Análisis de Riesgos para Yobel SCM

Enríquez Daniel, Tinoco Jeimmy, Toapanta Jonathan

Universidad de las Fuerzas Armadas ESPE
Departamento de Ciencias de la Computación
Quito – Pichincha – Ecuador

***Resumen*— Este documento analiza la gestión de la seguridad de la información en Yobel SCM Quito, identificando los activos críticos tecnológicos y de datos más relevantes, como el servidor empresarial, el ERP, y la base de datos de clientes. A través de metodologías como MAGERIT, se evaluaron amenazas internas (errores humanos, accesos indebidos) y externas (ciberataques, desastres naturales). Se clasificaron los riesgos por su probabilidad e impacto, priorizando los críticos, como ataques de DDoS y ransomware. Finalmente, se propusieron salvaguardas técnicas, administrativas y físicas para mitigar riesgos y garantizar la continuidad operativa, la protección de datos y el cumplimiento normativo.**

Palabras clave: Seguridad de la Información, Activos críticos, Análisis de riesgos,

I. Introducción

La información es un activo esencial en Yobel SCM, especialmente en su sucursal de Quito, donde los datos y sistemas tecnológicos son pilares para garantizar la continuidad operativa y la excelencia en la gestión de la cadena de suministro. Sin embargo, estos activos enfrentan amenazas internas, externas, naturales y tecnológicas que pueden comprometer su confidencialidad, integridad y disponibilidad, afectando la confianza de los clientes y la reputación empresarial.

En este contexto, se llevó a cabo un análisis integral basado en la metodología MAGERIT e ISO 27005, que permitió identificar los activos críticos, como el servidor empresarial, el ERP y la base de datos de clientes, y evaluar sus riesgos asociados. Se clasificaron las amenazas por probabilidad e impacto, priorizando aquellas que representan un riesgo crítico para las operaciones, como los ataques de ransomware y DDoS, así como las configuraciones incorrectas en sistemas clave.

El análisis concluye con un conjunto de salvaguardas técnicas, administrativas y físicas, diseñadas para mitigar los riesgos y fortalecer la resiliencia tecnológica de Yobel SCM. A través de un plan de acción bien estructurado, la organización busca garantizar la continuidad operativa, proteger la información estratégica y fomentar una cultura de seguridad entre sus colaboradores. Este documento detalla cada paso del proceso, desde la identificación de activos hasta la implementación de soluciones específicas.

II. Desarrollo de Contenidos

Yobel SCM es una empresa multinacional especializada en la gestión de la cadena de suministro (Supply Chain Management, SCM) en América Latina. Fundada hace más de 50 años, ofrece servicios integrales que abarcan planificación, abastecimiento, manufactura y logística, incluyendo almacenamiento, distribución y comercio exterior [1]. Su objetivo principal es optimizar las cadenas de suministro mediante tecnologías avanzadas y estándares de calidad elevados.

En una sucursal de Yobel SCM como la de Quito, los activos críticos pueden clasificarse en tangibles e intangibles, considerando las operaciones logísticas y de cadena de suministro que gestionan. A continuación, se describe cada una de las actividades según el proyecto planteado:

A. Descripción de qué es la seguridad de la información y por qué es crucial para la operación y sostenibilidad de la empresa elegida.

La seguridad de la información se refiere a las prácticas y sistemas destinados a proteger los datos y activos informáticos de una organización contra accesos no autorizados, alteraciones, divulgaciones, y destrucción. Esto abarca la confidencialidad, integridad, y disponibilidad de los datos.

[1] Para Yobel SCM, que maneja grandes volúmenes de información crítica como datos de clientes, inventarios y procesos logísticos, la seguridad de la información es fundamental para:

- Garantizar la Confianza de los Clientes: Los datos sensibles de los clientes requieren protección para evitar filtraciones.
- Continuidad Operativa: La pérdida de datos podría paralizar operaciones clave como la gestión de inventarios y distribución.
- Cumplimiento Normativo: En Ecuador, normativas de protección de datos como la Ley Orgánica de Protección de Datos Personales (LOPDP) obligan a implementar medidas de seguridad.
- Protección de la Reputación: Un incidente de seguridad puede dañar la imagen y credibilidad de la empresa.

B. Identificación y clasificación de los activos críticos de la empresa, diferenciando entre activos tangibles e intangibles y su relevancia para los objetivos del negocio.

En Yobel SCM existen varios activos de información que influyen directa e indirectamente en las operaciones diarias para conllevar adelante el trabajo de forma satisfactoria. Sin embargo, algunos activos son más importantes de proteger a diferencia de otros, ya que estos son relevantes para el negocio, y si alguno dejase de funcionar o fuese atacado es muy probable que la empresa no pueda operar de forma satisfactoria. A continuación, se detallan los activos críticos de información más importantes para la compañía.

TABLA I
ACTIVOS CRÍTICOS DE YOBEL CSM

Activo Crítico	Relevancia para el negocio	Tipo
Servidor Empresarial	Centraliza los procesos operativos y garantiza la capacidad de procesar datos críticos en tiempo real.	Tangible
Estaciones de trabajo	Permiten al personal operar sistemas logísticos y gestionar información de inventarios y clientes (ordenadores y laptops).	Tangible
ERP (Enterprise Resource Planning)	Integra las operaciones de la empresa, desde la gestión de inventarios hasta la planificación de rutas y recursos.	Intangible
Base de Datos de Clientes	Almacena información clave sobre clientes, órdenes y contratos, lo que es crucial para ofrecer un servicio personalizado.	Intangible
Sistema de Control de Inventario	Optimiza el almacenamiento y distribución, reduciendo costos y tiempos de entrega.	Intangible
Soluciones de Respaldo en la Nube	Protegen los datos contra pérdida por fallos del sistema o desastres naturales, garantizando la continuidad del negocio.	Intangible

Si bien es cierto que podrían integrarse algunos activos de valor monetario muy altos, estos no influyen directamente en las operaciones diarias de la empresa o son de fácil recuperación/solución por lo que no son agregados; tales como proyectores de reuniones, bandas de cargas, transporte, etc.

Por lo tanto, los activos expuestos se basaron en cuánto es su relación con las operaciones y sostenibilidad de la empresa, que se basa en: confianza de los clientes, continuidad operativa, cumplimiento normativo y protección de la reputación.

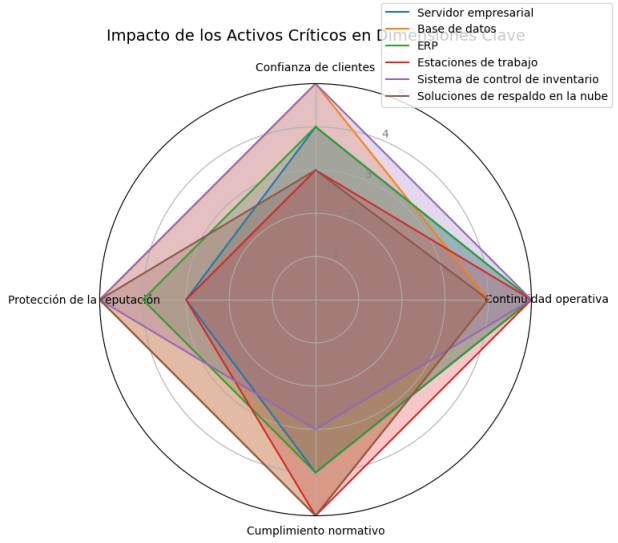

Fig. 1 Relación de los activos críticos con la importancia de las operaciones.

