TEC | Tecnológico de Costa Rica

Área Académica de Administración de Tecnologías de Información

Propuesta de un Plan de Gestión de Vulnerabilidades de Red para el departamento de IT Operations and Compliance de Symbiotic

Trabajo Final de Graduación para optar al grado de Licenciatura en Administración de Tecnología de Información

Elaborado por: Ariel Enrique Rodríguez Cruz

Prof. Tutor: MSc. Pedro Leiva Chinchilla

Cartago, Costa Rica

Semestre 2, 2023

Noviembre, 2023

Hoja de Aprobación

AREA ACADÉMICA DE ADMINISTRACIÓN DE TECNOLOGIA DE INFORMACIÓN

GRADO ACADEMICO LICENCIATURA

Los miembros de Tribunal Examinador de Área Académica de Administración de Tecnología de Información, recomendamos que el siguiente Trabajo Final de Graduación del estudiante Ariel Enrique Rodríguez Cruz sea aceptado como requisito parcial para optar por el grado académico de Licenciatura en Administración de Tecnología de Información.

TEC | Tecnológico de Costa Rica

Firmado digitalmente por YARIMA TATIANA SANDOVAL SANCHEZ (FIRMA)
Fecha: 2023.11.28 15:14:39 -06'00'

Ing. Yarima Sandoval Sánchez

Coordinación Trabajo Final de Graduación

JOSE AGUSTIN FRANCESA ALFARO (FIRMA)
2023.11.28 13:57:38 -06'00'

Msc. José Agustín Francesa Alfaro

Lector Académico

Lic. Isaac López Delgado

Lector de Industria

Firmado digitalmente por PEDRO IGNACIO LEIVA CHINCHILLA (FIRMA)
Fecha: 2023.11.28 12:06:36 -06'00'

MSc. Pedro Leiva Chinchilla

Profesor Tutor

Dedicatoria

A mi familia, por apoyarme en las diferentes etapas de mi vida y estar cuando lo necesite.

A mi madre, por ser una fuente de motivación y velar por mi bienestar.

A mi padre, por inspirarme a seguir adelante y enseñarme a trabajar para conseguir mis metas.

Agradecimientos

A mis hermanos, Iván y María quienes me han enseñado a trabajar para ser un ejemplo para ellos y me apoyaron durante la realización del proyecto.

A Valeria Martínez, por apoyarme en estos tres últimos años de la carrera, por motivarme, acompañarme y creer en mis capacidades, así como por ser mi fuente de descanso.

A mi profesor tutor, Pedro Leiva por ayudarme constantemente mientras realizaba el TFG, por su retroalimentación y consejos de vida y profesionales.

A mis amigos en especial a los últimos de este año y conocidos que, a lo largo de mi carrera universitaria, me acompañaron a experimentar un crecimiento tanto en lo profesional como en lo personal.

Al personal de Symbiotic tanto a mis jefes Guillermo Ávila, como a don Javier Chacón por brindarme la oportunidad de realizar el TFG y por los consejos para crecer como profesional.

Resumen

Este documento presenta la concepción y ejecución de un Plan de Gestión de Vulnerabilidades de Red, con el objetivo de establecer un marco de trabajo que abarque todas las fases del ciclo de vida de dicha gestión. El propósito central es estandarizar los procesos relacionados con la gestión de Vulnerabilidades de Red, alineándolos con las buenas prácticas de la industria, lo cual resulta esencial para salvaguardar activos críticos y datos sensibles manejados por Symbiotic.

El Capítulo I identifica la problemática en el departamento de IT Operations and Compliance, asociada con una gestión ineficiente de las vulnerabilidades de red. Se evidencian incumplimientos de estándares internacionales, dificultades en la comunicación entre equipos de seguridad y TI, y la falta de procedimientos claros para identificar y clasificar vulnerabilidades. El Capítulo II establece las bases teóricas necesarias.

La metodología adoptada, explicada en el Capítulo III, es cualitativa con un alcance explicativo y un diseño de investigación-acción. El Capítulo V presenta la solución, centrada en la implementación de un marco de trabajo basado en la metodología de BPM. Este enfoque busca estandarizar eficientemente las fases de detección, categorización, priorización, mitigación, evaluación y comunicación de vulnerabilidades de red, garantizando la adherencia a estándares internacionales.

Además, se propone una estrategia de implementación que aborda aspectos completados, asigna responsabilidades y establece un cronograma. Se incluye un plan de comunicación y la definición de métricas de control para monitorear y evaluar la efectividad del plan. En resumen, el documento propone una solución integral que no solo aborda las problemáticas identificadas, sino que también establece un camino claro para la implementación exitosa del plan de gestión de vulnerabilidades de red en Symbiotic.

Palabras Claves: Marco de Trabajo, Gestión de Vulnerabilidades de Red, BPM, Estandarización, Modelos, Procesos, Análisis, KPI’s, Vulnerabilidades de Red.

Abstract

This document introduces the conception and implementation of a Network Vulnerability Management Plan, aiming to establish a framework that encompasses all phases of its life cycle. The primary objective is to standardize processes related to Network Vulnerability Management, aligning them with industry best practices, which is essential for safeguarding critical assets and sensitive data handled by Symbiotic.

Chapter I identifies the issues within the IT Operations and Compliance department, linked to inefficient management of network vulnerabilities. There are observed breaches of international standards, communication challenges between security and IT teams, and a lack of clear procedures for identifying and classifying vulnerabilities. Chapter II lays down the necessary theoretical foundations.

The adopted methodology, explained in Chapter III, is qualitative with an explanatory scope and an action research design. Chapter V presents the solution, focusing on implementing a framework based on the BPM methodology. This approach aims to efficiently standardize the phases of detection, categorization, prioritization, mitigation, evaluation, and communication of network vulnerabilities, ensuring adherence to international standards.

Furthermore, a implementation strategy is proposed in Chapter V, addressing completed aspects, assigning responsibilities, and establishing a timeline. This includes a communication plan and the definition of control metrics to monitor and evaluate the plan's effectiveness. In summary, the document proposes a comprehensive solution that not only addresses identified issues but also establishes a clear path for the successful implementation of the network vulnerability management plan at Symbiotic.

Keywords: Framework, Vulnerability Management, BPM, Standardization, Models, Processes, Analysis, KPIs, Vulnerabilities.

Tabla de Contenidos

Índice de Figuras

Índice de Tablas

Nota Aclaratoria

Género[1]:

La actual tendencia al desdoblamiento indiscriminado del sustantivo en su forma masculina y femenina va contra el principio de economía del lenguaje y se funda en razones extralingüísticas. Por tanto, deben evitarse estas repeticiones, que generan dificultades sintácticas y de concordancia, que complican innecesariamente la redacción y lectura de los textos.

