FACULTAD DE POSTGRADOS

PROYECTO CAPSTONE: DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA ORGANIZACIÓN “VENTA CONSULTIVA DE TECNOLOGIA”

AUTORES

PAÚL FROILAN CONDO ESPINOZA

SEGUNDO JAVIER CAYO MOLINA

AÑO

2022

FACULTAD DE POSGRADOS

PROYECTO CAPSTONE: DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA ORGANIZACIÓN “VENTA CONSULTIVA DE TECNOLOGIA”

“Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el titulo MAGISTER EN GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN”

AUTORES:

PAUL CONDO

JAVIER CAYO

AÑO

2022

DECLARACIÓN DE AUTORÍA

"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."

PAÚL FROILAN CONDO ESPINOZA

CI: 1720662327

SEGUNDO JAVIER CAYO MOLINA

CI: 0502676968

DEDICATORIA

El presente trabajo dedico a mis hijos a mi esposa, su apoyo, parte fundamental de todos los logros.

A mis padres, sus consejos y bendiciones guían mis pasos.

Javier

RESUMEN

En la actualidad el avance tecnológico trae consigo desafíos que generan preocupaciones a los altos niveles organizacionales, garantizar un máximo nivel de disponibilidad, integridad y confidencialidad de la información en las organizaciones es un aspecto de gran importancia que se debe tener en cuenta dentro de las actividades cotidianas.

El presente proyecto, tiene como objetivo dar a conocer las diferentes fases que debe considerar la organización para implementar un sistema de gestión de seguridad de la información.

El alcance del proyecto contempla 5 fases, las que se detallan a continuación:

- Diagnóstico
- Clasificación de la información
- Inventario de activos
- Análisis de amenazas y vulnerabilidades
- Documentación

Para el desarrollo del proyecto se ha realizado con base en marcos de referencia y normas como ISO 27001, NIST, los mismos que ayudarán a llevar una gestión adecuada de la seguridad de la información en la organización.

Abstract

At present, technological progress brings with it challenges that generate concerns at high organizational levels, guaranteeing a maximum level of availability, integrity and confidentiality of information in organizations is an aspect of great importance that must be taken into account within the activities everyday.

This project aims to publicize the different phases that the organization must consider to implement an information security management system.

The scope of the project includes 5 phases, which are detailed below:

- Diagnostics
- Information Classification
- Actives' inventory
- Analysis of threats and vulnerabilities
- Documentation

For the development of the project, it has been based on reference frameworks and standards such as ISO 27001, NIST, which will help to carry out an adequate management of the information security in the organization.

Contenido

INTRODUCCIÓN

La organización de venta consultiva de tecnología, con enfoque a la venta de soluciones informáticas, en la actualidad se ha visto expuesta a una serie de ataques informáticos debido a vulnerabilidades de seguridades dentro de la institución, como ingeniería social, elevación de privilegios, denegación de servicio, ransomware, ingeniería social.

A partir de los hallazgos y la evaluación de los activos informáticos, se propone un Programa de Sistema de Gestión de la Seguridad Información, con el fin de mejorar la seguridad de la información en la organización.

Al implementar el SGSI uno de los factores importantes que se busca es la mejora continua, esto ayudará a evaluar, detectar y reducir las amenazas y riesgos que pueden afectar a la información. Se debe transformar en un ciclo que se repite, con nuevas implementaciones en seguridad, monitoreo, control continuo y ajustes permanentes para lograr un nivel alto de seguridad de la información en la organización.

El SGSI requiere que todos los miembros de la organización estén involucrados para que haya un cambio de mentalidad, de esta forma la seguridad pase a ser uno de los componentes más importantes en cualquier proceso o actividad de la organización.

14. DESARROLLO DEL PROGRAMA

14.1. Objetivo

El objetivo de este proyecto es desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI), tomando como referencia la norma ISO27001 y NIST, con lo cual se pretende mejorar la seguridad de la información en la organización de venta consultiva de tecnología.

14.1.1. Objetivos específicos

- Reducir el riesgo de que se produzca perdida de información en la organización.
- Evitar filtrado de información y accesos no autorizados
- Reducir el gasto operativo frente a incidentes de seguridad
- Establecer responsabilidades, roles y competencias basados en las buenas prácticas de seguridad de la información
- Crear cultura de seguridad de información en la organización.
- Diseñar medidas de seguridad para que los colaboradores, clientes y proveedores puedan acceder a la información de forma segura y controlada.
- Ofrecer continuidad de operación y servicio con normalidad o en el menor tiempo posible en el caso de producirse problemas importantes, tales como ataques de ramsonware, phishing, exploits.

14.1.2. Alcance

Para diseñar el SGSI, el proyecto está enfocado en los procesos de la organización, se tomó como referencia la norma ISO 27001 que cuenta con un ciclo PHVA (Planear, hacer, verificar, actuar) y el marco NIST que se enfoca en (Identificar, proteger, detectar, responder, recuperar), las mismas que nos permiten definir procesos que sean afines al SGSI.

Esto nos permitirá tener un estado de situación actual de la organización con relación a la seguridad de la información.

Para desarrollar el proyecto según los objetivos planteados se trabajará en cinco fases que se puede visualizar en la figura 1.

Figura 1 Fase Desarrollo SGSI

La implantación del SGSI, es una decisión estratégica para la organización siempre enfocado en asegurar la confidencialidad**,** integridad y disponibilidad de la información. El SGSI permitirá identificar y detectar posibles amenazas para prevenir su materialización que pongan en riesgo la seguridad de la información en la organización.

14.2. FASE 1 DIAGNÓSTICO

Antes de iniciar con el diagnóstico de SGSI se va a realizar una breve definición de herramientas y conceptos que se usaran para el desarrollo del proyecto

14.2.1. ISO 27001

"ISO 27001 es una norma desarrollada por ISO (organización internacional de Normalización) con el propósito de ayudar a gestionar la Seguridad de la Información en una empresa."

La nomenclatura exacta de la Norma actual es ISO/IEC 27001 que es la revisión de la norma en su primera versión que fue publicada en el año 2005 como una adaptación de ISO de la norma británica BS 7799-2.

"El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa." Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

"Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente."

(Advisera Expert Solutions Ltd, 2022)

14.2.2. NIST

El marco para la mejora de la seguridad cibernética en infraestructuras críticas, mejor conocida en inglés como NIST Cibersecurity Framework, fue emitida inicialmente en los Estados Unidos en febrero de 2.014.

La orientación del marco es ayudar a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporcionando un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

Figura 2 Marco Nist

(Villamizar, 2020)

14.2.3. Metodología

En esta fase de evaluación se ha considerado utilizar la norma ISO27001 y el marco NIST, partiendo del análisis de la situación actual de la organización, al revisar los diferentes esquemas de las normas nos permitirá identificar los puntos de cumplimiento y determinar el nivel de madurez en la que se encuentra la organización.

14.2.4. Diagnóstico

En la fase de diagnóstico permitirá conocer el estado actual de la organización, con relación a la seguridad de la información, para ello se ha realizado un mapeo entre la norma ISO27001 y el marco NIST, se ha realizado una evaluación con

la ayuda de los encargados de las diferentes áreas de la organización, con lo que se ha logrado obtener un estado de situación inicial.

14.2.5. Estado de situación actual

Para obtener el estado de situación actual de la organización, se ha diseñado una herramienta de evaluación del nivel de madurez de la seguridad de la información en el que se encuentra actualmente, se definió los siguientes parámetros de evaluación:

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Tabla 1Tabla de madurez del modelo de seguridad de la información.

En la tabla 2 se encuentra la escala para evaluar el cumplimiento de las normas, en la misma se divide en tres niveles, crítico (0% - 35%), intermedio (36% - 70%), suficiente (71% - 100%)

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Tabla 2 Tabla de Cumplimiento de normas

En la tabla 3 podemos observar la evaluación de la sección identificar del marco NIST y la norma ISO27001.

IDENTIFICAR			
MARCO DE REFERENCIA NIST			CUMPLIMIENTO A.
ID	SUBCATEGORIA	CONTROLES ACTUALES	31%
ID.AM-1	Se inventarian los dispositivos y sistemas físicos dentro de la organización.	se cuenta con un inventario de equipos y la respectima asigna	75
		cuenta con propietario la asignación de los equipos	75
ID.AM-2	Se inventarian las plataformas y aplicaciones de software dentro de la organización.	se cuenta con un inventario de equipos y la respectima asigna	75
		cuenta con propietario la asignación de los equipos	75
ID.AM-3	La comunicación organizacional y los flujos de datos están mapeados	No cuenta con politicas de intercambio de información	0
			0

Tabla 3 Tabla Nist Identificar

En la tabla 4 podemos observar la evaluación la sección proteger de la ISO27001 y marco NIST.

PROTEGER			
MARCO DE REFERENCIA NIST			CUMPLIMIENTO A.
ID	SUBCATEGORIA	CONTROLES ACTUALES	29%
PR.AC-1	Las identidades y las credenciales se emiten, gestionan, verifican, revocan y auditan para dispositivos, usuarios y procesos autorizados.	Se encuentra establecido un control de acceso en general pero no existe un procedimiento de asignacion de los derechos	40
		se cuenta con un control NO formal para revocación y elimina	40
		no se maneja es un unico role con accesos limitados	0
		Se maneja un control por parte de cambio de claves cada 90	60
		se cuenta con un control no formal de retiro de accesos cuando el personal sale de la organización	40

Tabla 4 Tabla Nist Proteger

En la tabla 5 podemos observar la evaluación de la sección detectar de la ISO27001 y marco NIST.

DETECTAR			
MARCO DE REFERENCIA NIST			CUMPLIMIENTO A.
ID	SUBCATEGORIA	CONTROLES ACTUALES	25%
DE.AE-1	Una línea de base de operaciones de red y flujos de datos esperados para usuarios y sistemas se establece y gestiona	Se cuenta con politica de procedimientos operacionales disponibles para los usuarios para el tratamiento de la información	40
			40
		Se realizan controles y segmentaciones de red y restricciones entre la segmentación	40
			40

Tabla 5 Tabla Nist Detectar

En la tabla 6 podemos observar la evaluación la sección responder de la ISO27001 y marco NIST.

RESPONDER			
MARCO DE REFERENCIA NIST			CUMPLIMIENTO A.
ID	SUBCATEGORIA	CONTROLES ACTUALES	12%
RS.RP-1	El plan de respuesta se ejecuta durante o después de un incidente	Cuenta con un plan de recuperación de respaldo no se tiene definido rpo y rto	5
RS.CO-1	El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	Es un proceso reactivo sin asignación de responsabilidades la persona a cargo de TI, es la encargada de realizar la recuperación	0
		Cuenta con control de capacitación a empleados y proveedores respecto a politicas y procedimientos según las responsabilidades de su cargo	0
		No se establece responsabilidades y procedimientos para incidentes de seguridad de información	0

Tabla 6 Tabla Nist Responder

En la tabla 7 podemos observar la evaluación de la sección recuperar de la ISO27001 y marco NIST.