Los activos con áreas más grandes en el gráfico (como la Base de datos de clientes) tienen un impacto mayor en las dimensiones clave, lo que puede guiar decisiones de priorización en seguridad.

Los activos con áreas más pequeñas (como el Servidor empresarial) pueden requerir mejoras específicas en algunas dimensiones.

C. Análisis de las posibles amenazas que podrían afectar a estos activos, incluyendo amenazas internas, externas, naturales y tecnológicas

El siguiente análisis tiene como propósito identificar y evaluar las principales amenazas que pueden comprometer los activos críticos dentro de Yobel SCM, como servidores, sistemas de gestión empresarial (ERP), bases de datos etc. Estos activos no solo respaldan las operaciones diarias, sino que también protegen información clave que impulsa la confianza del cliente, la continuidad operativa y el cumplimiento normativo.

Al mapear cada amenaza con el activo crítico que puede afectar, se logra una visión integral del impacto potencial en los objetivos estratégicos del negocio, sentando las bases para una gestión efectiva del riesgo. A continuación, se detalla cada una de las posibles amenazas:

TABLA II
AMENAZAS EN LOS ACTIVOS
CRÍTICOS DE YOBEL SCM

Tipo de amenaza	Descripción	Activo Crítico Afectado
Internas	Errores humanos: Configuración incorrecta de sistemas o borrado accidental de datos.	-Base de datos de clientes. -ERP
	Acceso indebido**:** Personal no autorizado accediendo a datos sensibles.	- Servidor empresarial - ERP
Externas	Ataques cibernéticos**:** Ransomware, phishing o malware.	- Sistema de respaldo en la nube - ERP - Base de datos de clientes
	Ataques DDoS: Saturación de los servidores con tráfico malicioso.	- Servidor empresarial
Naturales	Desastres naturales**:** Terremotos, temblores de bajo nivel, incendios o inundaciones que afecten la infraestructura física.	- Servidor empresarial - Estaciones de trabajo
Tenológicas	Fallos de hardware**:** Deterioro o mal funcionamiento de componentes físicos.	- Servidor empresarial - Estaciones de trabajo
	Brechas en actualizaciones de software**:** Vulnerabilidades explotadas por atacantes debido a software desactualizado.	- ERP - Sistema de control de inventario - Soluciones de respaldo en la nube

Para una mejor deducción, en el siguiente gráfico se ejemplifica las amenazas más concurrentes con relación al activo crítico afectado:

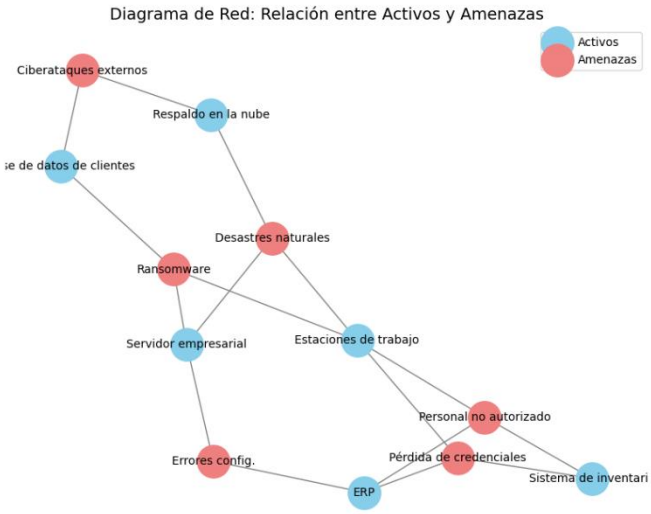

Fig. 2 Amenazas más concurrentes en relación a los activos críticos.

El gráfico muestra claramente cómo cada amenaza puede afectar a varios activos, ayudando a identificar focos de protección prioritaria. Donde las estaciones de trabajo y el servidor empresarial tienen varias amenazas conectadas, lo que indica su criticidad.

D. Evaluación de las vulnerabilidades existentes o potenciales que podrían ser explotadas por las amenazas identificadas, utilizando metodologías como MAGERIT y OCTAVE para su categorización y análisis.

En el contexto de Yobel SCM, la protección de los activos críticos, como su infraestructura TI y los sistemas de información, es fundamental para garantizar la continuidad operativa y el cumplimiento de los objetivos del negocio. La metodología MAGERIT ha sido implementada como un marco de análisis estructurado para identificar y evaluar vulnerabilidades específicas en los activos seleccionados, considerando las amenazas previamente analizadas.

A través de esta metodología, se busca priorizar las áreas de mayor riesgo y proponer medidas correctivas efectivas que refuercen la seguridad de la información y la resiliencia tecnológica de la empresa [2]. A continuación, se detalla el proceso:

1. Inventario de activos

El recuento de los activos corresponde a una fase relevante dentro de la gestión de riesgos ya que permite identificar, clasificar y evaluar los activos necesarios para llevar a cabo el funcionamiento de una serie de procesos de la organización. En el caso de la empresa Yobel SCM se ha llevado a cabo el proceso de identificación de los activos críticos que deben ser protegidos frente a las posibles amenazas y vulnerabilidades. Cada uno de estos activos, serán contabilizados de acuerdo a su finalidad, el valor estratégico para la empresa y su interdependencia con respecto a otros de los componentes esenciales del sistema.

Activos Críticos Identificados

La empresa Yobel SCM presenta una serie de activos fundamentales para llevar a cabo la continuidad de sus operaciones. Son activos tecnológicos: por un lado, el servidor empresarial, el cual almacena información operativa y financiera fundamental para la gestión diaria.

Por otro lado, el Sistema ERP (Enterprise Resource Planning), que integra procesos fundamentales para la operativa de la empresa, tales como finanzas, logística e inventarios. Y finalmente, el sistema de control de inventario, ideado para llevar una gestión en tiempo real de los niveles de stock disponible para asegurar la eficacia operativa [2]. En lo que respecta a los datos, la base de datos de clientes que contiene información confidencial y sensible de los socios comerciales de la organización, la cual le confiere un carácter estratégico de alta prioridad.