Este documento se redacta de acuerdo con las disposiciones actuales de la Real Academia Española con relación al uso del "género inclusivo". Al mismo tiempo se aclara que estamos a favor de la igualdad de derechos entre los géneros.

1. Introducción

En este primer capítulo se mencionan los aspectos generales sobre el trabajo final de graduación (TFG). El capítulo contiene información sobre Symbiotic, organización donde se realiza el proyecto. Así mismo el documento proporciona un contexto más claro sobre la problematica que posee la organización, así como los desafíos y las oportunidades que se presentan. Por otra parte, se definen los objetivos del TFG y se explican los resultados anticipados y los beneficios que se esperan obtener al finalizar el proyecto.

1.1. Descripción General

La seguridad de la información se ha convertido en una preocupación crucial en el entorno digital actual, donde la tecnología y la interconectividad juegan un papel fundamental tanto en nuestra vida diaria como en el desarrollo de las organizaciones. Las fallas de los sistemas y las aplicaciones representan una amenaza continua porque tienen el potencial de poner en peligro la disponibilidad, la integridad y la confidencialidad de los datos privados.

En este caso, el problema que presenta Symbiotc subyace en la ausencia de un marco de trabajo estándarizado para la de gestión de Vulnerabilidades de Red. A pesar de la adopción de estándares internacionales y la creciente demanda de soluciones seguras, la organización carece de una estrategia estructurada que satisfaga estas demandas.

Otro aspecto para considerar es la falta de conocimiento por parte del personal departamentos en la organización en cuanto a la gestión de Vulnerabilidades de Red. Esta insuficiencia limita la capacidad de los equipos para reconocer y abordar adecuadamente las Vulnerabilidades de Red en sus respectivas áreas de responsabilidad.

Por tanto, el objetivo de este proyecto es abordar esta problematica y ofrecer una propuesta viable para la Estandarización del proceso de gestión de Vulnerabilidades de Red a partir de la metodología de Business Process Management (BPM), de modo que garantice la pronta detección, categorización, priorización, mitigación, evaluación y comunicación de Vulnerabilidades de Red efectivamente y se adhiera a los estándares de la industria internacional.

Mediante este enfoque integral, se busca proporcionar a la organización los procesos necesarios para enfrentar los desafíos de seguridad de manera proactiva, garantizando la protección de la información confidencial de los clientes y fortaleciendo la confianza en sus servicios digitales. Los pasos necesarios para crear un enfoque completo de gestión de Vulnerabilidades de Red se examinarán en las secciones siguientes, incluida la categorización adecuada de la documentación existente, la implementación de protocolos claros y la capacitación del personal en la identificación y mitigación de Vulnerabilidades de Red. Esta solución mejorará la postura de seguridad de la organización, reducirá el riesgo de posibles violaciones de seguridad y garantizará la seguridad de los activos de la empresa y la información confidencial.

1.2. Antecedentes

En el siguiente apartado se brinda una descripción detallada de la organización donde se incluyen las características generales de la empresa, su misión, su visión, valores un esquema del equipo de trabajo del departamento.

1.2.1. Descripción de la organización

Symbiotic es una organización creada por el señor Javier Chacón Rivera, especialista en estrategia empresarial y transformación digital. Los estudios y especializaciones del señor Chacón ayudaron a que naciera alrededor del 2016 la idea de fundar una empresa de tecnología que se encargara principalmente de dar soporte de protección a los diferentes medios de pago, que existen en el mercado actual específicamente el medio de pago contactless. Esto surgió debido a la experiencia con varios proyectos de innovación previos a lo largo de la carrera del señor Chacón. El negocio comenzó como una PYME sin oficina, dedicada a desarrollar aplicaciones móviles para marketing, afirmó Ávila, (comunicación personal, 20 de abril de 2023)

Así mismo el sitio web de la organización y el departamento de *Marketing and Public Relations* de la empresa describen a la organización de la siguiente manera:

> Symbiotic es una empresa que se enfoca en la innovación tecnología a través del desarrollo de soluciones seguras y fáciles de usar, somos un desarrollador de software que transforma, automatiza y simplifica los procesos entre su negocio y sus clientes. Somos una agencia multidisciplinar de diseño y desarrollo digital que busca la excelencia y la innovación. (Symbiotic, 2023)

De esta forma se entiende que la idea del señor Chacón sobre Symbiotic es continuar siendo el pionero y líder en tecnología TapOnPhone en Costa Rica. Tiendo un enfoque en la mejora continua a través de la innovación, para posicionar a la empresa como líder en el suministro de soluciones seguras a entidades instituciones globales, compradores corporativos y empresas de tecnología. Algunas de las actividades que se desarrollan dentro de la organización son las siguientes:

- Software como servicio: la organización se centra en brindar soluciones de Software as a Service con el fin de vender soluciones en donde el software se pone a disposición de los clientes a través de un navegador web, normalmente mediante una suscripción.
- Aseguramiento de la protección y seguridad de la información: Symbiotic busca que en sus aplicaciones Contacless, la seguridad de la información debe ser lo primero. Con el fin de salvaguardar los datos de los usuarios y cumplir con las leyes de privacidad y protección de datos de acuerdo con estándares internacionales y la ley de protección de datos de Costa Rica.

1.2.1.1 Misión

A continuación, se indica la misión de la organización.

"Buscamos apasionadamente mejorar los procesos entre su empresa y sus clientes, a través de soluciones tecnológicas hechas a la medida y con la mejor calidad en el mercado" (Symbiotic, 2023)

1.2.1.2 Visión

A continuación, se define la visión de la organización:

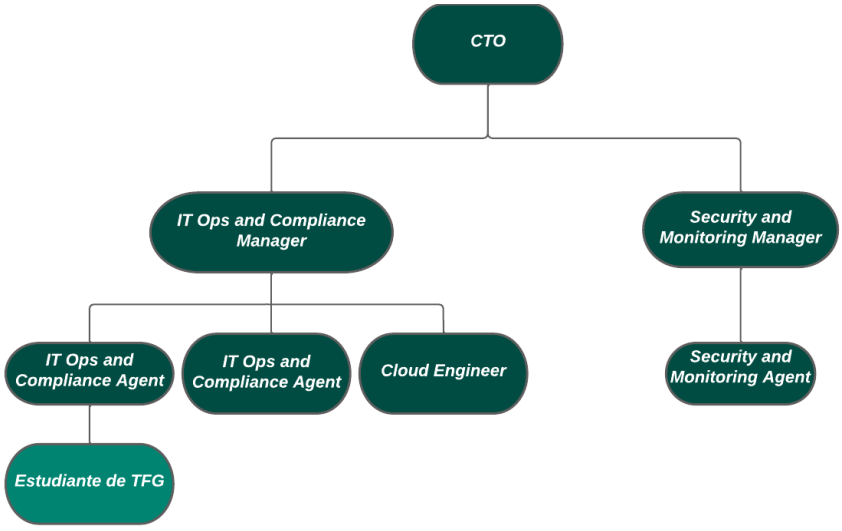
"Seremos reconocidos por nuestros públicos de interés como la desarrolladora de software líder en innovación, transformación y agilidad más importante a nivel mundial." (Symbiotic, 2023)

