en multas de organismos de control, no afecta a la operación e imagen de la empresa, no existe afectación a la salud de las personas y la comunidad y no se afecta a la ventaja competitiva.
MODERADO	Evento de riesgo que no implica pérdidas financieras, se incurre en multas de organismos de control, no afecta a la operación e imagen de la empresa, existe afectación parcial a la salud de las personas y no con la comunidad y no se afecta a la ventaja competitiva.
ALTO	Evento de riesgo que implica pérdidas financieras, se incurre en multas de organismos de control, afecta parcialmente a la operación e imagen de la empresa, existe afectación parcial a la salud de las personas y a la comunidad y no se afecta a la ventaja competitiva.
CRITICO	Evento de riesgo que implica pérdidas financieras, se incurre en multas de organismos de control, afecta a la operación e imagen de la empresa, existe afectación a la salud de las personas y la comunidad y se afecta a la ventaja competitiva.

12.3. Evaluación inicial de riesgos

La evaluación de riesgos para los activos críticos se realiza con base en una matriz donde por cada activo se desglosa sus componentes y las amenazas más comunes tomadas del marco de referencia MAGERIT,

Los riesgos son clasificados de acuerdo a la realidad de la empresa y las vulnerabilidades que pueden explotar estas amenazas con su impacto inherente para onbtener una evaluación inicial de la severidad por cada componente del activo de información, los resultados se muestran en el Anexo 2 Herramienta de Evaluación, Hoja: Matriz_Riesgos.

						Riesgo Inherente		
Activo	**Tipo**	**Amenaza**	**Vulnerabilidades**	**Impacto en Seguridad**	**Impacto Organizacional**	**Impacto RI**	**Probabilidad RI**	**Severidad RI**
Servidor Core	Hardware	Daño físico en arreglos de discos del servidor.	Ausencia de monitoreo de log de eventos.	Disponibilidad	Financiero / Imagen / Operación	Mayor	Muy Alta	Crítico
			Mantenimiento inadecuado de los servidores.	Disponibilidad	Financiero / Imagen / Operación	Mayor	Muy Alta	Crítico

Figura 9. Captura de la evaluación inicial de riesgos

Como resultado de la evaluación, se obtiene un nivel de severidad categorizado como: CRITICO, ALTO, MODERADO y BAJO, estos resultados sirven como primer elemento de análisis para enfocar los esfuerzos para atacar en el corto o mediano plazo la vulnerabilidad mediante controles.

12.4. Evaluación de controles existentes

La organización tiene varios controles implementados que se han tomado como evidencia y se evalúan en función de si estos son:

- Automáticos o manuales
- Preventivos, detectivos, correctivos o una mezcla de ellos
- Planificados o a demanda.

La existencia de uno o varios de ellos se utiliza para evaluar la fortaleza del control, es decir, para evaluar si los controles son débiles o fuertes, para mitigar, contener o reducir una amenaza se cuenta el número de controles y se tabula los resultados en función del Anexo 2 Herramienta de Evaluación, Hoja: Controles_existentes.

Como resultado de este análisis se obtiene una matriz de clasificación del riesgo inherente versus los controles actuales, una calificación “Crítica” muestra que los

controles existentes son débiles y es necesario reforzar los existentes, crear nuevos controles para que el impacto del riesgo inherente se reduzca, controle o mitigue, los resultados completos se encuentran en el Anexo 2 Herramienta de Evaluación, Hoja: Controles_existentes, a continuación, se muestra una captura del análisis realizado.

				Riesgo Inherente	Evaluacion de controles existentes				
Activo	**Tipo**	**Amenaza**	**Vulnerabilidades**	**Severidad RI**	**Controles existentes**	**Tipo de Control**	**Clasificación de Control**	**Frecuencia de Control**	**Nivel del Riesgo Residual**
Servidor Core	Hardware	Daño fisico en arreglos de discos del servidor.	Ausencia de monitoreo de log de eventos.	Crítico	Se revisa los logs de eventos.	Manual	Correctivo	Semestral	Alto
			Mantenimiento inadecuado de los servidores.	Crítico	Se realiza mantenimientos de equipos.	Manual	Correctivo	Semestral	Alto

Figura 10. Evaluación de controles existentes

12.5. Tratamiento de los riesgos

Para el tratamiento de los riesgos inherentes se plantean implementar controles o reforzar los existentes, incrementar su frecuencia, automatizarlos de ser posible y que estos sean preventivos, detectivos o correctivos. Como resultado del tratamiento se espera que el nivel de los riesgos inherentes baje de nivel o se mantengan controlados, el detalle de los controles establecidos se muestra en el Anexo 2 Herramienta de Evaluación, Hoja: Controles_existentes

			Tratamiento de los riesgos					
Activo	**Tipo**	**Nivel del Riesgo Residual**	**Controles a implementar**	**Tipo de Control**	**Clasificación de Control**	**Frecuencia de Control**	**Nivel de Riesgo Objetivo**	**Plan de Acción**
Servidor Core	Hardware	Alto	Revisión periódica de logs de eventos.	Manual	Preventivo	Semanal	Bajo	Monitorear y notificar de forma automatizada ante una alerta de error en el sistema del Servidor que permite realizar una acción rápida.
		Alto	Mantenimiento de equipos de manera peródica	Manual	Preventivo	Semestral	Moderado	Realizar el mantenimiento preventivo a los equipos de forma periódica y llevar un control de los mismos que permita automatizar el proceso de notificaciones.