RECUPERAR			
	MARCO DE REFERENCIA NIST		CUMPLIMIENTO A.
ID	SUBCATEGORIA	CONTROLES ACTUALES	28%
RC.RP-1	El plan de recuperación se ejecuta durante o después de un incidente de ciberseguridad	Cuenta con un plan de recuperación de respaldo no se tiene definido rpo y rto	5
RC.IM-1	Los planes de recuperación incorporan lecciones aprendidas	No se cuenta con lecciones aprendidas	0
RC.IM-2	Las estrategias de recuperación se actualizan	no cuenta con analisis de riesgos referente a incidentes de seguridad	0

Tabla 7 Tabla Nist Recuperar

Figura 3 Nivel de Madurez NIST

#	DOMINIO	Calificación Actual
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	14
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	31
A.8	GESTION DE ACTIVOS	61
A.9	CONTROL DE ACCESO	17
A.10	CRIPTOGRAFIA	0
A.11	SEGURIDAD FISICA Y DEL ENTORNO	30
A.12	SEGURIDAD DE LAS OPERACIONES	30
A.13	SEGURIDAD DE LAS COMUNICACIONES	26
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	26

A.15	RELACIONES CON LOS PROVEEDORES	50
A.16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	8
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DEL NEGOCIO	19
A.18	CUMPLIMIENTO	10
PROMEDIO EVALUACIÓN DE CONTROLES		**23**

Tabla 8 Nivel de Madurez ISO

Para ver con más detalle la evaluación de nivel de madurez referenciar a documento Herramienta de evaluación.xlsx pestaña dominios Nist – Iso

14.2.6. RESULTADOS

Como resultado de la evaluación, podemos concluir lo siguiente:

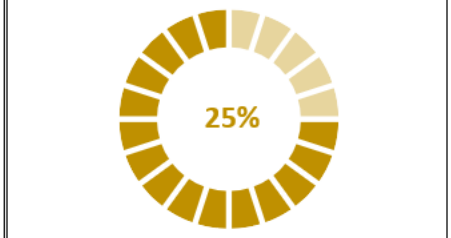
- La organización no cuenta con un área para la seguridad de la información.
- La organización actualmente maneja de manera informal la seguridad de la información, y no se rige por un gobierno.
- Basado en el proceso de evaluación con la norma ISO27001 y el marco NIST, la organización se encuentra en un nivel de madurez inicial de 25 %, donde no cuenta con identificación de activos, gestión de riesgos por lo cual no permite determinar el grado de criticidad de la información, los controles no están alineados a la preservación de la integridad, disponibilidad, confidencialidad y privacidad de la información.

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	INTERMEDIO
Repetible	CRÍTICO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Tabla 9 Tabla Nivel de madurez por nivel de cumplimiento

En la tabla 10 se puede observar el resultado de la evaluación de la organización.

MODELO EVALUACIÓN NIST				
ETIQUETAS	CALIFICACIÓN ENTIDAD		NIVEL ESPERADO	NIVEL IDEAL
IDENTIFICAR	31%		60%	100%
PROTEGER	29%		60%	100%
DETECTAR	25%		60%	100%
RESPONDER	12%		60%	100%
RECUPERAR	28%		60%	100%
MADUREZ	25%			



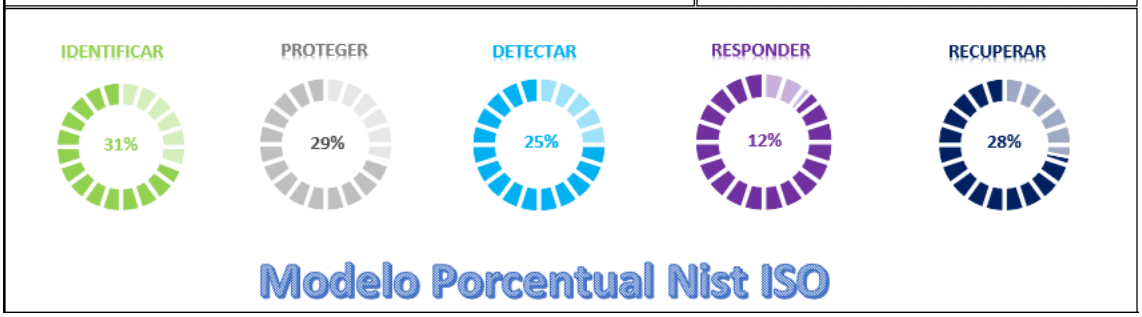


Tabla 10 Tabla Resultado General de Evaluación

Para visualizar la herramienta de evaluación completa, revisar el Anexo 1.

1. Herramienta de Evaluación (Dominios Nist Iso).xlsx
2. Herramienta de Evaluación Madurez SGSI- Pestaña (Revisión Inicial).xlsx

14.3. FASE 2 CLASIFICACIÓN DE LA INFORMACIÓN

14.3.1. Metodología

La clasificación de la información para un SGSI es un proceso de mucha importancia, el cual nos permite realizar una evaluación de los datos que posee la organización y la protección que cada uno requiere. Es considerado uno de los aspectos complejos pero interesantes de la gestión de seguridad de la información.

Para realizar la clasificación de información, se debe iniciar con la recopilación de la información de la organización en un inventario al cual se denomina activos, en el que se toma en cuenta los siguientes aspectos: quien lo posee y en qué tipo de formato está, por ejemplo, documentos electrónicos, bases de datos, documentos en papel o almacenamiento magnético.

Una vez realizado el inventario se realiza una clasificación de la información, para esto se sigue parámetros según las buenas prácticas en términos de confidencialidad, es decir, según a quien se le otorga acceso a la información.

Se incluye cuatro niveles de confidencialidad que se detalla a continuación:

- Secreto
- Confidencial
- Uso interno
- Publico

En la tabla 11 se puede observar la clasificación de la información en la organización.

Dominio de información	Nombre del tipo de información	Etiqueta confidencialidad	Dueño de la entidad
Cliente Persona Jurídica	Información General de cliente persona jurídica	**Confidencial**	Financiero, comercial, logística
	Información bancaria	**Secreto**	Financiero, comercial
	Información de implementaciones	**Secreto**	Cliente jurídico
	Información de contacto	**Uso interno**	Financiero, comercial
Prospecto de Clientes	Información general de prospecto de clientes	**Público**	Financiero, comercial
	Información de contacto prospecto de clientes	**Público**	Financiero, comercial
Empleados	Información general de empleados	**Uso interno**	Recursos humanos, financiero
	Información de contacto de empleados	**Confidencial**	Recursos humanos
	Información médica de empleados	**Uso interno**	Recursos humanos, área médica
	Información bancaria de los empleados	**Confidencial**	Recursos humanos, financiero, empleado
	Información financiera	**Confidencial**	Recursos humanos, financiero, empleado
Proveedores	Información general de proveedores	**Uso interno**	Comercial, financiero
	Información de contacto de proveedores	**Uso interno**	Comercial, financiero
	Información bancaria de los proveedores	**Confidencial**	Financiero, proveedor
	Información de productos del proveedor	**Confidencial**	Comercial
Socios	Información general de socios	**Uso interno**	Financiero, legal
	Información de contacto de socios	**Uso interno**	Financiero, legal
	Información financiera de los socios	**Confidencial**	Financiero, socio
	Acuerdos de la organización con los socios	**Confidencial**	Legal
Organización	Información general de la organización	**Uso interno**	Marketing

	Información de ubicabilidad de la organización	**Público**	Marketing
	Información de sucursales	**Público**	Cliente jurídico
Ex-clientes	Información general de cliente persona Jurídica	**Público**	Comercial
	Información bancaria	**Público**	Comercial
	Información de contacto	**Público**	Comercial

Tabla 11 Clasificación de la Información

Basados en la matriz de impacto, se hace referencia a estándares que se revisó con la organización con base a los requerimientos, los valores recolectados y sus pérdidas estimadas para cada tipo de impacto, se detalla en la tabla 12.

Niveles	Pérdidas financieras	Multas y sanciones de los Organismos de Control	Interrupción de operaciones	Salud de las personas	Pérdida de contratos
Catastrofico	≥ 200000	Proveedor incumplido	≥ 3 semana	Muerte	≥ 200000
Mayor	De 100000 a 199000	1 * 1000 del valor del contrato	De 1 a 2 semanas	Enfermedad catastrófica	De 100000 a 199000
Moderado	De 50000 a 99999	De 5000 a 10000	De 1 a 5 días	Hospitalización	De 50000 a 99999
Menor	De 5000 a 49999	De 1000 a 4999	De 1 día		De 5000 a 49999
Insignificante	≤ 49999	≤ 4999	≤ 1 día		≤ 49999

Tabla 12 Niveles de tolerancia

Como parte de la clasificación de tipos de información de la organización se ha realizado una evaluación en base a criterios de impacto y en aspectos de confidencialidad, integridad y disponibilidad con una criticidad total que nos ayudara a proteger la información crítica.

En la tabla 13 se puede observar la evaluación de los tipos de información.

Dominio de información	Nombre del tipo de información	Disponibilidad	Integridad	Confidencialidad	Cumplimiento	Criticidad Total
Cliente Persona Jurídica	Información General de cliente persona Juridica	Moderado	Catastrofico	Mayor	Mayor	Mayor
	Información Bancaria	Catastrofico	Catastrofico	Catastrofico	Moderado	Catastrofico
	Información de implementaciones	Menor	Catastrofico	Catastrofico	Mayor	Catastrofico
	Información de contacto	Menor	Mayor	Mayor	Menor	Moderado
Prospecto de Clientes	de Clientes	Menor	Menor	Menor	Menor	Menor
	Prospecto de Clientes	Menor	Menor	Menor	Menor	Menor
Empleados	empleados	Moderado	Moderado	Moderado	Menor	Moderado
	empleados	Mayor	Mayor	Mayor	Menor	Mayor
	empleados	Moderado	Moderado	Catastrofico	Menor	Moderado
	empleados	Mayor	Catastrofico	Catastrofico	Mayor	Mayor
	Información Financiera	Mayor	Mayor	Catastrofico	Mayor	Mayor
Proveedores	proveedores	Moderado	Mayor	Moderado	Moderado	Moderado
	proveedores	Moderado	Moderado	Mayor	Menor	Moderado
	proveedores	Mayor	Catastrofico	Catastrofico	Moderado	Mayor
	proveedor	Mayor	Mayor	Mayor	Moderado	Mayor

Tabla 13 Evaluación de tipos de Información

Para visualizar con más detalle hacer referencia en el Anexo 1 el documento Herramienta de Evaluación.xls Pestaña dominios de información.

14.3.2. Resultados

En base al levantamiento de información realizado y la segmentación, clasificación de información se logró identificar con los parámetros de medición los índices de criticidad de cada uno de ellos, esto permitirá segmentar lo activos de información más críticos con el fin de implementar controles y políticas de protección en seguridad de la información lo que ayudará a mejorar la integridad, confidencialidad y disponibilidad.

Para visualizar la clasificación de la información, revisar el Anexo 1.

Herramienta de Evaluación (Pestaña Dominios de Información).xlxs

14.4. FASE 3 INVENTARIO DE ACTIVOS DE INFORMACIÓN

14.4.1. Metodología

La identificación de activos críticos va de la mano con la clasificación de información que se revisó en la fase anterior.