1.2.1.3 Organización

En este apartado se presenta el equipo de trabajo que ayudará al estudiante a completar el proyecto final de graduación. Este se encuentra conformado por de cinco personas relacionadas al departamento de *IT Ops and Compliance* que posee la organización. El encargado directo del alumno es el jefe de dicho departamento *(IT Ops and Compliance Manager),* además de contar con dos *IT Compliance Agents*, los cuales tienen responsabilidades como conservar y gestionar la infraestructura tecnológica de la empresa, garantizar el cumplimiento de las políticas y normativas de seguridad y privacidad, y aplicar y mantener medidas de seguridad y protección de datos.

El puesto de *IT Ops and Compliance* es el puesto para el estudiante y el *Cloud Engineers* que se encargan de dar soporte en temas relacionados a cumplimiento de la infraestructura de la organización. Así mismo de un *Security and Monitoring Manager* y al de un *Security and Monitoring Agent,* los cuales se encargan de revisar y gestionar los accesos a diferentes recursos y gestionar, revisar y mitigar las alertas de seguridad. En la Figura 1se muestra el grupo encargado de ayudar al alumno del TFG.

Figura 1 Organigrama de la Organización



Fuente: Elaboración propia, 2023.

1.2.2. Trabajos similares realizados dentro y fuera de la organización

En la siguiente sección se definen los proyectos internos y externos que sirven como línea base para tener una mejor comprensión del tema, y que permiten identificar ideas claves para el desarrollo del proyecto en cuestión.

1.2.2.1 Proyectos Internos

Documentación del Plan de Control de Riesgos: este documento según Ávila (comunicación personal, 2023), permite alinear los requisitos de seguridad definidos en la certificación del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago o PCI DSS, requeridos por el departamento de IT Ops and Compliance y el departamento de DevOps deben tener acceso a una guía documentada. Además, este documento define las líneas de acción de los riesgos de código que se encuentren, no obstante, el documento no es integral, no se toman medidas para Vulnerabilidades de Red y más bien sirve de guía rápida para entrenamiento de personal nuevo o para consulta rápida de algún paso del proceso que se tenga en duda dentro de la organización o que se requiera para presentar una prueba de su existencia a clientes o proveedores.

Proyecto de Monitoreo de Vulnerabilidades de Red con la herramienta de IDS de GCP: Este proyecto, es el más reciente de la organización relacionado con el tema de seguridad según Ávila (comunicación personal, 2023). La iniciativa de este proyecto surge debido a la necesidad de monitorear las Vulnerabilidades de Red a los ambientes de la nube que posee la organización para obtener la certificación de PCI DSS. Así mismo, es importante recordar que Google es el proveedor de servicios del sistema de Monitoreo de Symbiotic, lo que permite que dentro de la organización se realicen auditorías semestrales acerca de cumplimiento de los requisitos de PCI DSS sobre el tema de Vulnerabilidades de Red en la infraestructura de la organización. Esto con el fin de planear procedimientos para corregir fallas de procesos o fugas de datos, según sea necesario.

1.2.2.2 Proyectos Externos

En el siguiente apartado permite indicar documentos externos a la organización.

***NIST Special Publication 800-40* :** este documento brinda las instrucciones para desarrollar un programa de administración de parches y Vulnerabilidades de Red para ayudar a las organizaciones a administrar las Vulnerabilidades de Red del software y aplicar parches de manera rápida y eficiente. El presente documento brinda recomendaciones para desarrollar políticas y procedimientos, seleccionar herramientas, realizar campañas de capacitación y concientización, y los pasos necesarios para establecer un programa de administración de parches, como la identificación, priorización, remediación y validación de Vulnerabilidades de Red.

Fortra y su plan de Gestión de Vulnerabilidades de Red: el caso de éxito de Fortra como compañía de ciberseguridad es la creación de su plan de Gestión de Vulnerabilidades de Red el cual tiene como objetivo ayudar a las organizaciones a identificar y remediar las Vulnerabilidades de Red en sus sistemas y aplicaciones. Según el artículo "Tripwire ExpertOps Case Study" realizado por (Tripwire, 2023)afirma que el equipo de operaciones de TI actualizó su Gestión de Vulnerabilidades de Red con Tripwire ExpertOps que Fortra desarrollo y se lograron obtener "una puntuación media del host en los sistemas de la empresa se redujo en un 50 por ciento. El número total de puntuaciones negativas se redujo en aproximadamente un 90 % en el transcurso de 10 meses." (Tripwire, 2023)

Trabajo Final de Graduación Metodología para la gestión de riesgos de TI basada en COBIT 5: Dicho documento desarrollado por (Alfaro, 2017) se enfoca en implementar las mejores prácticas e ideas de vanguardia en la gestión de riesgos de TI mientras se adhiere a los estándares utilizados globalmente por varias organizaciones. El objetivo es hacer posible que Deloitte brinde servicios de gestión de riesgos de TI que se ajusten a las necesidades y tendencias actuales de los clientes. La principal motivación de esta estrategia es estandarizar las actividades involucradas en la gestión de riesgos de tecnología de la información que Deloitte lleva a cabo como parte de sus servicios.