A continuación, se muestra una tabla con los activos más relevantes y su importancia en la empresa

TABLA III
CLASIFICACIÓN Y AMENAZAS DE LOS ACTIVOS CRÍTICOS

Activo	**Descripción**	**Categoría**	**Importancia**	**Dependencia**
Servidor empresarial	Almacén de datos operativos y financieros	Tecnológico	Crítico	ERP, base de datos, sistema de inventario
Estaciones de trabajo	Computadoras para tareas administrativas	Infraestructura	Alto	ERP
ERP	Gestión de procesos financieros y logísticos	Tecnológico	Crítico	Servidor empresarial
Base de datos de clientes	Información sensible de socios comerciales	Datos	Crítico	ERP, servidor empresarial
Sistema de control de inventario	Monitoreo de stock en tiempo real	Tecnológico	Alto	ERP
Soluciones de respaldo en la nube	Copias de seguridad de datos	Respaldos	Crítico	Todos los sistemas

2. Identificación de Amenazas y Vulnerabilidades

La identificación de las amenazas y vulnerabilidades es uno de los pasos principales que forman parte del análisis de riesgos, ya que se trata de un punto de apoyo para preverse posibles hechos que hacen peligrar la seguridad de los activos críticos. En este paso se analizan los factores internos y externos que podrían hacer peligrar la organización y las debilidades que podrían ser aprovechadas para hacer efectivas las amenazas. La relación entre el activo, la amenaza, y la vulnerabilidad, se podrá establecer fácilmente.

El análisis de las posibles amenazas externas a las que puede estar sometida Yobel SCM ha considerado las siguientes: ataques cibernéticos (que incluyen el envío de malware a través de correos electrónicos, ransomware y ataques de denegación de servicio), el espionaje industrial y, los desastres naturales (terremotos, entre otras catástrofes naturales), esto puede verse representado por la localización física de Yobel SCM a Quito, Ecuador.

Las amenazas internas a las que está sujeta Yobel SCM son: la información que puede ser proporcionada por el "error humano", la negligencia en la utilización de dispositivos extremos, los accesos a datos sensibles y los accesos a los sistemas críticos. Estas amenazas son especialmente importantes debido a que los empleados juegan un papel crucial en la operación de las configuraciones de sistemas.

En cuanto a las vulnerabilidades, se han encontrado elementos como los no cifrado de las bases de datos, contraseñas débiles, la configuración incorrecta de respaldos en la nube y sin redundancia los sistemas claves. Dicho esto, hacen que las vulnerabilidades anteriores sean factibles las posibilidades de que las amenazas han sido identificadas puedan ser causando mayores daños que afecten directa o indirectamente la integridad y saniticidad de los sistemas

Relación Activo-Amenaza-Vulnerabilidad

Para facilitar el análisis y comprensión de las posibles amenazas y vulnerabilidades que afectan a los activos críticos de Yobel SCM, se ha elaborado una tabla que establece una relación directa entre cada activo identificado, las amenazas específicas que podrían comprometerlo y las vulnerabilidades que podrían ser explotadas. Esta representación permite priorizar los riesgos y enfocar los esfuerzos en aquellos puntos donde la organización es más vulnerable, asegurando así una gestión eficiente y proactiva de la seguridad de la información.

TABLA IV
RELACIÓN ACTIVO-AMENAZA-VULNERABILIDAD EN YOBEL SCM

Activo	Amenaza	Vulnerabilidad
Servidor empresarial	Ataques de denegación de servicio (DDoS)	Falta de firewall avanzado
Estaciones de trabajo	Robo de datos mediante phishing	Contraseñas débiles
ERP	Ransomware	Falta de respaldo actualizado
Base de datos de clientes	Robo de credenciales	Políticas de acceso débiles
Sistema de control de inventario	Fallos de hardware	Falta de redundancia
Soluciones de respaldo en la nube	Configuración incorrecta	Permisos excesivos en acceso

3. Valoración de Riesgos

La valoración de riesgos se sitúa como una fase clave dentro de las características del análisis de un riesgo, porque se puede valorar el impacto y la probabilidad de que una amenaza concreta pueda darse al tener lugar una vulnerabilidad. Este enfoque permite analizar cuantitativa y cualitativamente la criticidad de los riesgos, de forma que puede ordenarse la acción a seguir para su tratamiento.

En el caso de Yobel SCM, la probabilidad y el impacto considerados como base para clasificar los riesgos en niveles crítico, alto, medio o bajo. Valorando de esta forma, la magnitud de las amenazas y permitió orientar los recursos hacia las áreas donde el riesgo es más notorio para la continuidad de negocio.

Matriz de Valoración de Riesgos

Como esta etapa de la fase debe contener un análisis estructurado de comparación de probabilidad e impacto, una tabla es la mejor forma de clasificar los riesgos de activo. Los elementos son:

Activo: Elemento crítico analizado.

Riesgo: Combinación de la amenaza y la vulnerabilidad que afecta al activo.

Probabilidad: Alta, media o baja, según la frecuencia con la que podría ocurrir el riesgo

Escala de probabilidad

TABLA IV
ESCALA DE PROBABILIDADES

Valor	Categoría	Descripción
1	Baja	Es poco probable que ocurra; la frecuencia es mínima.
2	Media	Existe una posibilidad moderada de que ocurra.
3	Alta	Es altamente probable que ocurra; sucede con frecuencia.

Donde el Impacto se mide en: alto, medio o bajo; dependiendo de la gravedad de las consecuencias para el negocio.

Escala de Impacto

TABLA V
ESCALA DE IMPACTOS

Valor	Categoría	Descripción
1	Baja	Las consecuencias serían mínimas y no afectarían significativamente las operaciones.
2	Media	Las operaciones serían notables, pero manejables.
3	Alta	Las consecuencias serían graves y afectarían de manera significativa las operaciones.

Nivel de Riesgo: Resultado de la combinación de probabilidad e impacto.

Los riesgos clasificados como críticos representan una amenaza inmediata y deben ser tratados de manera prioritaria, ya que comprometen la continuidad operativa de la empresa. Los riesgos altos también requieren atención urgente, pero permiten un enfoque a corto plazo. Los riesgos medios y bajos, aunque menos urgentes, deben ser monitorizados para evitar que evolucionen hacia escenarios más graves. Después de mostrar los parámatelos para la identificar el nivel del riesgo se tiene la siguiente tabla:

TABLA VI
CLASIFICACIÓN DE RIESGO

Activo	Riesgo	Probabilidad	Impacto	Nivel de riesgo
Servidor empresarial	Ataques de denegación de servicios	Alta	Alta	Crítico

Estaciones de trabajo	Robo de datos mediante phising	Media	Media	Medio
ERP	Ransomware	Alta	Alta	Crítico
Bade de datos de clientes	Robo de credenciales	Media	Alta	Alto
Sistema de control de inventario	Fallos de hardware	Baja	Medio	Bajo
Soluciones de respaldo en la nube	Configuración incorrecta	Media	Alta	Alto

La evaluación de riesgos efectuada, para los activos críticos, ha determinado que los riesgos de nivel crítico son el servidor empresarial y el sistema ERP, por la alta probabilidad y alto impacto que tienen los mismos. Los riesgos que se consideran de este tipo corresponden a ataques de denegación de servicio (DDoS) y ransomware; suponen una amenaza directa a la continuidad operativa de la organización y se puede afirmar que requieren atención inmediata.