En donde nos ayudamos con la clasificación de información para determinar el flujo o el proceso que sigue la información y donde se encuentran contenidas.

En la tabla 14 se observa los activos de información que fueron identificados en la organización, a los que se asignó una nomenclatura para ser identificados con facilidad.

Código	Codificación	Nombre de Activo de Información	Tipo de información	Clasificación Tipo de Información
1	SAP-PRODU-06	BASE DE DATOS	Modulo de Finanzas	Catastrofico
			Modulo de Recursos Humanos	Mayor
			Modulo de Logística	Mayor
2	SAP-PRODU-06	SERVIDOR SAP-PRODU-06	Base de Datos Sap	Catastrofico
			Aplicación SAP	Catastrofico
6	SAPROUTER	SERVIDOR DE CONEXIÓN REMOTA	Conexión Aplicación SAP	Catastrofico
	ARANDA-BDD	SERVIDOR ARANDA BDD	Base de Datos Mesa de Ayuda	Catastrofico
7	ARANDA-BDD	BASE DE DATOS MESA DE AYUDA	Registro de usuarios	Mayor
			Gestión de tickets	Mayor
			Seguimiento de Tickets	Mayor
			Reporte de Incidentes	Menor
			Registro de Tiempos	Mayor
			Gestón de Horas Extras	Mayor
			Aprobación de Horas de Soporte	Mayor
			Carga de Documentos Evidencia	Mayor

Tabla 14 Identificación de activos de información

14.4.2. Resultados

Como se puede observar en la matriz de activos de información, contienen los 12 activos de vital importancia para la organización, los mismos que fueron identificados con la ayuda del personal encargado, para continuar con las fases del proyecto se trabajará con el activo base de datos de sap y el servidor, los que se detalla a continuación.

1	SAP-PRODU-06	BASE DE DATOS
2	SAP-PRODU-06	SERVIDOR SAP-PRODU-06

Para visualizar los activos de información, revisar el Anexo 1.

Herramienta de Evaluación (Pestaña Inventario de Activos).xlsx

14.5. FASE 4 ANÁLISIS DE AMENAZAS Y VULENERABILIDADES DE ACTIVOS DE INFORMACIÓN.

En esta fase se realizará un análisis de vulnerabilidades basándonos en los activos seleccionados en la clasificación de la información.

Antes de iniciar con el análisis de las amenazas y vulnerabilidades se va a realizar una breve definición de herramientas y conceptos que se usaran.

14.5.1. Amenazas

Son situaciones que desencadenan en un incidente en la organización, causando daño material o pérdidas inmateriales de los activos de información.

(ISOTools, 2016)

14.5.2. Vulnerabilidades

Es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer la seguridad. Las vulnerabilidades pueden ser de varios tipos, hardware, software, humanas y pueden ser explotadas o utilizadas por intrusos o atacantes. (Rayas, 2020)

14.5.3. Metodología MAGERIT

Es una metodología de carácter público que puede ser utilizada libremente y no requiere autorización previa. Interesa principalmente a las entidades en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) para satisfacer el principio de la gestión de la seguridad basada en riesgos, así como el requisito de análisis y gestión de riesgos, considerando la dependencia de las tecnologías

de la información para cumplir misiones, prestar servicios y alcanzar los objetivos de la organización.

Siguiendo la terminología de la normativa ISO 31000, Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

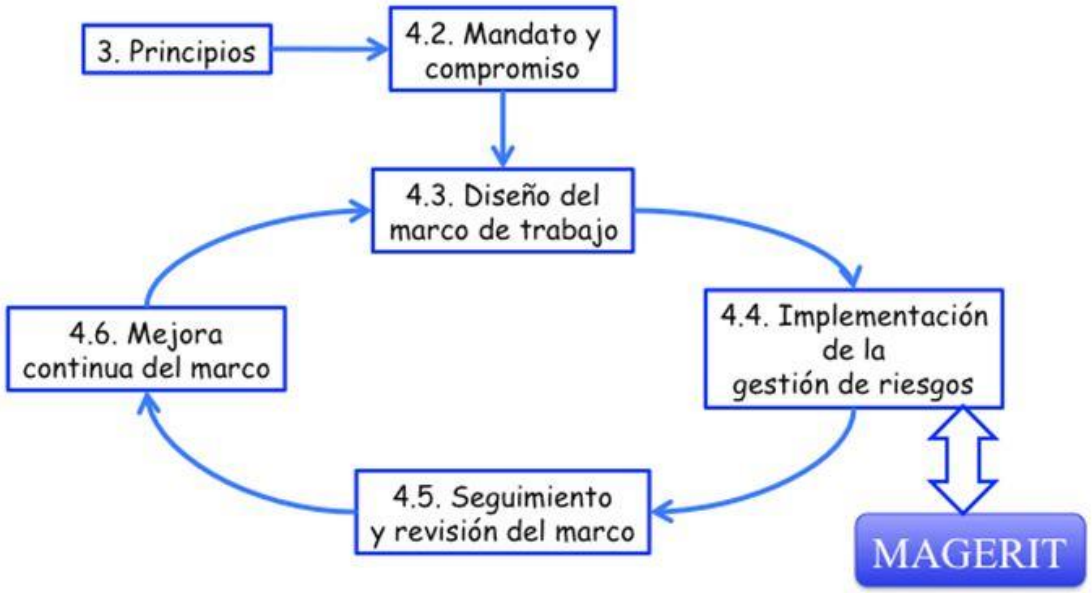


Figura 4 Metodología Magerit

(Portal de Administración Electrónica, 2012)

14.5.3.1. Catálogo de elementos Magerit

El catálogo marca pautas en cuanto a:

- Tipos de activos.
- Dimensiones de valoración de los activos.
- Criterios de valoración de los activos.
- Amenazas típicas sobre los sistemas de información.

- Salvaguardas a considerar para proteger sistemas de información.

(ISOTools, 2015)

14.5.4. Gestión de riesgos Seguridad de la Información

La gestión de riesgos de seguridad de la información es el proceso de identificar, comprender, evaluar, mitigar los riesgos y sus vulnerabilidades subyacentes y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus operaciones.

(Sullivan, 2016)

14.5.5. Riesgo

El riesgo consiste en las probabilidades de que una amenaza explote la vulnerabilidad de un activo de información y, por tanto, dañe a una organización.

Riesgo es el impacto y la probabilidad de que una amenaza (o de una serie de eventos, amenazas) puedan afectar de manera adversa la consecución de los objetivos. (Reyes, 2018)

Gestionar los riesgos es fundamental para gestionar la seguridad de la información de manera eficiente y responsable. (Isbel, 2021)

14.5.6. Mapa de Riesgos

Un mapa de riesgos (mapa de calor) es una herramienta de visualización de datos para comunicar los riesgos específicos que enfrenta una organización. Un mapa de riesgos ayuda a las organizaciones a identificar y priorizar los riesgos asociados con su negocio. Un mapa de calor de riesgo consiste en una matriz

con dos ejes, donde el eje Y representa la probabilidad de frecuencia del riesgo y el eje X representa el impacto que puede tener el mismo.

El mapa se representa gráficamente ubicando los riesgos en un cuadrante, dependiendo de la probabilidad de que determinado riesgo pueda ocurrir y el impacto cuantitativo o cualitativo que se produce en caso de que se materialice el riesgo. (Roy, 2018)

Figura 5 Mapa de Calor

Una adecuada estructuración del mapa de riesgos ayuda a mejorar el modelo de evaluación de riesgos de la organización. Para esto es necesario en primer lugar identificar detenidamente los riesgos inherentes a la organización y analizar qué eventos tanto externos como internos están ocasionando dichos riesgos.

Los riesgos identificados deben ser evaluados, estimando con qué frecuencia podrían aparecer y cuál es el impacto estimado a nivel financiero, reputacional y estratégico. (Londoño, 2022)

14.5.7. El riesgo inherente

Es aquel que puede existir de manera intrínseca en toda actividad, puede generarse por factores internos o externos y afectar la rentabilidad y el capital de las empresas. No puede ser eliminado, por lo cual su identificación debe contemplarse en los planes de gestión de las compañías. (Chubb, s.f.).

El Riesgo Inherente es el riesgo existente ante la ausencia de alguna acción que la dirección pueda tomar para alterar tanto la probabilidad o el impacto de este. (Macero, 2018)

Luego de haber definido los riesgos inherentes se deben identificar los controles mitigantes y de ahí resulta el riesgo residual. (Ibañies, 2009).

14.5.8. El riesgo residual

Se denomina riesgo residual al riesgo que persiste luego que se han hecho todos los esfuerzos para identificar y eliminar el riesgo.

RIESGO RESIDUAL = RIESGO INHERENTE – EFECTIVIDAD DE CONTROLES.

14.5.9. Metodología

Para el realizar el análisis de las amenazas y vulnerabilidades de los activos seleccionados se ha basado en la metodología Magerit, la misma que permite enfocar los esfuerzos en los riesgos que pueden resultar más críticos para la organización.

Para la matriz de impacto x probabilidad se ha establecido la escala de medición que se puede ver en la tabla 15 y nos ayudará para calificar y obtener el riesgo inherente.

	Grave Representa una posibilidad de pérdida alta que afecta gravemente a la continuidad del negocio que incluso puede llevar a la liquidación de la organización por lo que requiere de acciones inmediatas de los directivos.
	Importante. Representan una posibilidad de pérdida alta, puede afectar al funcionamiento normal de ciertos procesos, requiere de atención de la gerencia general .
	Bajo Evento de riesgo que representa una probabilidad que no afecta significativamente los procesos de la organización. Se administra con controles y procedimientos de rutina.
	Muy Bajo. Se vigilará, aunque no requiere medidas preventivas de partida.

Tabla 15 Escala de Evaluación

Agregando a la escala se establecerá variables contabilizadas del uno al cinco, tanto para el impacto como la probabilidad que se detalla a continuación en la siguiente descripción.

1 nada probable

2 poco probable

3 probable

4 muy probable

5 altamente Probable

Con los cuales se establecerá un promedio para colocar el valor del riesgo y obtener el riesgo inherente.

14.5.10. Activo 1

Nombre: SAP-PRODU-06

TIPO: Servidor Físico

HERRAMIENTA DE EVALUACIÓN RIESGOS ACTIVO							
NOMBRE DE ACTIVO	SAP-PRODU-06						
TIPO	SERVIDOR						
MARCA	HPE	MODELO	DL360 GEN10	SERIE	MXQ0020485	GARANTIA	EXPIRADAEXPIRADA (11-jul-2020)
FECHA	27-ago-22						
ELABORADO POR	FROILAN CONDO - JAVIER CAYO						

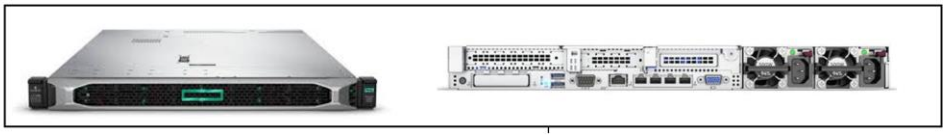


Figura 6 Figura Activo 1

En la tabla 14 se puede observar las amenazas levantadas para el activo de información y con esto identificar cuáles son las posibles vulnerabilidades que afectarían a las amenazas del activo de información.