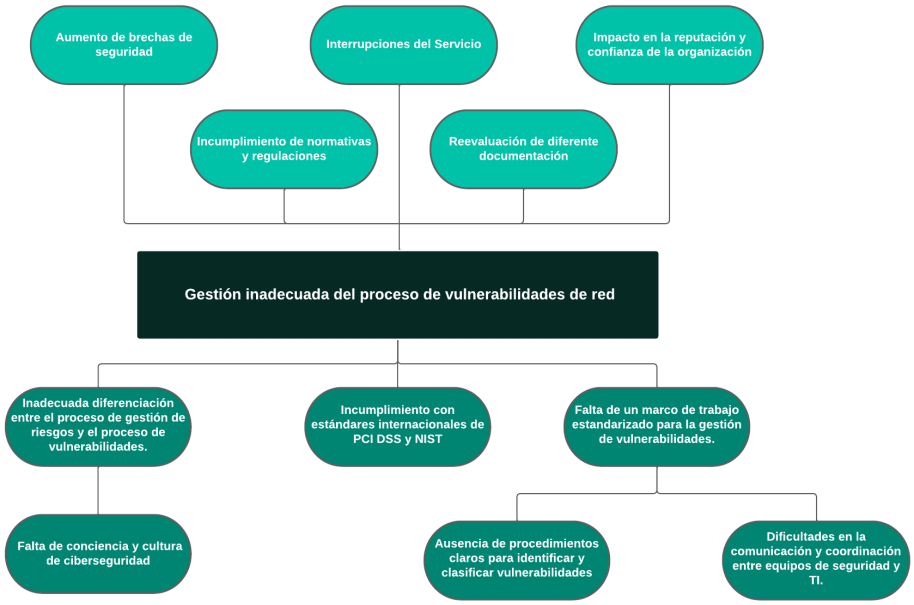
1.3. Planteamiento del problema

Este apartado describe la situación problemática hallada dentro del entorno de la organización elegida. Para esto se incluyen las características generales de la empresa, el esquema de las causas del problema relacionado con las operaciones y una conceptualización de la relevancia del proceso de Vulnerabilidades de Red basada en la comprensión y análisis de los estándares internacionales que la organización debe aplicar a diario, según el nicho de mercado que presta servicios.

1.3.1. Situación problemática

La Figura 2 ilustra mediante un diagrama del problema la situación problemática descrita en la organización.

Figura 2 Árbol del Problema



Fuente: Elaboración propia, 2023.

En el entorno actual de evolución tecnológica y crecientes amenazas cibernéticas, la seguridad de la información se ha convertido en un aspecto a considerar para las organizaciones. En el caso de Symbiotic, se ha identificado la problemática, la Gestión Inadecuada del Proceso de Vulnerabilidades de Red. Este conflicto abarca una serie de causas que contribuyen directamente a la incapacidad de la organización para administrar las Vulnerabilidades de Red de seguridad.

La primera de ellas está relacionada al problema es el incumplimiento y falta de alineación de los estándares internacionales como lo son PCI DSS *(Payment Card Industry Data Security Standard*) y NIST, debido a que Symbiotic no alinea el proceso de gestión de Vulnerabilidades de Red a las prácticas y medidas de seguridad que define la industria que son necesarias para prevenir y detectar Vulnerabilidades de Red.

La no alineación ha generado consecuencias negativas, ya que estas amenazas no son identificadas, clasificadas, priorizadas, mitigadas y evaluadas de manera sistemática, tal como lo exigen las buenas prácticas de la industria.

Esta situación plantea un desafío para Symbiotic, debido la infracción de un programa de gestión de Vulnerabilidades de Red, poniendo en riesgo la confidencialidad y seguridad de la información de los clientes, así como la reputación y la integridad de la organización. La relevancia de mantener un plan para la gestión de Vulnerabilidades de Red la describe (Scarfone K & Souppaya M, 2022)en el *National Institute of Standards and Technology, NIST Special Publication 800-40* , en donde afirma:

> El objetivo de mantener un programa de administración de Vulnerabilidades de Red en las organizaciones conlleva a la protección de los sistemas contra *malware*, amenazas y actualizar programas o software antivirus regularmente. Es obligatorio que todos los componentes del sistema que estén involucrados tengan implementado protocolos de seguridad con el fin de administrar las Vulnerabilidades de Red del sistema de manera proactiva antes que se produzca una explotación. (Scarfone K & Souppaya M, 2022)

La segunda causa en relación con la problemática la describe Ávila en el Apéndice C (comunicación personal, 2023), Symbiotic ha presentado problemas en abordar las amenazas en su infraestructura y sistemas tecnológicos, haciendo que existan posibilidades de brechas de seguridad.

Esto sucede debido a la ausencia de un marco de trabajo estándarizado y claramente definido para la gestión de Vulnerabilidades de Red, razón que ha empujado a Symbiotic a la adopción de procedimientos poco eficaces, lo que complica la tarea de proteger la información de manera integral contra las amenazas de seguridad.

Como tercera causa para considerar se encuentra una inadecuada diferenciación del proceso de gestión de riesgos y el proceso de Vulnerabilidades de Red ya que Ávila (comunicación personal, 2023), afirma que esto lleva la confusión en la identificación y evaluación de los riesgos de seguridad, lo cual conlleva a los responsables de la seguridad en Symbiotic no distingan claramente los enfoques de gestión de riesgos y de Vulnerabilidades de Red.

La diferenciación de los procesos mencionados anteriormente, lo explica (Hallet & Chen, 2021) de la siguiente manera:

> El enfoque del NIST antepone la identificación de amenazas a las Vulnerabilidades de Red, lo que presupone que todas las amenazas al identificarse y asignarse a Vulnerabilidades de Red. Cabe destacar que la evaluación de riesgos también debe ser eficaz en situaciones en las que las amenazas son menos evidentes o aún no están generalizadas y, por lo tanto, algunas organizaciones que están particularmente arraigadas en la adopción digital también considerar la posibilidad de realizar un proceso Vulnerabilidades de Red de forma independiente.

Otra causa del problema descrito anteriormente está relacionada con una serie de consecuencias en la documentación, de manera que resulta necesario revaluar el protocolo actual debido a la inadecuada categorización de Vulnerabilidades de Red. Esta evaluación, permitirá el reconocimiento de brechas del proceso existente contra las buenas prácticas de la industria.

Además, dentro de esta problemática se encuentra el hecho de que los empleados carecen de una comprensión de los riesgos y amenazas de seguridad como resultado de la falta de cultura y conciencia de seguridad cibernética, lo que genera que actúen de manera descuidada o peligrosa en lo que respecta a la seguridad y control de Vulnerabilidades de Red. Ávila (comunicación personal, 2023)

En este contexto, es imprescindible abordar la problemática descrita, desarrollando estrategias efectivas para establecer y mantener la propuesta de un plan gestión de Vulnerabilidades de Red, el cual debe cumplir con las mejores prácticas de la industria de modo que garantiza un marco de trabajo alrededor de las Vulnerabilidades de Red en los ambientes de desarrollo y en los componentes del sistema.

1.3.2. Justificación del proyecto

A continuación, se muestra la razón de ser del estudio al problema expuesto en el apartado anterior que existe en Symbiotic.