Por otro lado, los riesgos que se consideran altos corresponden al robo de credenciales en la base de datos de clientes y a la falta de la configuración correcta de las soluciones de respaldo en la nube. Dichos riesgos, si bien no son lo crítico y no han mostrado un nivel de urgencia tal como lo han hecho los riesgos críticos, requieren igualmente acciones prioritarias por el alto impacto que los mismos pueden llegar a tener en la seguridad y disponibilidad de los sistemas.

4. Análisis y Selección de salvaguardas

La búsqueda, análisis y selección de las salvaguardas es una parte esencial de la gestión de los riesgos, ya que establece las medidas que deben tomarse con el objetivo de mitigar o gestionar los riesgos hechos visibles. Las medidas que aquí se indican, a veces denominadas salvaguardas o controles, tienen como función la reducción de la probabilidad en la que las amenazas pueden hacerse visibles, acotar el impacto de los riesgos o, en otros casos, eliminar el riesgo por completo.

En el estudio de Yobel SCM, se han priorizado los riesgos críticos y altos, y se han definido las estrategias de tratamiento para cada uno de ellos. Las opciones de tratamiento incluyen mitigación, mediante controles técnicos o administrativos; transferencia del riesgo a un tercero (seguros); aceptación del riesgo o evitación total (si fuera posible).

Propuesta de controles de salvaguardas

A continuación, se muestra una tabla que detalla las salvaguardas recomendadas para cada activo crítico en función del riesgo identificado:

TABLA VII
CONTROLES Y SALVAGUARDAS

Activo Crítico	Riesgo Identificado	Salvaguarda Propuesta	Estrategia de tratamiento
Servidor empresarial	Ataques de denegación de servicios	Implementar un firewall avanzado con protección anti-DDoS; monitoreo continuo con herramientas SIEM	Mitigación
Estaciones de trabajo	Robo de datos mediante phishing	Establecer políticas de autenticación multifactor (MFA) y capacitación regular sobre prevención de phishing	Mitigación
ERP	Ransomware	Implementar respaldos automáticos y encriptados; realizar actualizaciones regulares del software	Mitigación
Base de datos de clientes	Robo de credenciales	Aplicar cifrado avanzado (AES-256) para datos sensibles; revisar políticas de acceso regularmente	Mitigación
Sistema de control de inventario	Fallos de hardware	Establecer redundancia de hardware y realizar pruebas periódicas de recuperación	Mitigación
Soluciones de respaldo en la nube	Configuración incorrecta	Realizar auditorías regulares de configuración y permisos; implementar autenticación multifactor	Mitigación

La tabla de controles y salvaguardas propuesta destaca las medidas más importantes para controlar los riesgos más críticos y altos identificados en Yobel SCM. Se incluyen prioridades como el contar con firewalls avanzados, herramientas SIEM para la protección del servidor empresarial contra ataques DDoS y la capacitación frente al phishing en estaciones de trabajo con autenticación multifactor; el cifrado avanzado de los datos sensibles almacenados en la base de datos de clientes. Las medidas proyectadas tienen como objetivo fortalecer la seguridad y garantizar la continuidad de la operación de los sistemas esenciales.

5. Plan de acción

El plan de acción tiene como finalidad definir y estructurar las actividades necesarias para poder establecer las salvaguardias de las que se ha hecho referencia, asegurándose que la gestión de los riesgos identificados se lleva a cabo. Este plan no solo hace un planteamiento de los procedimientos a ejecutar, ya que también incluye los responsables, los plazos y los recursos a implementar. En el caso de Yobel SCM, el enfoque se da en la línea de abordar primero los mayores y críticos, es decir, aplicar una solución que pueda darse de manera escalonada pero ágil sin interferir en la organización.

Elementos Clave del Plan de Acción

Los elementos clave que conforman el plan de acción se mostraran mediante literales y se explicara el funcionamiento de cada uno de ellos:

A. Priorización de Actividades

Las acciones se priorizan en función del nivel de riesgo y el impacto potencial en los activos críticos. Los riesgos críticos, como los asociados al servidor empresarial y el ERP, requieren atención inmediata. Por otro lado, los riesgos altos relacionados con la base de datos de clientes y los respaldos en la nube, deben

ser tratados en el corto plazo.

B. Asignación de responsables

Cada acción será asignada a un equipo o individuo responsable. El equipo de TI liderará la implementación de controles tecnológicos, como firewalls, SIEM y autenticación multifactor, mientras que los responsables de seguridad de la información supervisarán las políticas de acceso y el cifrado de datos.

C. Cronograma de Ejecución

Se establecerán plazos claros para cada actividad:

i. Los riesgos críticos deberán ser mitigados en un plazo no mayor a 3 meses.

ii. Las acciones para riesgos altos deben completarse en un período de 6 meses.

D. Seguimiento y Monitoreo

EI seguimiento y control se encargarán de garantizar la adherencia de las salvaguardas implementadas. Para ello se llevarán a cabo auditorías internas en los trimestres en los que se haga una revisión de consistencia de configuraciones de seguridad, políticas de acceso y medidas de cifrado en los activos críticos y también se utilizarán herramientas SIEM (Security Information and Event Management) para la supervisión en tiempo real generando alertas automáticas en caso de actividad sospechosa.

Los registros de acceso se revisarán de forma diaria para detectar posibles anomalías y dar respuestas a tiempo a los incidentes de seguridad. Esto garantizará la actualización a posibles amenazas nuevas que puedan surgir.A continuación, se muestra una tabla que especifica en detalle el plan de acción.

TABLA VIII
PLAN DE ACCIÓN

Riesgo	**Acción propuesta**	**Responsable**	**Plazo**	**Recursos necesarios**
Atauqes de denegación de servicios	Implementar firewall avanzado y herramientas SIEM.	Equipo de TI	3 meses	Software especializado, capacitación
Ransomware	Respaldos automáticos y actualizaciones regulares.	Equipo de TI	3 meses	Infraestructura de respaldo
Robo de credenciales (base de datos)	Implementar cifrado AES-256 y políticas de acceso.	Responsable de Seguridad TI	6 meses	Herramientas de cifrado, auditorías
Configuración incorrecta (Respaldos en la nube)	Auditorías regulares y autenticación multifactor.	Equipo de TI	6 meses	Acceso a servicios en la nube

E. Propuesta de controles adecuados y salvaguardas para mitigar los riesgos asociados a las vulnerabilidades identificadas, incluyendo controles físicos, administrativos y técnicos.

Partiendo de la metodología MAGERIT previamente realizada para la mitigación de riesgos de las vulnerabilidades detectadas en Yobel SCM, se han desarrollado controles integrales considerándose las medidas técnicas, las administrativas y las físicas. Estas medidas pretenden reducir tanto la probabilidad de ocurrencia como el impacto de los riesgos sobre los activos esenciales de la misma.