AMENAZAS	Vulnerabilidades
Desastres naturales	El equipo no cuenta con un sistema de respaldo recurrente y una frecuencia establecida El persona no se encuentra capacitado ante un evento de desastre natural No cuenta con plan DRP
Avería de origen físico o lógico	No cuenta con tareas recurrentes de mantenimiento físico Los contratos de soporte de infraestructura se encuentran vencidos Falta Herramienta de monitorización y gestión de recursos no se cuenta con una aplicación que valide el estado de
Condiciones inadecuadas de temperatura o humedad	El espacio físico no cuenta con las condiciones requeridas para que el equipo mantenga una funcionalidad adecuada
Errores del administrador	Persona no cuenta con la experiencia necesaria para realizar actividades No se cuenta con un proceso de control de cambios (actualizaciones y mantenimiento)
Errores de mantenimiento / actualización de equipos	Persona no cuenta con la experiencia necesaria para realizar
Caída del sistema por agotamiento de recursos	Falta de Gestión de cambios (mejoras y sustituciones) Persona no cuenta con la experiencia necesaria para la distribución y dimensionamiento del hardware
Abuso de privilegios de acceso	No se encuentra bien definido el perfil de de usuarios La cultura de aprendizaje a los usuarios no es muy efectiva
Acceso no autorizado	No cuenta con auditoria de control de accesos No se encuentra bien definido el perfil de de usuarios La cultura de aprendizaje a los usuarios no es muy efectiva El equipo no cuenta con un sistema de respaldo recurrente y una frecuencia establecida
Manipulación de los equipos	No cuenta con auditoria de control de accesos No se encuentra bien definido el perfil de de usuarios
Manipulación de los equipos	No cuenta con auditoria de control de accesos No se encuentra bien definido el perfil de de usuarios

Tabla 16 Tabla Vulnerabilidades

A continuación, evaluamos mediante el impacto x probabilidad que puedan ocurrir las vulnerabilidades expuestas en la tabla 17 y definimos un valor de riesgo resultante.

AMENAZAS	Probabilidad	Impacto	Valor Riesgo
Desastres naturales	2	5	10
Avería de origen físico o lógico	1	9	9
Condiciones inadecuadas de temperatura o humedad	3	5	15
Errores del administrador	3	5	15
Errores de mantenimiento / actualización de equipos	3	5	15
Caída del sistema por agotamiento de recursos	2	5	10
Abuso de privilegios de acceso	3	5	15
Acceso no autorizado	2	2	4
Manipulación de los equipos	2	4	8
Manipulación de los equipos	2	4	8

Tabla 17 Valor de Riesgo activo 1

Una vez que se establece los parámetros de impacto x probabilidad nos dará como resultante el riesgo inherente como muestra la tabla 18.

AMENAZAS	Probabilidad	Impacto	Valor Riesgo	Riesgo innerente
Desastres naturales	2	5	10	Grave
Avería de origen físico o lógico	1	9	9	Importante
Condiciones inadecuadas de temperatura o humedad	3	5	15	Grave
Errores del administrador	3	5	15	Grave
Errores de mantenimiento / actualización de equipos	3	5	15	Grave
Caída del sistema por agotamiento de recursos	2	5	10	Grave
Abuso de privilegios de acceso	3	5	15	Grave
Acceso no autorizado	2	2	4	Bajo
Manipulación de los equipos	2	4	8	Bajo
Manipulación de los equipos	2	4	8	Bajo

Tabla 18 Riesgo Inherente

Una vez realizado la revisión del riesgo inherente la colocamos en un mapa de calor para establecer controles y obtener el riesgo residual.

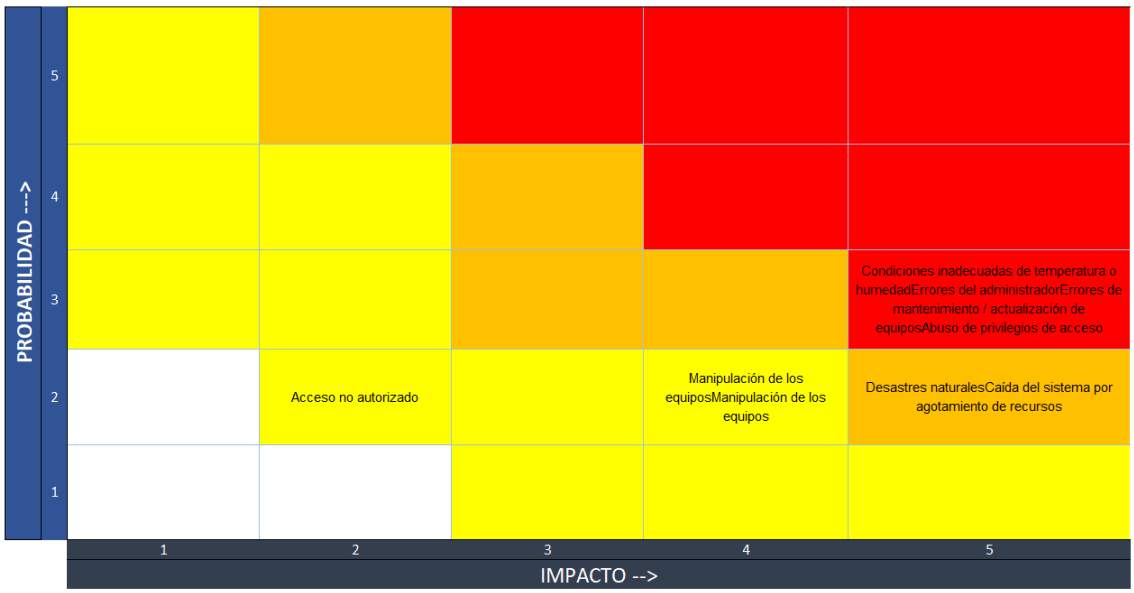


Figura 7 Matriz impacto x Probabilidad Activo 1

En la figura 7 se pudo visualizar que tenemos varios frentes que debemos considerar respectos a las amenazas con las vulnerabilidades:

- ✓ Importante probabilidad e importante impacto
- ✓ Desastres naturales
- ✓ Caída de sistema por agotamiento de recursos
- ✓ Grave probabilidad y grave impacto
- ✓ Condiciones inadecuadas de temperatura o humedad
- ✓ Errores de administrador
- ✓ Errores de mantenimiento

14.5.10.1. Riesgo residual

Antes de obtener el control residual realizaremos una revisión previa de los controles existentes realizando una calificación para esta actividad se estableció las siguientes tablas de valoración:

Tipo	Observación
Manual	No cuenta con un sistema automatizado
Automática	Se realiza el proceso enteramente automático

Tabla 19 Tipo de Control

Tipo	Observación
Reactivo	Cuando se suscita el evento y el control no lo pudo contener
Defectivo	Cuando se realiza búsqueda de los que paso
Preventivo	Es el q analiza posibles amenazas y se adelanta

Tabla 20 Clasificación de Control

14.5.10.2. Frecuencia del control

La frecuencia del control es cuando se revisa el control y se deber realizar correcciones de este, esto ayuda a mejorar la protección del activo.

14.5.10.3. Fortaleza del control

En la tabla 21 fue definida con revisión de la organización y con la revisión de estándares.

Tipo	Observación
Alto	Cuando el control es automático y preventivo
Medio	Cuando el control es automático y detectivo
Bajo o Débil	Cuando el control es manual y reactivo

Tabla 21 Fortaleza de Control

14.5.10.4. Clasificación control existente

En la tabla 22 nos muestra la calificación de controles existentes y el nivel de fortaleza cuenta el control.

		CALIFICACIÓN CONTROL EXISTENTE			
AMENAZA	CONTROL EXISTENTE	TIPO DE CONTROL	CLASIFICACIÓN DE CONTROL	FRECUENCIA DE CONTROL	FORTALEZA DE CONTROL
Desastres naturales	Recuperar el ambiente de los respaldos de la fecha disponible una vez habilitado y pasado el desastre	Manual	Reactivo	ANUAL	DEBIL
Avería de origen físico o lógico	Verificar componentes averiados de manera física	Manual	Reactivo	MENSUAL	DEBIL
Condiciones inadecuadas de temperatura o humedad	no cuenta con un control existente	-	-	-	-
Errores del administrador	no cuenta con un control existente	-	-	-	-
Errores de mantenimiento / actualización de equipos	Recuperar del ultimo backup / en caso de falla de hardware remplazar con un equipo tipo PC	Manual	Reactivo	MENSUAL	DEBIL
Caída del sistema por agotamiento de recursos	Revisión inicial de recursos desde sistema operativo una vez reportado falla de sistema	Manual	Reactivo	MENSUAL	DEBIL
Abuso de privilegios de acceso	Solo los usuarios con perfil de admin tienen acceso a la infromación	Manual	Detectivo	SEMANAL	DEBIL
Acceso no autorizado	Acceso restringido al centro de computo	Manual	Preventivo	DIARIO	MEDIO
Manipulación de los equipos	Acceso restringido al centro de computo	Manual	Preventivo	DIARIO	MEDIO

Tabla 22 Clasificación de Control existente

Luego de la revisión y medición de la fortaleza del control se establece controles que mejoren la disponibilidad, integridad y confidencialidad y se realiza una nueva medición como se observa en la tabla 23.