Según las causas de la Figura 2, es esencial abordar la dificulta presentada mediante estrategias efectivas que permitan establecer y mantener un Plan de Gestión de Vulnerabilidades de Red. Ante la falta de un marco de referencia el presente proyecto busca plantear un proceso estándarizado, permitiendo solventar las necesidades que fueron encontradas en esta área. Este proceso abarca la adecuada documentación de las actividades relacionadas a las Vulnerabilidades de Red, también brinda la definición de un marco de trabajo con un enfoque práctico. Este énfasis tiene el propósito de ayudar a toda aquella persona responsable de realizar el proceso de gestión en cuestión tener una comprensión sobre los pasos a realizar de una manera adecuada.

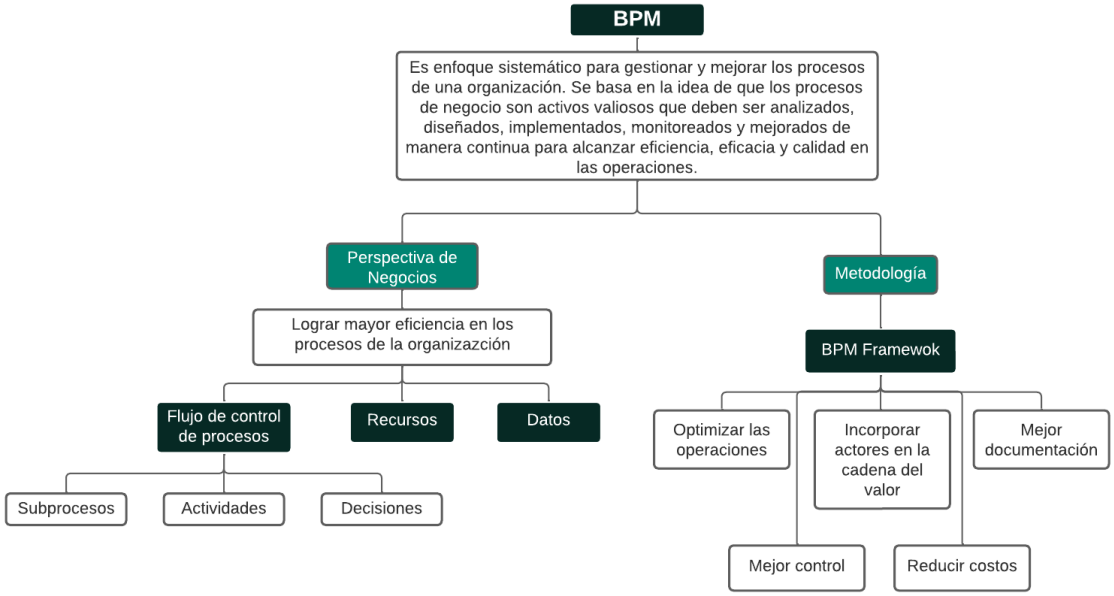
Otro factor que apoya el cumplimiento del proyecto es la idea de expandir el trabajo multidisciplinario en la organización. Según el *CTO y IT Ops and Compliance Manager* de Symbiotic (comunicación personal, 2023), la empresa busca la colaboración del personal de los departamentos *de IT Ops and Compliance* junto con el departamento *DevOps* con el objetivo realizar actividades de seguridad preventivas en equipos multifuncionales, con el fin de afectar directamente la causa de dificultades en la comunicación y coordinación entre equipos de seguridad y TI, descrita en la Figura 2. Tener un plan de gestión que sirva como marco de trabajo también permite que las actividades que se realizan dentro del proceso de Vulnerabilidades de Red sean notificadas de forma efectiva mediante la definición de planes de comunicación.

Una razón que suma para la elaboración del proyecto se encuentra relacionada con el mantenimiento proactivo de la seguridad. Esto gracias, a la posesión de un programa de gestión de Vulnerabilidades de Red, que implica adoptar un enfoque dinámico para la seguridad de una organización. Esto permite evaluar regularmente los sistemas, identificar nuevas Vulnerabilidades de Red, aplicar parches y actualizaciones de seguridad, con el objetivo de mantener un monitoreo constante para detectar amenazas potenciales. Como consecuencia, se le facilita al departamento de *IT Operations and Compliance* de Symbiotic administrar adecuadamente estas Vulnerabilidades de Red, con el finde reducir el riesgo de exponer datos confidenciales. (Ávila, comunicación personal, 2023).

Debido a la naturaleza del proyecto se debe seguir los lineamientos de los estándares internacionales, en vista que la propuesta del Plan de Gestión incluye indicadores para la evaluación periódica del proceso y sus controles de seguridad. Además, se encuentra que un plan de gestión brinda la oportunidad de desarrollar habilidades profesionales relevantes en el campo de la seguridad de la información y la gestión de riesgos.

Desde la perspectiva de los Sistemas de Información (SI), el proyecto se verá respaldado por la metodología BPM definida por Dumas, M. La Rosa, M (2018). La Figura 3 resume la definición, los beneficios y los pasos necesarios para enfatizar la importancia de la administración de procesos de negocio como un dominio perteneciente a Sistemas de Información, y que tiene relación directa con la situación problemática.

Figura 3 Área de estudio de BPM



Fuente: Elaboración propia, 2023.

El uso de la metodología BPM en este proyecto de propuesta del Plan de Gestión de Vulnerabilidades de Red permite la Estandarización y documentación de las actividades que se realizan en este proceso. Al desarrollar el proyecto se busca utilizar un enfoque coherente durante todo el flujo del proceso, desde la identificación de Vulnerabilidades de Red hasta la comunicación. Además, la eficiencia y la calidad en la gestión de la vulnerabilidad se promueven mediante, un adecuado perfilado de las actividades.

Así mismo, el Plan de Gestión de Vulnerabilidades de Red establece un procedimiento estructurado cuyas bases se encuentran en la gestión de procesos de negocio (BPM) para la detección temprana de Vulnerabilidades de Red. Esto permite al departamento de Departamento *de IT Ops and Compliance* de Symbiotic la posibilidad de identificar y evaluar rápidamente las fallas de seguridad para abordar y reducir los riesgos.

De esta forma, el área de estudio seleccionada sobre Administración de Procesos de Negocios (BPM), desempeña un papel importante en el desarrollo del proyecto y en la estrategia global de seguridad de la información de Symbiotic. El objetivo de BPM es mejorar la eficacia y la eficiencia operativa, identificando, documentando y optimizando los procesos empresariales.