Controles de integración

i. Controles técnicos

la aplicación de controles técnicos se debe realizar mediante el despliegue de firewalls avanzados y herramientas SIEM para la vigilancia continua y en tiempo real de amenazas. También se recomienda la aplicación de cifrado avanzado (AES-256) en datos sensibles y la implementación de políticas de autenticación multifactor (MFA) para la protección de acceso a sistemas. Asimismo, se da prioridad a la realización de backups automáticos y cifrados con auditorías periódicas en las configuraciones para los sistemas críticos.

ii. Controles administrativos

Los controles administrativos abarcan la formación continuada del personal para la prevención del phishing y las buenas prácticas en ciberseguridad. Igualmente, se propone la creación de políticas claras de acceso, revisando periódicamente los permisos asignados para verificar que son los adecuados. Aparte de esto, se propone la programación de auditorías trimestrales que midan la efectividad de las medidas de control implementadas garantizando su adecuación frente a nuevas amenazas.

iii. Controles físicos

Para los controles físicos se aconseja reforzar la seguridad de las instalaciones a través el acceso restringido a áreas críticas, como los servidores de la empresa. Se considera igualmente muy importante asegurar la redundancia del hardware crítico haciendo todo lo posible por evitar los riesgos asociados a los fallos operativos o la pérdida de datos y por la continuidad de las operaciones de la organización.

F. Análisis de gestión de riesgos para Yobel SCM siguiendo ISO 27005, ISO 31000 y NIST SP 800-30

La gestión de riesgos en Yobel SCM es un pilar esencial para garantizar la seguridad de los activos tecnológicos y la continuidad operativa. Este análisis aborda los riesgos de los activos críticos seleccionados en el área de TI, utilizando como guía las directrices de ISO 27005, ISO 31000 y el marco metodológico del NIST SP 800-30. A lo largo del proceso, se identifican amenazas, vulnerabilidades y controles específicos para cada activo, asegurando un tratamiento adaptado a las necesidades de la organización [3].

1. Establecimiento del Contexto

El establecimiento del contexto es el punto de partida, ya que permite comprender la relación entre los activos de TI, los procesos de negocio y las amenazas que los rodean.

1. Activos Críticos Identificados:

- Servidor empresarial: Almacena datos operativos y financieros. Su función es clave para gestionar las operaciones diarias y los servicios que ofrece Yobel SCM.
- Estaciones de trabajo: Computadoras utilizadas por los empleados para llevar a cabo tareas administrativas y operativas.
- ERP (Enterprise Resource Planning): Sistema que integra áreas como finanzas, logística e inventario.

- Base de datos de clientes: Contiene información sensible y confidencial sobre los socios comerciales de Yobel.
- Sistema de control de inventario: Monitoreo en tiempo real del stock, clave para garantizar la eficiencia operativa.
- Soluciones de respaldo en la nube: Copias de seguridad para recuperación ante desastres.

2. Entorno de Operación:

- Ubicación: Quito, Ecuador, donde la sucursal está expuesta a riesgos naturales como terremotos y posibles inundaciones.
- Infraestructura Tecnológica: Conexiones de red internas y externas, con servidores alojados localmente y respaldos en la nube.

3. Criterios de Riesgo:

Los riesgos se clasifican como bajos, medios, altos o críticos según su impacto y probabilidad:

 Críticos: Requieren intervención inmediata, ya que comprometen la continuidad del negocio.

 Altos: Necesitan tratamiento a corto plazo.

 Medios: Evaluación del costo-beneficio para tratarlos.

 Bajos: Supervisión periódica sin necesidad de intervención inmediata.

4. Partes Interesadas:

- Alta dirección: Toma decisiones estratégicas basadas en los resultados del análisis.
- Equipo de TI: Responsable de implementar y mantener los controles.
- Personal operativo: Usuarios de los sistemas, clave para prevenir riesgos operativos.

2. Identificación de Riesgos

La identificación de riesgos incluye un análisis exhaustivo de las posibles amenazas y vulnerabilidades que podrían afectar a los activos.

1. Amenazas Externas:
   - Ataques cibernéticos: Ransomware, phishing, ataques de denegación de servicio (DDoS).
   - Espionaje industrial: Intentos de acceder a información confidencial por parte de competidores.
   - Desastres naturales: Terremotos o inundaciones que afecten las instalaciones.
2. Amenazas Internas:
   - Errores humanos: Configuraciones incorrectas, pérdida de datos.
   - Negligencia: Uso inadecuado de dispositivos externos (USB infectados).
   - Acceso no autorizado: Empleados con permisos excesivos.
3. Vulnerabilidades Detectadas:
   - Falta de cifrado en la base de datos de clientes.
   - Contraseñas débiles o políticas de cambio poco estrictas.
   - Configuración inadecuada en respaldos en la nube.
   - Ausencia de redundancia en el sistema de control de inventario.
4. Relación Activo-Amenaza-Vulnerabilidad:

TABLA IX
RELACIÓN ACTIVO-AMENAZA-VULNERABILIDAD

Activo	Amenaza	Vulnerabilidad
Servidor empresarial	Ataque DDoS	Falta de firewall avanzado
Estaciones de trabajo	Robo de datos mediante phishing	Contraseñas débiles
ERP	Ransomware	Falta de respaldo actualizado
Base de datos de clientes	Robo de credenciales	Políticas de acceso débiles
Sistema de inventario	Fallos de hardware	Falta de redundancia
Respaldo en la nube	Configuración incorrecta	Permisos excesivos en accesos

3. Análisis del Riesgo

El análisis del riesgo se realiza mediante la evaluación de probabilidad e impacto de cada amenaza, utilizando una matriz de criticidad.

1.Matriz de Probabilidad e Impacto:

- Probabilidad: Alta, media, baja.
- Impacto: Alto, medio, bajo.

TABLA X
MATRIZ DE PROBABILIDAD DE IMPACTO

Activo	Riesgo	Probabilidad	Impacto	Nivel de Riesgo
Servidor empresarial	Ataque DDoS	Alta	Alta	Crítico
Estaciones de trabajo	Robo de datos mediante phishing	Media	Media	Medio
ERP	Ransomware	Alta	Alta	Crítico
Base de datos de clientes	Robo de credenciales	Media	Alta	Alto
Sistema de inventario	Fallos de hardware	Baja	Medio	Bajo
Respaldo en la nube	Configuración incorrecta	Media	Alta	Alto

4.Tratamiento del Riesgo

Para cada riesgo identificado, se define una estrategia basada en las opciones de mitigación, transferencia, aceptación o evitación.