VULNERABILIDADES	El equipo no cuenta con un sistema de respaldo recurrente y una frecuencia establecida	El persona no se encuentra capacitado ante un evento de desastre natural	No cuenta con plan DRP	No cuenta con tareas recurrentes de mantenimiento físico	Los contratos de soporte de infraestructura se encuentran vencidos	Falta Herramienta de monitorización y gestión de recursos	No se cuenta con una aplicación que valide el estado de funcionamiento del hardware	No cuenta con una aquitectura en alta disponibilidad el equipo es standalone	El espacio físico no cuenta con las condiciones requeridas para que el equipo mantenga una funcionalidad adecuada	Persona no cuenta con la experiencia necesaria para realizar actividades	No se cuenta con un proceso de control de cambios (actualizaciones-mantenimiento)	No cuenta con auditoria de control de accesos	No se encuentra bien definido el perfil de de usuarios	La cultura de aprendizaje a los usuarios no es muy efectiva	El equipo no cuenta con un sistema de respaldo recurrente y una frecuencia establecida	CALIFICACIÓN CONTROLES PROPUESTOS				
																	TIPO DE CONTROL	CLASIFICACIÓN DE CONTROL	FRECUENCIA DE CONTROL	TALEZA DEL CONT	
			X														MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO	
X																	AUTOMATICO	PREVENTIVO	DIARIO	ALTO	MEDIO
	X																MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO	
				X	X												MANUAL	PREVENTIVO	ANUAL	MEDIO	
						X	X	X									MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO	
						X											AUTOMATICO	PREVENTIVO	DIARIO	ALTO	ALTO
							X										AUTOMATICO	PREVENTIVO	SEMESTRAL	ALTO	
							X										AUTOMATICO	PREVENTIVO	ANUAL	ALTO	
									X								AUTOMATICO	PREVENTIVO	DIARIO	ALTO	ALTO
											X						MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO	MEDIO
										X											
											X						AUTOMATICO	PREVENTIVO	MENSUAL	ALTO	MEDIO
										X							MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO	
													x				AUTOMATICO	PREVENTIVO	DIARIO	ALTO	ALTO
																x	AUTOMATICO	PREVENTIVO	DIARIO	ALTO	ALTO
												x	x				AUTOMATICO	PREVENTIVO	MENSUAL	ALTO	ALTO
													x				AUTOMATICO	PREVENTIVO	TRIMESTRAL	ALTO	ALTO
												x	x	x			AUTOMATICO	PREVENTIVO	MENSUAL	ALTO	ALTO
																	AUTOMATICO	PREVENTIVO	TRIMESTRAL	ALTO	ALTO
												x	x	x			AUTOMATICO	PREVENTIVO	MENSUAL	ALTO	ALTO
																x	AUTOMATICO	PREVENTIVO	TRIMESTRAL	ALTO	ALTO

Tabla 23 Controles recomendados

El mismo que nos permite ver los cambios con las calificaciones anteriores vistos en la tabla 24 y con lo cual se puede determinar un riesgo residual

	CALIFICACIÓN CONTROLES PROPUESTOS							
AMENAZA	TIPO DE CONTROL	CLASIFICACIÓN DE CONTROL	FRECUENCIA DE CONTROL	TALEZA DEL CONT		RIESGO INHERENTE	RIESGO RESIDUAL	RIESGO SIMULADO
Desastres naturales	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO	MEDIO	Grave	Bajo	Muy bajo
	AUTOMATICO	PREVENTIVO	DIARIO	ALTO				
	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO				
Avería de origen físico o lógico	MANUAL	PREVENTIVO	ANUAL	MEDIO	ALTO	Importante	Bajo	Muy bajo
	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO				
	AUTOMATICO	PREVENTIVO	DIARIO	ALTO				
	AUTOMATICO	PREVENTIVO	SEMESTRAL	ALTO				
	AUTOMATICO	PREVENTIVO	ANUAL	ALTO				
Condiciones inadecuadas de temperatura o humedad	AUTOMATICO	PREVENTIVO	DIARIO	ALTO	ALTO	Grave	Grave	Bajo
Errores del administrador	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO	MEDIO	Grave	Grave	Bajo
Errores de mantenimiento / actualización de equipos	AUTOMATICO	PREVENTIVO	MENSUAL	ALTO	MEDIO	Grave	Bajo	muy bajo
	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO				
Caída del sistema por agotamiento de recursos	AUTOMATICO	PREVENTIVO	DIARIO	ALTO	ALTO	Grave	Bajo	muy bajo
	AUTOMATICO	PREVENTIVO	DIARIO	ALTO	ALTO			
Abuso de privilegios de acceso	AUTOMATICO	PREVENTIVO	MENSUAL	ALTO	ALTO	Grave	Importante	Bajo
	AUTOMATICO	PREVENTIVO	TRIMESTRAL	ALTO	ALTO			
Acceso no autorizado	AUTOMATICO	PREVENTIVO	MENSUAL	ALTO	ALTO	Bajo	muy bajo	Muy Bajo
	AUTOMATICO	PREVENTIVO	TRIMESTRAL	ALTO	ALTO			
Manipulación de los equipos	AUTOMATICO	PREVENTIVO	MENSUAL	ALTO	ALTO	Bajo	Bajo	muy bajo
	AUTOMATICO	PREVENTIVO	TRIMESTRAL	ALTO	ALTO			

Tabla 24 Riesgo Residual

14.5.10.5. Riesgo Simulado

A continuación, se expondrá el riesgo simulado que es una medición en la matriz de impacto que nos permitirá ver el comportamiento con los controles planteados para mitigar las vulnerabilidades encontradas en el activo de información.

14.5.10.6. Matriz Impacto x Probabilidad Simulada

A continuación, la valoración tanto del riesgo (probabilidad x impacto) y el riesgo inherente con los controles planteados tomando las mismas escalas de evaluación.

AMENAZAS	Probabilidad	Impacto	Valor Riesgo	Riesgo innerente
Desastres naturales	1	2	2	muy bajo
Avería de origen físico o lógico	1	2	2	muy bajo
Condiciones inadecuadas de temperatura o humeda	1	3	3	Bajo
Errores del administrador	1	3	3	Bajo
Errores de mantenimiento / actualización de equipos	1	2	2	muy bajo
Caída del sistema por agotamiento de recursos	1	2	2	muy bajo
Abuso de privilegios de acceso	1	3	3	Bajo
Acceso no autorizado	1	3	3	Bajo
Manipulación de los equipos	1	2	2	muy bajo

Tabla 25Tabla de probabilidad por impacto simulado

14.5.10.7. Mapa de Calor Simulado

Como se puede observar en la figura 8, aplicando los controles podemos concluir que satisfacen las necesidades actuales y se reduce el riesgo bajando a las zonas de bajo impacto y probabilidad.

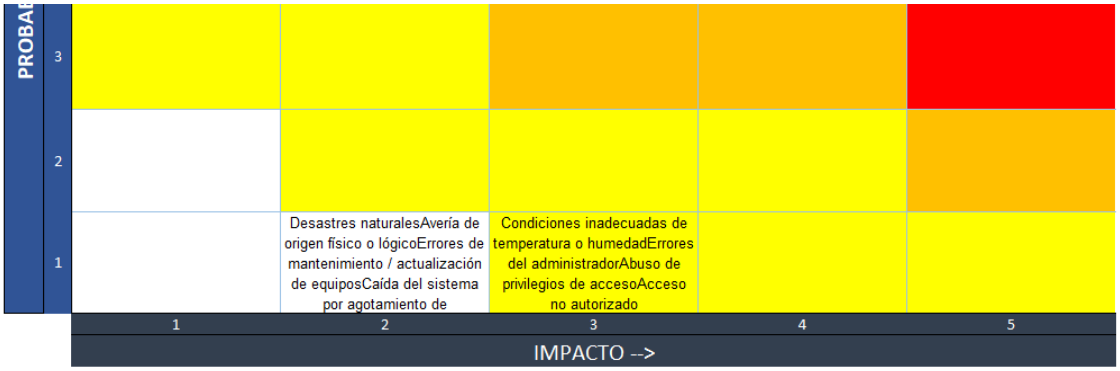


Figura 8 Matriz Impacto x probabilidad Simulado

14.5.10.8. Riesgo Simulado

Tomando en cuenta las tablas de evaluación podemos observar que en concordancia con el mapa de calor los controles planteados reducirían los riesgos de seguridad de información.

AMENAZA	RIESGO INHERENTE	RIESGO RESIDUAL	RIESGO SIMULADO
Desastres naturales	Grave	Bajo	Muy bajo
Avería de origen físico o lógico	Importante	Bajo	Muy bajo
Condiciones inadecuadas de temperatura o humedad	Grave	Grave	Bajo
Errores del administrador	Grave	Grave	Bajo
Errores de mantenimiento / actualización de equipos	Grave	Bajo	muy bajo
Caída del sistema por agotamiento de recursos	Grave	Bajo	muy bajo
Abuso de privilegios de acceso	Grave	Importante	Bajo
Acceso no autorizado	Bajo	muy bajo	Muy Bajo
Manipulación de los equipos	Bajo	Bajo	muy bajo

Tabla 26 Riesgo Simulado

Para visualizar con más detalle hacer referencia el documento Activo crítico servidor.xlsx del anexo 2.

14.5.11. Activo 2 Base de datos

Nombre: SAP-PRODU-06

TIPO: Base de Datos

	HERRAMIENTA DE EVALUACIÓN RIESGOS ACTIVO
NOMBRE DE ACTIVO	SAP-PRODU-06
TIPO	BASE D E DATOS
FECHA	27-ago-22
ELABORADO POR	FROILAN CONDO - JAVIER CAYO

En la tabla 27 se puede observar las amenazas que se identificaron para el activo de información, con esto se puede identificar cuáles son las posibles vulnerabilidades que afectarían a las amenazas del activo de información.

AMENAZAS	Vulnerabilidades
Errores de usuarios	Personal no cuenta con capacitación Falta de formación y conciencia sobre seguridad Falta de documentación
Errores del administrador	Falta de políticas para administración de plataforma Personal no cuenta con la suficiente capacitación para administrar la plataforma Falta de documentación Falta de política adecuada de respaldo de información Inadecuada segregación de funciones
Errores de monitorización	Falta de registros de auditoria Falta de documentación
Difusión de software dañino	Falta de políticas para el uso de la criptografía Falta de política adecuada de respaldo de información
Fugas de información	Alteración de información sin supervisión Falta de registros de auditoria
Destrucción de información	Falta de política adecuada de respaldo de información Falta de registros de auditoria
Errores de mantenimiento / actualización de programas	Mantenimiento inadecuado Falta de política de control de cambios Falta de docuementación Falta de política adecuada de respaldo de información
Suplantación de la identidad del usuario	Ausencia de sistemas de identificación y autenticación Falta de formación y conciencia sobre seguridad Contraseñas predeterminadas no modificadas
Abuso de privilegios de acceso	Ausencia de sistemas de identificación y autenticación Falta de formación y conciencia sobre seguridad
Acceso no autorizado	Falta de política de acceso No cuenta con roles definidos para los usuarios Falta de registros de auditoria
Modificación deliberada de la información	Falta de política adecuada de respaldo de información Falta de registros de auditoria Falta de formación y conciencia sobre seguridad No existe una correcta manipulación de información
Divulgación de información	Falta de formación y conciencia sobre seguridad No cuenta con un acuerdo de confidencialidad No existe una correcta manipulación de información

Tabla 27 Tabla de Vulnerabilidades base de datos

A continuación, en la tabla 28 evaluamos mediante el impacto x probabilidad que puedan ocurrir las vulnerabilidades expuestas en la tabla x y definimos un valor de riesgo resultante.

AMENAZAS	Vulnerabilidades	Probabilidad	Impacto	Valor Riesgo
Errores de usuarios	Personal no cuenta con capacitación Falta de formación y conciencia sobre seguridad	1	5	5
Errores del administrador	administración de plataforma Personal no cuenta con la suficiente capacitación para administrar la plataforma Falta de documentación Falta de política adecuada de	2	5	10
Errores de monitorización	Falta de registros de auditoria Falta de documentación	1	3	3
Difusión de software dañino	Falta de políticas para el uso de la criptografía	1	5	5
Fugas de información	Alteración de información sin supervisión	3	5	15
Destrucción de información	Falta de política adecuada de respaldo de información	2	5	10
Errores de mantenimiento / actualización de programas	Mantenimiento inadecuado Falta de política de control de cambios Falta de docuementación Falta de política adecuada de respaldo	2	5	10
Suplantación de la identidad del usuario	Ausencia de sistemas de identificación y autenticación Falta de formación y conciencia sobre	1	5	5
Abuso de privilegios de acceso	Ausencia de sistemas de identificación y autenticación	2	5	10
Acceso no autorizado	Falta de política de acceso No cuenta con roles definidos para los usuarios	2	5	10
Modificación deliberada de la información	respaldo de información Falta de registros de auditoria Falta de formación y conciencia sobre seguridad	1	5	5
Divulgación de información	sobre seguridad No cuenta con un acuerdo de confidencialidad	3	5	15

Tabla 28 Valor de Riesgo Activo 2

Una vez que se establece los parámetros de impacto x probabilidad nos dará como resultante el riesgo inherente como se muestra en la tabla 29.