Dichas medidas ayudan a mejorar la postura general de seguridad de la organización y garantiza la continuidad de los procesos empresariales críticos que Symbiotic desarrolla. Esta propuesta contribuirá a fortalecer la posición de seguridad de la organización, disminuir la probabilidad de posibles violaciones de seguridad y a salvaguardar la confidencialidad de la información de los clientes y los recursos de Symbiotic.

1.3.3. Beneficios esperados o aportes del Trabajo Final de Graduación

El proyecto de implementar un Plan de Gestión de Vulnerabilidades de Red en el departamento de IT Operations and Compliance de Symbiotic, ofrece una serie de beneficios los cuales serán puntualmente listados según su categoría, ya sean beneficios directos o indirectos.

1.3.3.1 Beneficios Directos

Enseguida se desglosan los beneficios directos de este proyecto para la organización.

- Alineación de los protocolos de seguridad con las buenas prácticas a partir del establecimiento de métricas.
- Definición de un sistema de métricas periódico que se alinee a los diferentes marcos de referencia que define las buenas prácticas de la industria.
- Definición de un marco de trabajo alrededor de la Gestión de Vulnerabilidades de Red.
- Comprensión en la documentación de los procedimientos de gestión de Vulnerabilidades de Red.
- Garantizar que el trabajo final de graduación (TFG) se adhiera al estándar PCI DSS 4.0 implica directamente el cumplimiento de normativas de seguridad críticas para la protección de datos de tarjetas de pago.
- Implementar las directrices de PCI DSS directamente mejora la seguridad de los datos de tarjetas de pago, reduciendo riesgos y fortaleciendo la integridad financiera de la organización.

1.3.3.2 Beneficios Indirectos

En este apartado se indica los beneficios indirectos de la organización.

- Ayuda a mejorar la productividad de administración de las Vulnerabilidades de Red.
- Demostrar un compromiso con la seguridad y la protección de datos sensibles, a las instituciones financieras.
- Abordar de manera proactiva las Vulnerabilidades de Red según las buenas prácticas internacionales.
- Cumplir con estándares como PCI DSS contribuye a construir la confianza del cliente, mejorando la reputación y fidelidad hacia la empresa.
- La implementación de PCI DSS induce prácticas de desarrollo más sólidas y una cultura organizacional centrada en la seguridad, mejorando la calidad global de proyectos y operaciones.

1.4. Objetivos del Trabajo Final de Graduación

En el presente apartado se establece el objetivo general y los objetivos específicos del proyecto.

1.4.1. Objetivo general

Proponer un Plan de Gestión de Vulnerabilidades de Red para la definición de un marco de trabajo que aborde las actividades de su ciclo de vida que se administran en el departamento de *IT Operations and Compliance* de Symbiotic, a partir del uso de las buenas prácticas de la industria.

1.4.2. Objetivos específicos

- Analizar la situación actual de la gestión de Vulnerabilidades de Red para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria.
- Diseñar un marco de trabajo de la Gestión de Vulnerabilidades de Red para la Estandarización de las actividades de su ciclo de vida basado en las buenas prácticas internacionales.
- Definir indicadores de desempeño (KPI) para la medición del rendimiento del proceso de gestión de Vulnerabilidades de Red en términos de las fases de su ciclo de vida.

1.5. Alcance

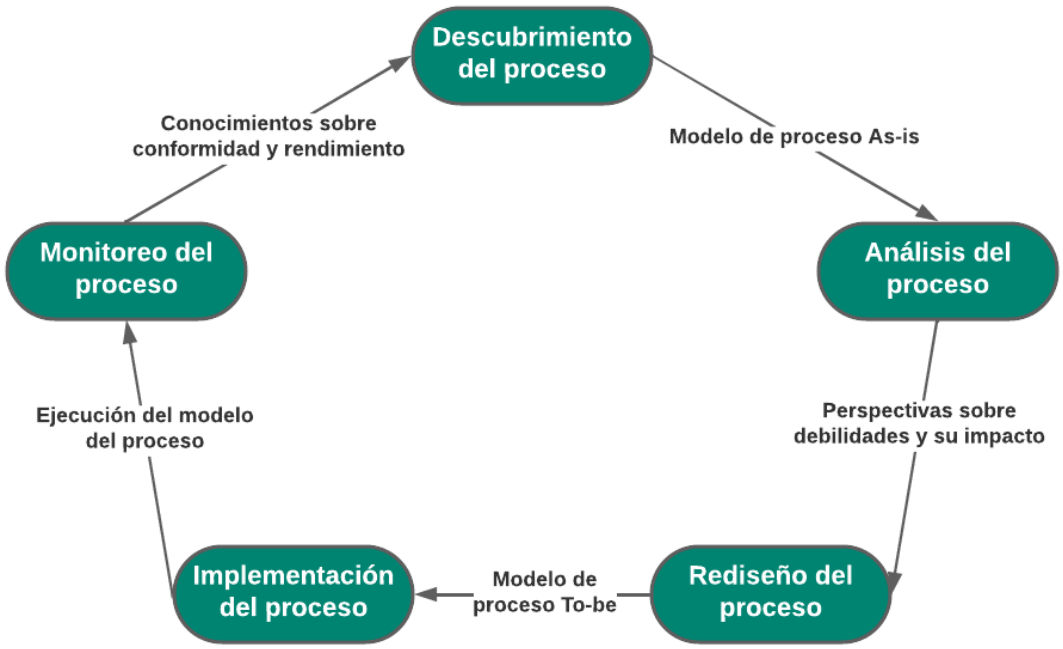
En esta sección se definen los parámetros y procedimientos necesarios para el desarrollo de este proyecto dentro del con el marco de referencia de BPM descrito por Dumas, M. La Rosa, M (2018), en su libro *Fundamentals of Business Process Management.*

El objetivo general del proyecto es introducir y proporcionar una metodología para la gestión de Vulnerabilidades de Red a Symbiotic, que promueva la alineación de los procesos con el estándar de la industria, a partir de la metodología de BPM y así establecer un proceso sistemático y organizado, asegurando la rentabilidad y viabilidad y el éxito de la gestión de recursos en todos los sectores relacionados a esta práctica en Symbiotic.

El alcance del proyecto se centra en el cumplimiento del plan de gestión de vulnerabilidades de red conforme a los estándares de PCI DSS. La iniciativa tiene como objetivo principal asegurar la seguridad de los datos de tarjetas de pago, identificando y abordando posibles debilidades en la infraestructura de red.

Así mismo, alcance se determinará con base en los entregables, la participación de los actores identificados para cada área del proyecto, el nivel de influencia y autoridad asignado a cada uno de ellos, así como la información que comprende los activos del proceso con el fin de determinar los requisitos y funciones clave necesarios para completar el plan. Para esto se utilizará la Figura 4, en donde se muestran las etapas que se plantean desarrollar para el anteproyecto.