TABLA XI
TRATAMIENTO DEL RIESGO

Activo Crítico	Riesgo Identificado	Estrategia de Tratamiento
Servidor Empresarial	Exposición a ataques cibernéticos (DDoS, intrusiones, fallos)	- Implementar firewall avanzado y mitigación contra DDoS. - Monitoreo continuo mediante herramientas SIEM para detectar actividades sospechosas en tiempo real.
Estaciones de Trabajo	Phishing, malware, acceso no autorizado a dispositivos	- Capacitación continua en prevención de phishing. - Autenticación multifactor (MFA) obligatoria. - Antivirus y políticas de seguridad de endpoints.
ERP (Enterprise Resource Planning)	Pérdida de datos, ataques cibernéticos, fallos en software	- Respaldos automáticos y encriptados de bases de datos. - Actualización continua del software. - Auditoría de logs de acceso y cambios críticos.
Base de Datos de Clientes	Robo de datos, acceso no autorizado a información personal	- Implementar cifrado avanzado de datos (AES-256). - Establecer contraseñas robustas con políticas de caducidad periódica. - Auditorías de acceso regulares.
Sistema de Inventario	Pérdida de datos, interrupción en la operación	- Redundancia de hardware y software para garantizar disponibilidad. - Backup en tiempo real de datos e inventarios.
Respaldo en la Nube	Acceso no autorizado, pérdida de datos almacenados en la nube	- Revisión de permisos de acceso regularmente. - Implementar autenticación multifactor para acceder a los respaldos en la nube. - Monitoreo de actividades.

5. Monitoreo y Revisión

El monitoreo y la revisión constante son fundamentales para garantizar que las estrategias de tratamiento sean efectivas a largo plazo y que los riesgos sigan siendo gestionados adecuadamente [3].

Auditorías Periódicas:

• Revisión de Configuraciones de Seguridad: Se llevará a cabo una auditoría interna cada seis meses para revisar las configuraciones de seguridad de todos los sistemas críticos, incluidos firewalls, sistemas de respaldo y bases de datos. Estas auditorías estarán alineadas con las mejores prácticas de ciberseguridad y las normas internacionales.

• Actualización de Políticas: Las políticas de seguridad deben ser actualizadas anualmente, y siempre que surjan nuevas amenazas, tomando en cuenta tendencias emergentes y nuevas vulnerabilidades descubiertas en el entorno tecnológico.

Supervisión Continua:

• Monitoreo de Seguridad en Tiempo Real: Se implementará un sistema centralizado de monitoreo utilizando herramientas de SIEM para detectar actividades sospechosas o eventos inusuales en tiempo real. El sistema generará alertas automáticas que serán analizadas inmediatamente por el equipo de TI.

• Revisión de Logs: Se revisarán los logs de acceso y actividad de los sistemas críticos de manera diaria para detectar posibles amenazas y actividades inusuales, como intentos de acceso no autorizado.

6. Comunicación y Consulta

La comunicación y la consulta son esenciales para asegurar que todos los involucrados estén alineados con los objetivos de seguridad y que las estrategias de tratamiento de riesgos se implementen correctamente [5].

Informes Periódicos:

• Informes a la Alta Dirección: Se presentarán informes trimestrales a la alta dirección sobre los avances en la gestión de riesgos, incluyendo estadísticas de incidentes de seguridad, acciones correctivas implementadas y áreas de mejora. Los informes estarán acompañados de un análisis del impacto potencial de los riesgos identificados en los objetivos estratégicos de la empresa.

• Reuniones de Consulta con el Equipo de TI: Además de los informes, se organizarán reuniones mensuales con el equipo de TI para evaluar el estado de la infraestructura tecnológica, discutir incidentes recientes y ajustar las políticas de seguridad según las necesidades emergentes.

Capacitación:

• Capacitación en Ciberseguridad: Se organizarán talleres anuales sobre ciberseguridad para todo el personal, cubriendo temas como la protección contra phishing, el uso de contraseñas seguras, y la detección de actividades sospechosas. Estos talleres también incluirán sesiones prácticas donde los empleados puedan simular y aprender a manejar posibles incidentes de seguridad.

• Sensibilización de los Empleados: A través de campañas de concientización continua, se fomentará una cultura de seguridad en toda la empresa. El objetivo es hacer que todos los empleados sean responsables de la seguridad de los activos informáticos y estén capacitados para identificar y prevenir amenazas antes de que ocurran.

G. Aplicación de métodos cuantitativos y cualitativos para evaluar la severidad de los riesgos y la efectividad de las respuestas propuestas.

Al clasificar los activos de la organización, el objetivo principal es asignarles un valor que refleje su importancia para la empresa. Este proceso se puede abordar mediante dos tipos de análisis: cuantitativo y cualitativo. A continuación, se detalla cada uno de los métodos implementados en Yobel CSM [5].

Método Cuantitativo

El método cuantitativo permitirá asignar valores monetarios específicos a los riesgos y sus posibles consecuencias, proporcionando un análisis detallado basado en métricas financieras. A continuación, se aplican los pasos

1. Asignar un valor al activo

Es importante declarar una serie de valores monetarios a cada uno de los activos críticos, puesto a que manejará la importancia económica en caso de pérdida y de la misma manera armar un plan de recuperación. Las siguientes cifras son aproximadas:

TABLA XII
VALORES ECONÓMICOS A CADA UNO DE LOS ACTIVOS

Activo	Valor para la organización ($)	Costo de mantenimiento ($/año)	Beneficios ($/año)	Costo de recuperación ($)	Valor para la competencia ($)	Costo de adquisición ($)
Servidor empresarial	50 000	5 000	200 000	60 000	100 000	50 000
Base de Datos de Clientes	75 000	10 000	500 000	100 000	150 000	75 000
ERP	60 000	12 000	300 000	80 000	120 000	60 000
Sistema de control de inventario	40 000	6 000	150 000	50 000	80 000	40 000
Estaciones de trabajo	30 000	4 000	100 000	35 000	50 000	30 000
Soluciones de Respaldo	35 000	8 000	120 000	45 000	70 000	35 000

En la que:

- Valor para la Organización: Representa el valor intrínseco del activo basado en su utilidad para las operaciones diarias.
- Costo de Mantenimiento: Incluye gastos asociados al soporte, actualizaciones y monitoreo anual.
- Beneficios: Estimación de los beneficios generados anualmente por el activo.
- Costo de Recuperación: Coste estimado para restaurar o reemplazar el activo en caso de pérdida.
- Valor para la Competencia: Monto estimado que el activo representaría si fuera adquirido por competidores.
- Costo de Adquisición: Inversión inicial realizada para desarrollar o adquirir el activo.

2. Estimar la pérdida potencial por amenaza

En consiguiente, se debe estimar cuánto puede llegar a afectar cada una de las amenazas, para Yobel SCM se resume en las siguientes:

TABLA XIII
PÉRDIDA POTENCIAL POR AMENAZA

Activo	Amenaza	Daño potencial	Pérdida de productividad	Costo de recuperación ($)	Valor de la pérdida ($)
Servidor empresarial	Ataques DDoS	Interrupción de la operación de sistemas	$ 10 000/día	15 000	25 000
Base de datos de clientes	Robo de datos	Pérdida de confianza de clientes	$20 000	50 000	52 500
ERP	Ransomware	Pérdida de acceso a procesos clave	$ 15 000/día	20 000	36 000
Sistema de control de inventario	Fallos de hardware	Pérdida de inventarios en tiempo real	$ 5000/día	10 000	16 000
Estaciones de trabajo	Robo de datos	Pérdida de datos sensibles	$3 000/día	5 000	9 000
Soluciones de respaldo en la nube	Configuración incorrecta	Pérdida de capacidad de recuperación de datos	$8 000	15 000	17 500

En la que:

- Amenaza: Tipo de amenaza identificada para cada activo.
- Daño Potencial: Impacto general que causaría la amenaza, como pérdida de productividad o daño a la operación.
- Pérdida de Productividad: Estimación de la pérdida diaria de productividad que podría generar la amenaza.
- Costo de Recuperación: Estimación de los costos para restaurar el activo a su estado funcional después de un incidente.
- Valor de la Pérdida ($): Se calcula como el valor total potencial de la pérdida combinando la interrupción, recuperación y otros impactos financieros.