AMENAZAS	Vulnerabilidades	Probabilidad	Impacto	Valor Riesgo	Riesgo innerente
Errores de usuarios	Personal no cuenta con capacitación Falta de formación y conciencia sobre seguridad	1	5	5	Bajo
Errores del administrador	administración de plataforma Personal no cuenta con la suficiente capacitación para administrar la plataforma Falta de documentación Falta de política adecuada de	2	5	10	Importante
Errores de monitorización	Falta de registros de auditoria Falta de documentación	1	3	3	Bajo
Difusión de software dañino	Falta de políticas para el uso de la criptografía	1	5	5	Bajo
Fugas de información	Alteración de información sin supervisión	3	5	15	Grave
Destrucción de información	Falta de política adecuada de respaldo de información	2	5	10	Importante
Errores de mantenimiento / actualización de programas	Mantenimiento inadecuado Falta de política de control de cambios Falta de docuementación Falta de política adecuada de respaldo	2	5	10	Importante
Suplantación de la identidad del usuario	Ausencia de sistemas de identificación y autenticación Falta de formación y conciencia sobre	1	5	5	Bajo
Abuso de privilegios de acceso	Ausencia de sistemas de identificación y autenticación	2	5	10	Importante
Acceso no autorizado	Falta de política de acceso No cuenta con roles definidos para los usuarios	2	5	10	Importante
Modificación deliberada de la información	respaldo de información Falta de registros de auditoria Falta de formación y conciencia sobre seguridad	1	5	5	Bajo
Divulgación de información	sobre seguridad No cuenta con un acuerdo de confidencialidad	3	5	15	Grave

Tabla 29 Riesgo Inherente

Una vez realizado la revisión del riesgo inherente la colocamos en un mapa de calor para establecer controles y obtener el riesgo residual.

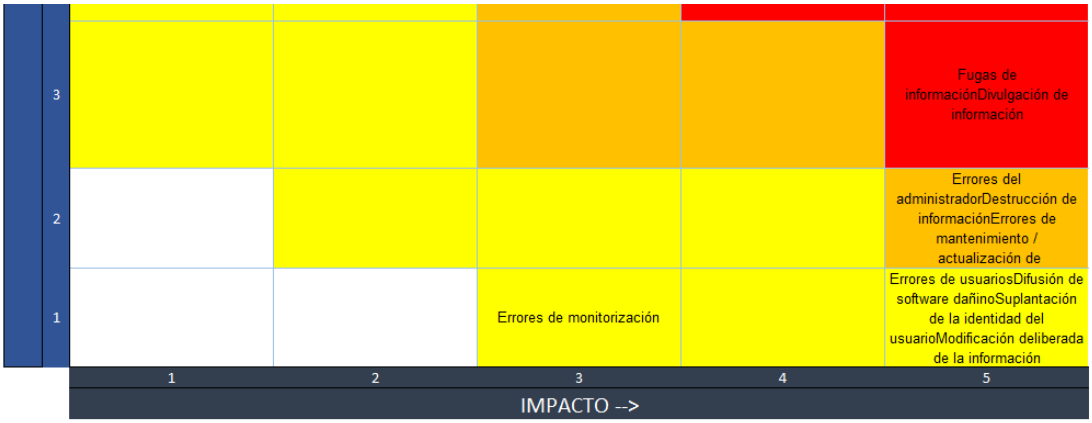


Figura 9 Mapa de Calor activo 2

En la figura anterior nos permite visualizar que tenemos varios frentes que se deben considerar con relación a las amenazas y vulnerabilidades:

- ✓ Importante probabilidad e importante impacto
- ✓ Fugas de información
- ✓ Divulgación de Información
- ✓ Errores de administrador
- ✓ Errores de mantenimiento/ Actualización de programas
- ✓ Abuso de privilegios de acceso
- ✓ Errores de difusión de software dañino
- ✓ Suplantación de identidad
- ✓ Modificación deliberada de la información

14.5.11.1. Riesgo residual

Antes de tener el control residual re realizará una revisión previa de los controles existentes, para esta actividad se estableció las siguientes tablas de valoración:

Tipo	Observación
Manual	No cuenta con un sistema automatizado
Automática	Se realiza el proceso enteramente automático

Tabla 30 Tipo de Control activo 2

Tipo	Observación
Reactivo	Cuando se suscita el evento y el control no lo pudo contener
Defectivo	Cuando se realiza búsqueda de los que paso
Preventivo	Es el q analiza posibles amenazas y se adelanta

Tabla 31 Clasificación de Control

14.5.11.2. Frecuencia del control

Es cuando se revisa el control y se debe realizar correcciones, puede ser definida como diario, semanal, mensual, semestral, anual.

14.5.11.3. Fortaleza del control

La tabla 32 fue definida con revisión de la organización y en base a la revisión de los estándares.

Tipo	Observación
Alto	Cuando el control es automático y preventivo
Medio	Cuando el control es automático y detectivo
Bajo o Débil	Cuando el control es manual y reactivo

Tabla 32 escala de Evaluación

14.5.11.4. Calificación control existente

En la siguiente tabla nos muestra la calificación de controles existentes y el nivel de fortaleza que cuenta el control.

AMENAZA	CONTROL EXISTENTE	TIPO DE CONTROL	CLASIFICACIÓN DE CONTROL	FRECUENCIA DE CONTROL	FORTALEZA DE CONTROL
Errores de usuarios	No cuenta con un control existente	-	-	-	
Errores del administrador	Capacita a personal en manejo de la base de datos	Manual	Reactivo	Semestral	DEBIL
Errores de monitorización	No cuenta con un control existente	-	-	-	
Difusión de software dañino	No cuenta con un control existente	-	-	-	
Fugas de información	No cuenta con un control existente	-	-	-	
Destrucción de información	Recuperar del ultimo backup disponible	Manual	Reactivo	MENSUAL	DEBIL
Errores de mantenimiento / actualización de programas	Procedimiento para control de cambios	Manual	Reactivo	MENSUAL	DEBIL
Suplantación de la identidad del usuario	No cuenta con un control existente	-	-	-	
Abuso de privilegios de acceso	Política de control de acceso	Manual	Preventivo	MENSUAL	MEDIO
Modificación deliberada de la información	Recuperar del ultimo backup disponible	Manual	Preventivo	DIARIO	MEDIO
Divulgación de información	No cuenta con un control existente	-	-	-	

Tabla 33 Clasificación control existente

Luego de la revisión y medición de la fortaleza del control se establece controles que mejoren la disponibilidad, integridad y confidencialidad, se realiza una nueva medición, como se puede observar en la tabla 34.

	Alteración de Falta de regis	Falta de políti de informació Falta de regis	Mantenimien Falta de políti Falta de docu Falta de políti de informació	Ausencia de s autenticación Falta de form seguridad Contraseñas r modificadas	Ausencia de s autenticación Falta de form seguridad	Falta de políti No cuenta cor usuarios Falta de regis	Falta de políti de informació Falta de regis Falta de form seguridad No existe una información	CALIFICACIÓN CONTROLES PROPUESTOS			
AMENAZA								TIPO DE CONTROL	CLASIFICACIÓN DE CONTROL	FRECUENCIA DE CONTROL	FORTALEZA DEL CONTROL
Errores de usuarios								MANUAL	PREVENTIVO	SEMESTRAL	MEDIO
								MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO
Errores del administrador								AUTOMATICO	PREVENTIVO	TRIMESTRAL	ALTO
								MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO
											ALTO
								MANUAL	PREVENTIVO	SEMESTRAL	MEDIO
Errores de monitorización								AUTOMATICO	PREVENTIVO	DIARIO	ALTO
Difusión de software dañino							X	MANUAL	PREVENTIVO	DIARIO	MEDIO
Fugas de información								MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO
Destrucción de información	X						X	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO
Errores de mantenimiento / actualización de programas	X						X	AUTOMÁTICO	PREVENTIVO	SEMESTRAL	ALTO
Suplantación de la identidad del usuario			X				X	AUTOMÁTICO	PREVENTIVO	SEMESTRAL	ALTO
Abuso de privilegios de acceso				X			X	AUTOMÁTICO	PREVENTIVO	MENSUAL	ALTO
Modificación deliberada de la información								AUTOMÁTICO	PREVENTIVO	MENSUAL	ALTO
Divulgación de información	X						X	MANUAL	PREVENTIVO	MENSUAL	MEDIO

Tabla 34 Calificación control existente

El mismo que nos permite ver los cambios con las calificaciones anteriores vistos en la tabla x y, con lo cual se puede obtener un riesgo residual.

	CALIFICACIÓN CONTROLES PROPUESTOS						
AMENAZA	TIPO DE CONT	CLASIFICACIÓN DE CC	FRECUENCIA DE COI	FORTALEZA DEL CONTRO		RIESGO INHERENTE	RIESGO RESIDUAL
Errores de usuarios	MANUAL	PREVENTIVO	SEMESTRAL	MEDIO	MEDIO	Bajo	Bajo
	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO			
Errores del administrador	AUTOMATICO	PREVENTIVO	TRIMESTRAL	ALTO	MEDIO	Importante	Bajo
	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO			
				ALTO			
	MANUAL	PREVENTIVO	SEMESTRAL	MEDIO			
Errores de monitorización	AUTOMATICO	PREVENTIVO	DIARIO	ALTO	ALTO	Bajo	Muy Bajo
Difusión de software dañino	MANUAL	PREVENTIVO	DIARIO	MEDIO	MEDIO	Bajo	Bajo
Fugas de información	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO	MEDIO	Grave	Importante
Destrucción de información	MANUAL	PREVENTIVO	TRIMESTRAL	MEDIO	MEDIO	Importante	Bajo
Errores de mantenimiento / actualización de programas	AUTOMÁTICO	PREVENTIVO	SEMESTRAL	ALTO	ALTO	Importante	Bajo
Suplantación de la identidad del usuario	AUTOMÁTICO	PREVENTIVO	SEMESTRAL	ALTO	ALTO	Bajo	Muy Bajo
Abuso de privilegios de acceso	AUTOMÁTICO	PREVENTIVO	MENSUAL	ALTO	ALTO	Importante	Bajo
Modificación deliberada de la información	AUTOMÁTICO	PREVENTIVO	MENSUAL	ALTO	ALTO	Importante	Bajo
Divulgación de información	MANUAL	PREVENTIVO	MENSUAL	MEDIO	MEDIO	Bajo	Muy Bajo

Tabla 35 Riesgo Residual

14.5.11.5. Riesgo Simulado

Como un valor agregado al proyecto se ha planteado realizar un riesgo simulado, que sería una medición en la matriz de impacto que nos permitirá ver el comportamiento con los controles planteados para mitigar las vulnerabilidades encontradas en el activo de información.