Figura 4 Ciclo de Vida BPM



Fuente: Adaptado de Dumas, M. La Rosa, M (2018) *Fundamentals of Business Process Management*, pág. 51.

A continuación, en la Figura 4, referente al Anexo I se detallan las etapas del proyecto que se buscan abarcar para presentar la solución al problema descrito en sesiones anteriores:

Descubrimiento del proceso: en esta etapa se identifica y define el proceso de negocio que necesita ser mejorado, para cuyo desarrollo se pone en práctica el Proceso de Gestión de Vulnerabilidades de Red. Además, en esta etapa se realiza un análisis exhaustivo de los subprocesos y actividades actuales junto con el establecimiento de metas para especificar los flujos de trabajo, tareas y normativas.

Modelado del proceso: la etapa de modelado de procesos se centra en la creación de representaciones visuales del Proceso de Gestión de Vulnerabilidades de Red utilizando la notación de *Business Process Management Notation* (BPMN). Estos modelos ofrecen una visión clara y normalizada del flujo de actividades, las funciones y responsabilidades de los participantes que desarrollan el proceso. De este modo, se busca ejecutar el modelo "As is" y contrastarlo con el modelo "To be".

Análisis del proceso: en esta etapa, se realizan los estudios correspondientes al Proceso de Gestión de Vulnerabilidades de Red. Estos análisis ayudan a comprender cómo funciona el proceso, cómo se mueve la información y cómo cooperan los diversos actores involucrados.

Rediseño del proceso: tomando como base la etapa de análisis del proceso, esta fase consiste en implementar las mejoras encontradas al Proceso de Gestión de Vulnerabilidad. Estas mejoras buscan el rediseño de roles y responsabilidades, la redefinición del orden de los procesos, la reasignación de tareas; así mismo, evaluar los costos (dentro de un análisis costo-beneficio), asignar recursos y determinar los tiempos necesarios para cada una de estas acciones.

Ejecución del proceso: en esta etapa, se especializa por la puesta en ejecución el plan de gestión Vulnerabilidades de Red propuesto y el inicio del proceso de gestión de Vulnerabilidades de Red.

Seguimiento del proceso: El seguimiento continuo se realiza mientras se lleva a cabo el proceso para asegurarse de que todas las etapas y actividades se completen correctamente y en el plazo previsto. El desempeño del proceso de gestión de Vulnerabilidades de Red se medirá mediante un conjunto de métricas y KPI.

1.6. Supuestos

A continuación, se especifican los elementos, que se asume que se cumplirán o serán veredictos en la realización del proyecto.

- El proyecto se llevará a cabo bajo un constante monitoreo de los avances por parte del responsable directo de la organización y del responsable académico.
- Se cuenta con la ayuda y disponibilidad del personal de los departamentos de Compliance y DevOps.
- Se tendrá acceso a la información existente en la base de conocimiento de la organización a menos que sea requerido algún tipo de permiso o supervisión bajo el responsable directo de la empresa.

1.7. Entregables

En el siguiente apartado se describen los entregables que tendrá el proyecto, tomando en cuenta los entregables de gestión del proyecto y los entregables del producto solicitados por Symbiotic.

1.7.1. Entregables de Producto

El propósito de esta sección es definir todos los documentos y entregables que se encuentran asociados a cada objetivo del proyecto. Esta información se ilustra en Tabla 1 en donde cada columna define el objetivo, el entregable y la descripción del entregable del producto para el presente proyecto.

Tabla 1 Entregables del Producto

Objetivos específicos	Entregable	Descripción del entregable producto
Analizar la situación actual de la gestión de Vulnerabilidades de Red para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria.	Informe de la situación actual. Análisis de Brecha.	Este informe debe proporcionar un panorama completo de la gestión de Vulnerabilidades de Red en el departamento de IT Operations and Compliance de Symbiotic. Debe incluir una descripción detallada del proceso actual, con la descripción de las fortalezas y debilidades de este. El informe debe destacar las áreas que requieren mejoras y proponer recomendaciones para optimizar la gestión de Vulnerabilidades de Red.

Objetivos específicos	Entregable	Descripción del entregable producto
	Modelado de procesos As Is.	Estos modelos permiten entender el proceso vigente tal cual se ejecuta. El entregable hará que sea más fácil demostrar las actividades en las que el departamento de Cumplimiento y operaciones de TI de Symbiotic sobresale y en las que debe mejorar.
Diseñar un marco de trabajo de la Gestión de Vulnerabilidades de Red para la Estandarización de las actividades de su ciclo de vida basado en las buenas prácticas internacionales.	Plan de Gestión de Vulnerabilidades de Red • Política de Gestión de Vulnerabilidades de Red. • Plan de Comunicación de Gestión de Vulnerabilidades de Red. • Material de Entrenamiento para el Personal. • Documentación de los procedimientos.	Este entregable corresponde a toda la documentación referente a la normativa interna de Symbiotic, planes de comunicación y entrenamiento, cuyo objetivo consiste en reducir el riesgo de ataques cibernéticos y garantizar la continuidad del negocio mediante la implementación de un plan eficaz de gestión de Vulnerabilidades de Red que identifique, categorice, mitigue y evalúe las Vulnerabilidades de Red de manera rápida y eficaz.
Definir indicadores de desempeño (KPI) para la medición del rendimiento del proceso de gestión de Vulnerabilidades de Red en términos de las fases de su ciclo de vida.	Catálogo de indicadores	Con respecto a las diversas facetas del proceso de gestión de Vulnerabilidades de Red, este entregable tiene como objetivo crear un catálogo de indicadores. Estos indicadores deben estar en línea con las metas del proceso para la gestión de la vulnerabilidad. Cada indicador, su método de cálculo, la fuente de datos requerida y la frecuencia de medición se describen claramente en el catálogo.

Fuente: Elaboración propia, 2023.

1.7.2. Entregables Académicos

En esta sección se describen los artefactos asociados a los entregables académicos del proyecto, con el fin de optar por una Licenciatura en Administración de Tecnologías de Información. Los resultados académicos que se desarrollan son los siguientes:

- Capítulo 1 Introducción.
- Capítulo 2: Marco conceptual.
- Capítulo 3. Marco metodológico.
- Capítulo 4: Análisis de Resultados.
- Capítulo 5: Soluciones sugeridas.
- Capítulo 6: Conclusiones y recomendaciones.