Con estos datos, ya se puede calcular la Expectativa de una Sola Pérdida (SLE)

TABLA XIV
VALORES DE SLE

Activo	Valor del Activo ($)	Factor de Exposición ($)	SLE ($)
Servidor empresarial	50 000	0.5	25 000
Base de datos de clientes	75 000	0.7	52 500
ERP	60 000	0.6	36 000
Sistema de control de inventario	40 000	0.4	16 000
Estaciones de trabajo	30 000	0.3	9 000
Soluicones de respaldo en la nube	35 000	0.5	17 500

3. Realizar un análisis de las amenazas

TABLA XIV
VALORES ALE

Activo	Valor del Activo ($)	Factor de Exposición ($)	SLE ($)	ARO	ALE
Servidor empresarial	50 000	0.5	25 000	0.5	12 500
Base de datos de clientes	75 000	0.7	52 500	0.25	13 125
ERP	60 000	0.6	36 000	0.40	14 400
Sistema de control de inventario	40 000	0.4	16 000	0.20	3 200
Estaciones de trabajo	30 000	0.3	9 000	0.30	2 700
Soluicones de respaldo en la nube	35 000	0.5	17 500	0.15	2 625

Como se puede apreciar, el ERP tiene el mayor ALE, seguido por la Base de Datos de Clientes y el Servidor Empresarial, lo que los convierte en los activos más prioritarios para protección.

Para una mejor interpretación de los resultados, el siguiente gráfico presenta las pérdidas anuales esperadas considerando la frecuencia de ocurrencia.

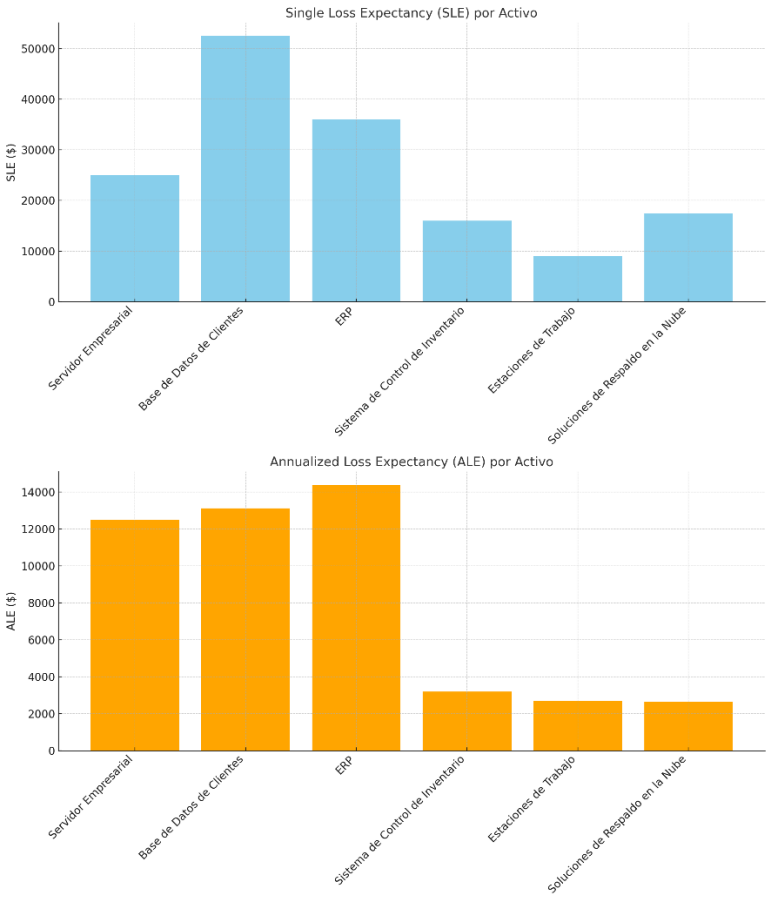

Fig. 3 Análisis de las amenazas según su SLE y ALE.

El gráfico muestra las pérdidas esperadas por un único evento de amenaza para cada activo. Donde los activos con mayor SLE son la Base de Datos de Clientes y el ERP, reflejando su alta criticidad en caso de pérdida.

Método Cualitativo

El análisis de riesgo cualitativo debe realizarse cuando Yobel SCM produzca un cambio en la percepción de un riesgo y cuando se haya identificado un nuevo riesgo. Sin embargo, a esta altura del desarrollo es difícil percibir un nuevo posible riesgo, por lo que se utilizará los ya existentes para llevar a cabo la ejemplificación [4].

1. Identificar de riesgos

Para el método cualitativo, se ha identificado los siguientes riesgos según las amenazas y vulnerabilidades expuestas en los activos críticos de Yobel SCM:

Internas:

- Errores humanos: Configuración incorrecta de sistemas o borrado accidental de datos.
- Acceso indebido: Personal no autorizado accediendo a datos sensibles.

Externas:

- Ataques cibernéticos: Ransomware, phishing o malware.

- Ataques DDoS: Saturación de los servidores con tráfico malicioso.

Naturales:

- Desastres naturales: Terremotos, temblores de bajo nivel, incendios o inundaciones que afecten la infraestructura física.

Tecnológicas:

- Fallos de hardware: Deterioro o mal funcionamiento de componentes físicos.
- Brechas en actualizaciones de software: Vulnerabilidades explotadas por atacantes debido a software desactualizado.