A continuación, en la tabla 36 se puede observar la valoración tanto del riesgo (probabilidad x impacto) y el riesgo inherente con los controles planteados tomando las mismas escalas de evaluación.

AMENAZAS	Controles	Probabilidad	Impacto	Valor Riesgo	Riesgo inherente
Errores de usuarios	Registre el acceso a datos confidenciales, incluida la modificación y eliminación. Establecer políticas de capacitación continua a los usuarios.	1	2	2	muy bajo
Errores del administrador	Registre el acceso a datos confidenciales, incluida la modificación y eliminación. Restringuir los privilegios de administrador a las cuentas de administrador dedicadas en los activos de la empresa. Relaizar un inventario de usuarios, debe incluir cuentas de usuario y de administrador, importante registrar el nombre de la persona encargada	1	2	2	muy bajo
Errores de monitorización	Realizar revisiones de registros de auditoría para detectar anomalías o eventos anormales que podrían indicar una amenaza potencial. Recopilar registros de auditoría, consultas de DNS , cuando corresponda y sea compatible.	1	2	2	muy bajo
Difusión de software dañino	Utilizar software antimalware basado en el comportamiento. Configurar actualizaciones automáticas para archivos de firmas antimalware. Establecer y mantener un proceso de recuperación de datos.	1	4	4	Bajo
Fugas de información	Implementar un firewall a la base de datos. Establecer y mantener un proceso de configuración, eliminar parámetros por defecto	1	2	2	muy bajo
Destrucción de información	Registrar el acceso a datos confidenciales, incluida la modificación y eliminación. Implementar políticas de respaldo de información	1	2	2	muy bajo
Errores de mantenimiento / actualización de programas	Implementar procedimientos para el control de cambios. Establecer y mantener un proceso de recuperación de datos.	1	2	2	muy bajo
Suplantación de la identidad del usuario	caracteres. Implemetar multiple factor de autenticación. Centralizar la gestión de cuentas a través de un directorio o servicio de identidad.	1	3	3	Bajo
Abuso de privilegios de acceso	Registre el acceso a datos confidenciales, incluida la modificación y eliminación. Centralizar la gestión de cuentas a través de un directorio o servicio de identidad.	1	2	2	muy bajo
Acceso no autorizado	Registre el acceso a datos confidenciales, incluida la modificación y eliminación. Eliminar o deshabilitar cualquier cuenta inactiva después de un período de inactividad, o por salida de usuario. Validar que todas las cuentas activas estén autorizadas	1	2	2	muy bajo
Modificación deliberada de la información	Registre el acceso a datos confidenciales, incluida la modificación y eliminación. Establecer y mantener un proceso de recuperación de datos.	1	1	1	muy bajo
Divulgación de información	Registre el acceso a datos confidenciales, incluida la modificación y eliminación. Implementar acuerdos de confidencialidad para usaurios y proveedores de servicios. Establecer y mantener un proceso de recuperación de datos.	1	1	1	muy bajo

Tabla 36 Riesgo Inherente

14.5.11.6. Mapa de Calor Simulado

Como se puede observar en la tabla 37, al aplicar los controles podemos concluir que satisfacen las necesidades actuales y se reduce el riesgo bajando a las zonas de bajo impacto y probabilidad.

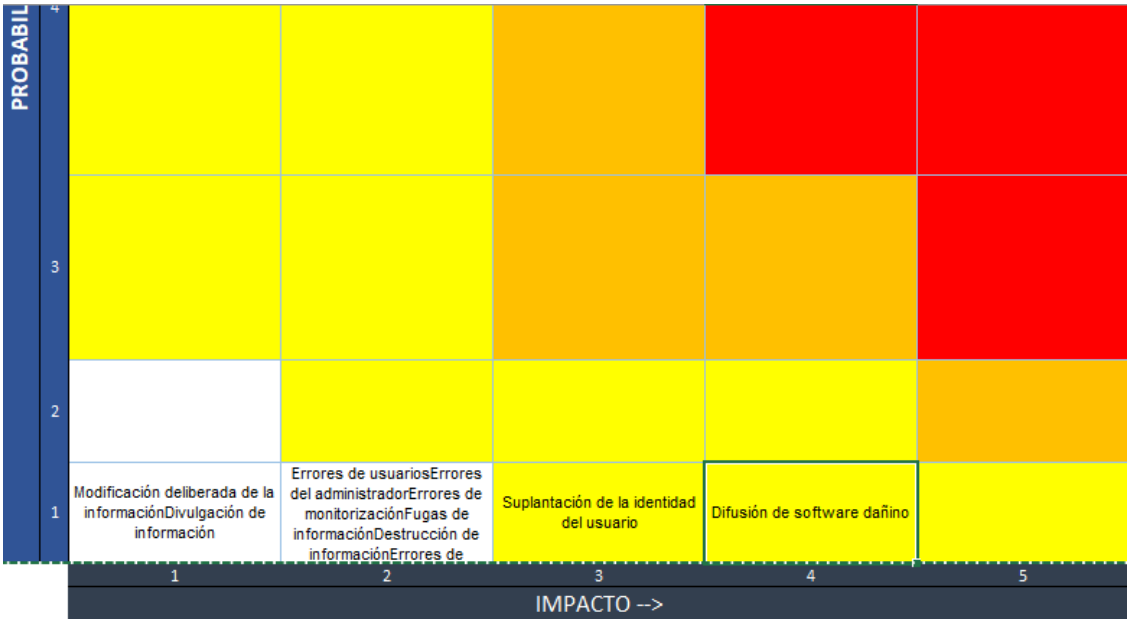


Tabla 37 Mapa de calor simulado

14.5.11.7.Riesgo Simulado

Tomando en cuenta las tablas de evaluación podemos observar que en concordancia con el mapa de calor los controles planteados ayudarán a reducir los riesgos de seguridad de la información.

RIESGO INHERENTE	RIESGO SIMULADO
Bajo	muy bajo
Importante	muy bajo
Bajo	muy bajo
Bajo	Bajo
Grave	muy bajo
Importante	muy bajo
Importante	muy bajo
Bajo	Bajo
Importante	muy bajo
Importante	muy bajo
Bajo	muy bajo

Tabla 38 Riesgo Simulado luego de aplicación de controles

Para visualizar con más detalle hacer referencia el documento Activo crítico servidor.xlsx del anexo 3.

14.5.11.8. Resultados

Una vez realizado el levantamiento de riesgos vulnerabilidades de ambos activos de información se concluye.

El riesgo inherente sin controles tiene alto nivel de riesgo en ser vulnerado y dado que el nivel de información que cuenta el activo de información son críticos para la organización y representan niveles de perdida importantes, e incluso con el riesgo inherente con los controles actuales no satisface la integridad, disponibilidad y confidencialidad de la información se ha colocado una propuesta para la organización y se ha agregado el ejercicio de como cambiaria el nivel de protección reduciendo de ambos activos de impacto grave, importante y bajo a bajos y muy bajos que sería una propuesta importante con el establecimiento de políticas y el SGSI para solventarlos.

14.6. FASE 5 ANÁLISIS DE AMENAZAS Y VULENERABILIDADES DE ACTIVOS DE INFORMACIÓN.

14.7. Roadmap planes de acción

14.7.1. Metodología

En esta sección se elaborará una esquematización de planes de acción el mismo que es un paso importante que permite mantener una planificación de la implementación de un SGSI, del cual será alimentado por controles obtenidos en la fase de evaluación del estado actual del sistema de gestión de seguridad y a lo largo del desarrollo del capstone y análisis de vulnerabilidades.

La elaboración de planes de acción está compuesta por códigos de aplicación, actividades o acciones a implementar, responsable, coste de ejecución, tiempo dividido en los 4 trimestres del año, los mismos que serán priorizados por la organización para la ejecución.

En la tabla 39 se puede observar una muestra de los los planes de acción propuestos.

ID	PLAN DE ACCIÓN	RESPONSABLE
PA01	Fortalecer el control de Gestión de Activos	Gerencia de Sistemas
PA02	Establecer políticas y procedimientos de intercambio de información, acuerdos de intercambio	Gerencia de Sistemas
PA03	Fortalecer los controles actuales con respecto a la seguridad fisica del entorno para prevenir el acceso físico no autorizado, los daños e interferencia a la información	Gerencia de Sistemas
PA04	Fortalecer control de manipulación de información	Gerencia de Sistemas
PA05	Asigne roles claves y responsabilidades responder a incidentes, incluido el personal de legal, TI, seguridad de la información, instalaciones, relaciones públicas, recursos humanos, personal de respuesta a incidentes y analistas, según corresponda. Revise esta salvaguarda anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.	Gerencia de Sistemas
PA06	Fortalecer el proceso para evaluar a los proveedores de servicios que poseen datos confidenciales o que son responsables de las plataformas o procesos de TI críticos de una empresa, para garantizar que estos proveedores protejan esas plataformas y datos de manera adecuada.	Gerencia de Sistemas
PA07	Establecer control de desastres naturales y recuperación	Gerencia de Sistemas
PA08	Establecer aspectos de seguridad de informacion en la continuidad de negocio	Gerencia de Sistemas

Tabla 39 Planes de acción

14.7.2. Resultados

Se ha levantado dentro del todo proceso 210 planes de acción, los mismos que se han dividido para su ejecución en 2 años, se realizarán trabajos trimestrales por temas de presupuesto y limitado personal, para lo cual aún se debe desarrollar los proyectos específicos de cada plan de acción hacer una estimación económica y personal que va a estar a cargo.

El plan de acción ayudara a la organización a mantenerse alineados a largo plazo del programa de SGSI.

Para visualizar con más detalle hacer referencia el documento Planes de Acción SGSI.xlsx del anexo 4.

14.8. Políticas de alto nivel

14.8.1.Metodología

Implementar un SGSI se debe complementar con las políticas de seguridad, las mismas se desarrollan con el fin de proteger la información y los diferentes sistemas de la organización, de esta forma garantizar la integridad, confidencialidad y disponibilidad de la información.

Las políticas de seguridad de la información deben ser socializadas a todo el personal de la organización.

Las políticas que se han planteado para el proyecto tienen la siguiente estructura:

- Descripción de la política
- Roles, responsabilidad
- Periodicidad

A continuación, se detalla las políticas planteadas para el proyecto.

1. Política de Gestión de Seguridad de la información

La política de Seguridad de la información define los lineamientos que deben cumplir el personal y terceros de la organización de ventas consultivas, con el fin de establecer los niveles requeridos de confidencialidad, integridad y disponibilidad.
El área correspondiente de seguridad de información de la organización debe aprobar, comunicar, publicar y mantener el presente documento de políticas de la seguridad de la información.