Figura 11. Tratamiento de los riesgos.

13. Fase 5. Desarrollo de políticas de alto nivel

La organización requiere el desarrollo de políticas de alto nivel para que sean los pilares en donde el SGSI va a regirse, el programa deberá alinear las estrategias y planes de acción para mitigar las vulnerabilidades obtenidas de todo el sistema, estas políticas requieren que exista un responsable que debe promover el cumplimiento, ejecutar acciones, mostrar indicadores, generar acciones correctivas y alcanzar la mejora continua.

13.1. Revisión

Las políticas se desarrollaron tomando como referencia los Controles de la ISO/IEC 27001 y se adaptaron a la organización considerando los que son aplicables, que fueron en su totalidad.

Las políticas aplican tanto para los activos que se catalogaron en su etapa inicial como críticos, y los que en el futuro se vayan agregando o evaluando o mejorando, a continuación se muestra un extracto de las políticas desarrolladas para la empresa, el desarrollo completo se encuentra en el Anexo 3 Políticas de alto nivel.

13.2. Conclusión

El desarrollo de políticas de alto nivel no solamente debe estar ligado a los activos críticos ya que la evaluación es una fotografía en este momento de la realidad de la organización, se requiere una política que englobe la mayor cantidad de controles aplicables y que permita tener un responsable y aplicar priorización en la ejecución de las mismas.

Una correcta definición de las políticas debe realizarse en conjunto con la organización para que estén alineadas a sus objetivos estratégicos y puedan ayudar y no limitar su operación.

14. Conclusiones y recomendaciones

14.1. Conclusiones

La medición del estado actual de la seguridad de la información es necesaria para conocer el estado actual de los controles existentes en la empresa, nos da una pauta sobre la existencia de un inventario de activos y la evaluación de las amenazas y vulnerabilidades que afecten a dichos activos.

La clasificación de los activos de información por criticidad ayuda a la empresa a definir y seleccionar las acciones a realizar con base en el apetito de riesgo con base en criterios establecidos sea para tratar el riesgo o mantenerlo presente.

La matriz de riesgos es importante ya que se describen riesgos que afectan a las empresas de acuerdo a su giro de negocio, a la naturaleza de la industria, su interacción con el medio ambiente y comunidad, el marco regulatorio que aplique e inclusive las nuevas tendencias a las que la empresa pueda migrar o incluir.

La implementación de un SGSI permite mantener procesos continuos, medibles y sostenibles en el tiempo con el objetivo de precautelar la información de la empresa, teniendo en cuenta como factor principal el apoyo de la alta gerencia en el ciclo de vida del programa.

14.2. Recomendaciones

La iniciativa de la empresa en cuanto a mejorar la protección de la información generada en sus procesos es importante, ya que la información es transversal en toda la organización e involucra a personal dueño del proceso para que sea responsable de la custodia de la información, independientemente como se genere, el área técnica, Sistemas o Tecnología de la empresa debe proveer los recursos necesarios para que los objetivos empresariales se cumplan, por eso es importante que se realice un inventario de activos de información y que haya una sinergia entre departamentos con el fin de que el bien más preciado para la empresa pueda ser protegido,

Todo proceso debe ser medible en el tiempo, el SGSI requiere una constante medición con el objetivo de alcanzar una mejora continua, el SGSI no es un

proyecto que tiene principio y fin, es un programa que requiere desde la delegación de autoridad, presupuesto y medidores de cumplimiento para que pueda ser sostenible en el tiempo y se mantenga vigente ante las amenazas nuevas que surjan durante la vida de la empresa.

Bibliografía

Comercio, C. F. (2022). *Marco de ciberseguridad del NIST*. Obtenido de https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

ESET, L. (15 de 11 de 2022). *Guía básica de seguridad IT para PYME en 6 pasos.* Obtenido de DataSecurityGuide.eset.com: WeLiveSecurity.com/latam

INCIBE, I. N. (2016). *Tendencias en el mercado de la Ciberseguridad.* Madrid: INCIBE Ministerio de Industria, energia y turismo.

ITAhora. (octubre de 2022). *https://itahora.com/2022/10/17/ataques-de-ciberseguridad-crecen-en-un-400/*. Obtenido de https://itahora.com/2022/10/17/ataques-de-ciberseguridad-crecen-en-un-400/

Publicas, M. d. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

UNE, A. E. (2017). *UNE-EN ISO/IEC 27001.* Genova: AENOR Internacional S.A.U.

Índice de Tablas

Índice de Figuras

ANEXOS

Anexo 1. Caso de negocio.

Anexo 2 Herramienta de Evaluación, Hoja: Resultados_Matriz_Evaluacion

Anexo 2. Herramienta de Evaluación, Hoja: Tipo_informacion

Anexo 2. Herramienta de Evaluación, Hoja: Matriz_Riesgos

Anexo 2. Herramienta de Evaluación, Hoja: Controles_existentes

Anexo 3. Políticas de alto nivel.