2. Clasificar de riesgos

En este paso, se clasifica los riesgos identificados según su probabilidad de ocurrencia y el impacto que tendrían si se materializan. Para ello se utilizó una escala de 1 a 5 para ambos factores:

TABLA XV
CLASIFICACIÓN DE RIESGOS

Riesgo	Probabilidad	Impacto	Clasificación de Riesgo
Errores humanos (Configuración/Acceso indebido)	3	4	Medio-Alto
Ataques cibernéticos (Ransomware/Phishing/Malware)	4	5	Alto
Ataques DDoS	3	5	Alto
Desastres Naturales	2	4	Medio
Fallos de Hardware	3	3	Medio
Brechas de Actualizaciones de software	3	4	Medio-Alto

En la que cada uno de los datos se clasifican en los siguientes parámetros:

Escala de Probabilidad:

- **1:** Rara vez ocurre
- **2:** Ocurre ocasionalmente
- **3:** Ocurre a menudo
- **4:** Muy probable
- **5:** Casi seguro que ocurre

Escala de Impacto:

- **1:** Mínimo impacto en la operación
- **2:** Impacto manejable, sin grandes consecuencias
- **3:** Afecta ciertas operaciones, puede ser gestionado
- **4:** Impacto significativo, interrumpe operaciones clave
- **5:** Impacto crítico, afecta gravemente la continuidad operativa

Para una mejor interpretación de resultados, se puede apreciar el siguiente gráfico, en la que mientras más arriba y hacia la derecha se encuentre el punto de riesgo, es más probable que ocurra:

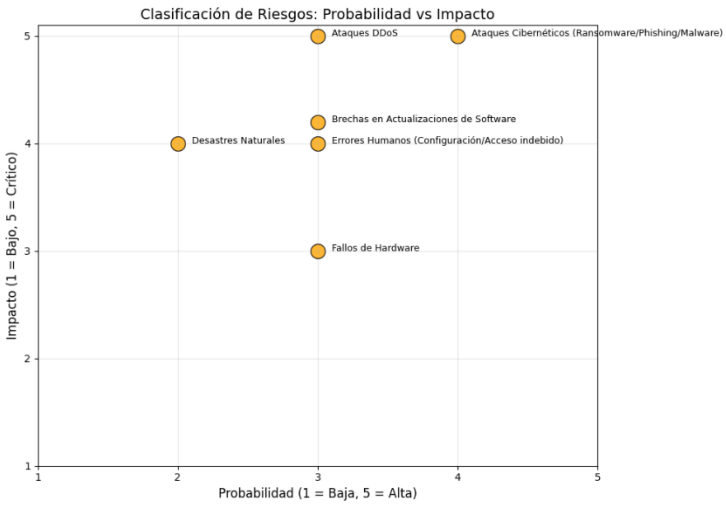

Fig. 4 Clasificación de los riesgos según su probabilidad

3. Controlar los riesgos

Una vez clasificados, pasamos a controlar los riesgos. Para cada riesgo, definimos las estrategias para mitigar su probabilidad o impacto:

TABLA XVI
ESTRATEGIAS PARA MITIGAR LA PROBABILIDAD O IMPACTO

Riesgo	Control Propuesto	Estrategia de Tratamiento
Errores Humanos (Configuración/Acceso indebido)	Implementar políticas de acceso basadas en roles (RBAC), autenticación multifactor (MFA) y capacitación continua en ciberseguridad.	Mitigación y Prevención
Ataques Cibernéticos (Ransomware/Phishing/Malware)	Uso de antivirus avanzado, implementación de firewalls, capacitación en phishing, realizar backups automáticos y encriptados	Mitigación y Prevención
Ataques DDoS	Implementar protección contra DDoS, como firewalls avanzados, y monitoreo continuo con herramientas SIEM.	Mitigación
Desastres Naturales	Implementar soluciones de respaldo en la nube, realizar simulacros de recuperación ante desastres (DRP), y reforzar infraestructura física (backup).	Mitigación y Prevención
Fallos de Hardware	Implementar redundancia de hardware y sistemas de respaldo en tiempo real. Realizar mantenimiento preventivo regular.	Mitigación

Brechas en Actualizaciones de Software	Establecer un calendario de actualizaciones regulares de software y auditorías de vulnerabilidades.	Mitigación

Este análisis cualitativo proporciona un enfoque integral para gestionar los riesgos en la organización, priorizando aquellos con mayor probabilidad e impacto, y proponiendo controles efectivos para reducir su impacto en la operación.

III. CONCLUSIONES

1. **Gestión de Activos Críticos:**
   - Se identificaron y valoraron seis activos fundamentales para Yobel SCM: el servidor empresarial, el ERP, la base de datos de clientes, el sistema de control de inventario, las estaciones de trabajo y las soluciones de respaldo en la nube. Estos activos son pilares para garantizar la eficiencia operativa y la continuidad del negocio.
2. **Relevancia de los Activos:**
   - Cada activo fue evaluado según su impacto y su aporte estratégico. Por ejemplo, el ERP y la base de datos de clientes demostraron ser los activos con mayor criticidad debido a su influencia directa en la integración de procesos y la gestión de información sensible.
3. **Identificación de Amenazas:**
   - Las amenazas se clasificaron en internas, externas, naturales y tecnológicas, destacando riesgos como ataques cibernéticos (ransomware, DDoS), errores humanos y desastres naturales. Estos riesgos representan un desafío continuo para la seguridad de los activos críticos.
4. **Aplicación del Método Cuantitativo:**
   - El análisis cuantitativo permitió asignar valores monetarios a los activos y calcular indicadores clave como el SLE (Single Loss Expectancy) y el ALE (Annualized Loss Expectancy). Este enfoque cuantificó el impacto económico de cada amenaza, ayudando a priorizar las medidas de mitigación.
5. **Aplicación del Método Cualitativo:**
   - A través del método cualitativo, se clasificaron los riesgos según su probabilidad e impacto, utilizando una escala descriptiva. Esto permitió identificar riesgos altos, como ataques cibernéticos y errores humanos, y definir estrategias específicas de control y mitigación.
6. **Propuesta de Controles:**
   - Se diseñaron medidas técnicas (firewalls avanzados, cifrado, autenticación multifactor), administrativas (políticas de acceso, capacitación continua) y físicas (respaldo en la nube, redundancia de hardware) para proteger los activos y minimizar los riesgos identificados.
7. **Visualización y Análisis de Datos:**
   - Los gráficos y tablas presentados facilitaron la comprensión de la clasificación de riesgos, el impacto financiero esperado y las relaciones entre amenazas y activos. Estas visualizaciones son herramientas valiosas para la toma de decisiones estratégicas.
8. **Aplicación de MAGERIT:**
   - La metodología MAGERIT fue clave para estructurar el análisis de riesgos, proporcionando un marco sólido para evaluar la seguridad de los activos y definir un plan de acción alineado con los objetivos organizacionales.
9. **Impacto General en Yobel SCM:**
   - Este análisis refuerza la importancia de la seguridad de la información en la sucursal de Quito, destacando cómo la gestión proactiva de riesgos puede proteger los activos más valiosos, garantizar la continuidad operativa y fortalecer la confianza de los clientes.

REFERENCIAS

[1] Yobel SCM. (2022.). Ecuador: Soluciones de logística integral. Recuperado el 10 de diciembre de 2024, de https://www.yobelscm.biz/ecuador/

[2] Instituto Nacional de Tecnologías de la Comunicación. (2021). MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (v.3). España: Ministerio de Hacienda y Administraciones Públicas. Recuperado de https://www.csi.gob.es/

[3] International Organization for Standardization. (2019). ISO/IEC 27005:2018 – Information Security Risk Management. Ginebra: ISO. Recuperado de https://www.iso.org/

[4] Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security (6th ed.). Boston: Cengage Learning.

[5] Consejo Nacional de Ciberseguridad de Ecuador. (2021). Guía para la Protección de Infraestructuras Críticas. Quito, Ecuador.