La política del sistema de seguridad de la información deberá ser presentada de forma efectiva a todo personal de la organización e incluido a terceros mediante contratos y acuerdos que formalicen la aceptación de este.

Roles y Responsabilidades

- Dirección
- Recursos Humanos
- Empleados
- Contratistas

Periodicidad

- Trimestral

2. Revisión de Política de Sistema de Gestión de seguridad de información

Las políticas de seguridad deben ser revisadas y actualizadas para asegurar la aplicabilidad y eficacia.
Esta actualización en caso de cambios regulatorios por industria o legislación.

Roles y Responsabilidades

- Dirección
- Recursos Humanos
- Empleados
- Contratistas

Periodicidad

- Trimestral

3. Política Recursos Humanos de Contratación de Personal

El objetivo de esta política es asegurar tanto de parte de los empleados y contratistas entiendan sus responsabilidades y si cumplen su perfil para las funciones para las que se consideran.

Revisar los antecedentes de los candidatos al puesto que aplican de acuerdo con las leyes, normativas vigentes.

Establecer términos y condiciones en el contrato de trabajo respecto a la seguridad de información con el empleado y la organización.

Roles y Responsabilidades

- Recursos Humanos

Periodicidad

- Anual

4. Política Recursos Humanos Durante el Empleo

El objetivo de esta política es precautelar que tanto empleados y contratistas conozcan y cumplan con sus responsabilidades en el aspecto de seguridad de la información.

Se debe exigir a empleados y contratistas, que sigan las normas de seguridad de información aplicables a su puesto de trabajo de acuerdo con las políticas y procedimientos de la organización.

Se deberá establecer a nivel de organización una adecuada educación, concienciación y capacitación con actualizaciones trimestrales sobre políticas de seguridad según el puesto de trabajo.

Establecer dentro de la política procesos disciplinarios en el caso de incumplimiento de las políticas o en el caso de haber ocasionado brechas de seguridad.

Roles y Responsabilidades

- Dirección
- Recursos Humanos
- Empleados
- Contratistas

Periodicidad

- Trimestral

5. Política Recursos Humanos Remoción el Empleo

Proteger a la organización como parte del proceso de cambio finalización de relaciones del empleado o contratista.

Con la política se debe informar las responsabilidades en seguridad de información y obligaciones vigentes luego de la finalización o cambio del empleado y las que se deben cumplir.

Roles y Responsabilidades

- Recursos Humanos
- Empleados o Contratistas

Periodicidad

- Trimestral

6. Política de Gestión de Activos Responsabilidad

Se debe tener una identificación de activos dentro de la organización los cuales deben ser inventariados, documentados, colocar reglas de uso para el tratamiento de la información.

Dentro de la política se establecerá un proceso de devolución de activos al finalizar el contrato.

Roles y Responsabilidades

- Recursos Humanos
- Empleados o Contratistas

Periodicidad

- Trimestral

7. Política de Gestión de Clasificación de la información

Garantizar que la información reciba un nivel adecuado de protección de acuerdo con el nivel de importancia asignada para la organización frente a requisitos legales, sensibilidad y criticidad ante revelación o modificación no autorizadas mediante procedimientos para la manipulación de la información.

Roles y Responsabilidades

- Recursos Humanos
- Empleados o Contratistas

Periodicidad

- Trimestral

8. Política de Uso Aceptable de los Activos

Esta política se aplica a todos los activos de información administrados en la Organización, cualquiera sea su forma (físico y/o lógico) en que se encuentre, a fin de cumplir lo siguiente:

a) Garantizar que los activos de información reciban un apropiado nivel de protección

b) Clasificar la información para señalar su sensibilidad y criticidad

c) Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación, el encargado es el responsable de asegurar que, para la utilización de los activos contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Roles y Responsabilidades

- Dirección
- Recursos Humanos
- Empleados
- Contratistas

Periodicidad

- Trimestral

9. Política de autenticación

El área de Sistemas de la organización será responsable del acceso a los sistemas de información internos y externos, equipos electrónicos, unidades y servicios de red, basados en un modelo de acceso por roles, mediante la identificación y que se puede clasificar de la siguiente manera:

- Algo que el usuario conoce (por ejemplo: una clave de identificación)
- Algo que el usuario posee (por ejemplo: una tarjeta)
- Algo que el usuario es (por ejemplo: características biométricas

Roles y Responsabilidades

- Dirección
- Recursos Humanos
- Empleados
- Contratistas

Periodicidad

- Trimestral

10. Política de backup

La organización establece que todos los días se deben ejecutar obligatoriamente una copia de respaldo total de las bases de datos en producción y máquinas virtuales. Las copias diarias deben de mantenerse en un lugar alejado del centro de cómputo, mensualmente se debe mantener una copia de respaldo offsite, asimismo de las fuentes de los sistemas cada vez que exista una modificación y actualización.

Roles y Responsabilidades

- Dirección
- Recursos Humanos
- Empleados
- Contratistas

Periodicidad

- Trimestral

14.8.2. Resultados

Al aplicar las políticas de seguridad, ayudará a mejorar la protección de los activos, como fundamental la información, en especial la que es considerada sensible para la organización.

15. CONCLUSIONES Y RECOMENDACIONES

15.1. Conclusiones

- La organización de ventas consultivas actualmente no cuenta con procedimientos o un área asignada para la salvaguarda de la información.
- Los procesos que se llevan a cabo son realizados de manera empírica sin contar con una base de políticas establecidas, solamente se aplican normas generales para la gestión de la información las cuales son insuficientes para el aseguramiento de la información
- Al no contar con un sistema de gestión de seguridad de la información que salvaguarde y actúe de manera preventiva durante un ataque, la organización reacciona de manera reactiva y correctiva causando desperdicio de recursos.
- Se evidenció que no contaban con manejo adecuado de los activos de información, por lo cual se encuentran expuestos en gran medida ante amenazas y vulnerabilidades.
- En cuanto a la protección física existen procedimientos que están enfocados en ciertos ámbitos como ubicación y protección de equipos, pero no se toman en cuenta mantenimientos, áreas de seguridad, acceso a lugares restringidos, lo cual expone la integridad de los equipos, la información y el personal.
- En la parte de gestión de accesos se pudo evidenciar que no se cuenta con un procedimiento acorde por el área de sistemas, no existe controles de cambio de clave, límite de caracteres de clave, no se realiza una validación de que el acceso sea lo suficientemente fuerte y confiable.
- La implementación de un SGSI ayudará a la organización a proteger los activos de información, esto se logra a través de controles y políticas de seguridad, que deben ser aplicadas en la organización.

15.2. Recomendaciones

- Se recomienda implementar un área encargada de seguridad.
- Se recomienda implementar un Sistema de Gestión de seguridad de la información el mismo que debe ser supervisado gestionado monitoreado, auditado de manera continua enfocado a la protección de la información y mejora continua.
- Mejorar los controles de acceso a las diferentes plataformas de la organización, implementar doble factor de autenticación.
- Se recomienda integrar una campaña de concientización de personal inmerso en el manejo de información dentro de la organización.
- Se recomienda capacitar continuamente en temas de seguridad de la información a todo el personal de la organización.

Referencias

Advisera Expert Solutions Ltd. (07 de 04 de 2022). *https://advisera.com*. Obtenido de https://advisera.com: https://advisera.com/27001academy/es/que-es-iso-27001/

Chubb. (s.f.). *chubb.com*. Obtenido de chubb.com: chubb.com/co-es/pymes/articulos/que-es-el-riesgo-inherente-y-como-actuar.html#:~:text=El%20riesgo%20inherente%20es%20aquel,de%20gestión%20de%20las%20compañías.

Ibañies, A. (2 de 12 de 2009). *es.scribd.com.* Obtenido de es.scribd.com: https://es.scribd.com/doc/23446329/TI-Auditoria-de-Sistemas

Isbel. (5 de 4 de 2021). *https://isbel.com.* Obtenido de https://isbel.com: https://isbel.com/seguridad-de-la-informacion-vulnerabilidades-riesgos/#:~:text=El%20riesgo%20consiste%20en%20las,de%20manera%20eficiente%20y%20responsable.

ISOTools. (6 de 3 de 2015). *https://www.pmg-ssi.com*. Obtenido de https://www.pmg-ssi.com: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/#:~:text=El%20m%C3%A9todo%20MAGERIT%2C%20son%20las,An%C3%A1lisis%20y%20Gesti%C3%B3n%20de%20Riesgos).

ISOTools. (6 de 4 de 2016). *https://www.pmg-ssi.com*. Obtenido de https://www.pmg-ssi.com: https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

Londoño, I. (13 de 10 de 2022). *www.piranirisk.com*. Obtenido de www.piranirisk.com: https://www.piranirisk.com/es/blog/mapa-de-calor-una-herramienta-para-optimizar-la-gestion-de-riesgos

Macero, B. (16 de 10 de 2018). *https://www.yumpu.com.* Obtenido de https://www.yumpu.com: https://www.yumpu.com/es/document/view/62150485/informe-coso-resumen

Portal de Administración Electrónica. (1 de 10 de 2012). *https://administracionelectronica.gob.es*. Obtenido de https://administracionelectronica.gob.es: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Rayas, A. (22 de 7 de 2020). *https://www.hostdime.com*. Obtenido de https://www.hostdime.com: https://www.hostdime.com.pe/blog/que-es-una-vulnerabilidad-en-seguridad-informatica-ejemplos/#:~:text=Las%20vulnerabilidades%20pueden%20permitir%20a,poder%20conectarse%20al%20sistema%20inform%C3%A1tico.

Reyes, W. (26 de 11 de 2018). *https://es.scribd.com.* Obtenido de https://es.scribd.com: https://es.scribd.com/document/394196412/Riesgo-Inherente-y-Residual

Roy, M. (7 de 04 de 2018). *www.computerweekly.com*. Obtenido de www.computerweekly.com: https://www.computerweekly.com/es/definicion/Mapa-

de-riesgos-o-mapa-de-calor-de-riesgos#:~:text=Un%20mapa%20de%20riesgos%2C%20tambi%C3%A9n,riesgos%20asociados%20con%20su%20negocio.

Sullivan, P. (22 de 11 de 2016). *https://www.computerweekly.com*. Obtenido de https://www.computerweekly.com: https://www.computerweekly.com/es/consejo/Gestion-de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes

Villamizar, C. (22 de 10 de 2020). *https://www.globalsuitesolutions.com*. Obtenido de https://www.globalsuitesolutions.com: https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/

ANEXOS

Anexo 1. Herramienta de evaluación.xlsx

Herramienta%20de%20Evaluación.xlsx

Anexo 2. Activo crítico servidor.xlsx

Activo%20crítico%20servidor.xlsx

Anexo 3. Activo crítico base de datos.xlsx

Activo%20crítico%20base%20de%20dat

Anexo 4. Planes de Acción SGSI.xlsx

Planes%20de%20Acción%20SGSI.xlsx

https://udlaec-my.sharepoint.com/:f:/g/personal/segundo_cayo_udla_edu_ec/Eufv4h_eFPhPop0bL2ZXZK0BX9A7jWSwO0NSJeKCX01h_w?e=cMKJ1F