1.8. Limitaciones

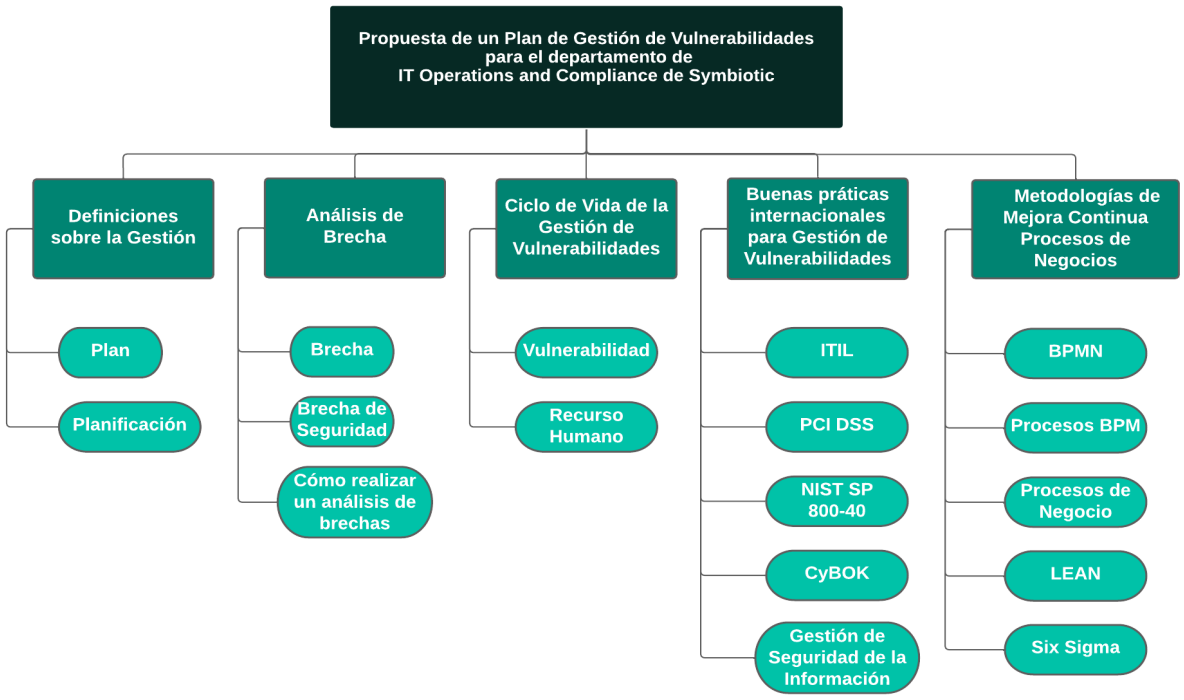
El siguiente apartado se indican los factores que tienen la potencial de restringir la realización del proyecto.

- El proyecto se enfoca exclusivamente en el análisis del proceso de vulnerabilidades de red gestionadas en Symbiotic.
- Las áreas de prioridad para el análisis y desarrollo del proyecto se basan en los departamentos de Compliance y DevOps otros departamentos de la organización no serán tomados en cuenta.
- La recolección de información del personal los departamentos mencionados anteriormente deben ser accedida en la base de conocimientos de la organización. Para esto se debe trabajar con solicitudes de acceso dependiendo del rol o responsabilidad.
- No se contempla cualquier ente terciario que no tenga intervención directa con el proceso seleccionado.
- Se deben tomar en cuenta los lineamientos establecidos por el requerimiento 6 del estándar de PCI DSS, Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard), en su versión más actualizada 4.0.
- La Gerencia General solicitó que este proyecto, no tenga la información sensible y cualquier otro tipo de información que expone datos relevantes a las operaciones de forma anónima.

2. Marco Conceptual

En el siguiente capitulo se describen las bases teóricas y conceptuales relevantes para la realización del proyecto. De igual modo, se busca que dichas definiciones y conceptos sirvan para brindar objetividad y respaldar el presente documento. Por ende, a partir de la Figura 5 este capítulo explora los estándares internacionales, así como los marcos de referencia de trabajo como lo son ITIL, NIST Special Publication 800-40, PCI DSS, CyBOK.

Figura 5 Árbol de conceptos



Fuente: Elaboración propia, 2023.

El capítulo también busca explorar todos aquellos elementos y aspectos que permiten entender de la gestión de Vulnerabilidades de Red, metodologías de mejora continua de procesos, estrategias de abarcar las Vulnerabilidades de Red, los procesos, las herramientas y el recurso humano como se detallan en la Figura 5.

2.1. Definiciones sobre la Gestión

Este apartado se encarga de contextualizar las definiciones relacionadas con el tema.

2.1.1. Plan

El primer punto por tratar es la definición de un plan que la (Real Academia Española, 2023c) la contextualiza de la siguiente manera "Escrito en que sumariamente se precisan los detalles para realizar una obra.", también la describe como "Modelo sistemático de una actuación pública o privada, que se elabora anticipadamente para dirigirla y encauzarla". De este modo se entiende que un plan es un mecanismo sistemático que define una serie de pautas para lograr una tarea o actividad tiendo en cuenta los detalles para realizarla.

Las definiciones anteriores, se centran en la gestión de los detalles. En este punto es donde surge el segundo concepto de relevancia del proyecto el cual es la gestión. Dicho termino la (Real Academia Española, 2023b) lo define como: "Acción y efecto de administrar". Con esta definición se explora que la actividad de gestionar conlleva coordinar y supervisar diversos movimientos con el propósito de alcanzar resultados deseados, ya sea en el ámbito empresarial, organizacional o en cualquier otro contexto.

La labor de gestionar descrita conlleva una consecuencia mucho más amplia que abarca tomar decisiones estratégicas, asignar los recursos de manera adecuada, delegar responsabilidades, vigilar el progreso y realizar ajustes según sea necesario para lograr con éxito el cumplimiento de objetivos y proyectos establecidos.

2.1.2. Planificación

Continuando con el desarrollo de este capítulo se considera importante el concepto de planificar, para esto se utilizará la definición brindada por (Gartner, 2023)

> La "estrategia" crea un entendimiento común de lo que la empresa quiere conseguir y qué tiene que hacer para lograrlo. Los planes tienen y especifican las acciones sistemáticas que se deben seguir para alcanzar un objetivo. (Gartner, 2023b)

Esta delimitación deja en claro que la planificación es más que un conjunto de herramientas que ayudan a establecer una línea base para guiar la toma de decisiones en las organizaciones, evaluar el progreso y ajustar los enfoques en el camino. Estas herramientas también se utilizan para evaluar los indicadores que utilizará la organización. El análisis de estos indicadores es fundamental para diseñar el Plan de Gestión de Vulnerabilidades de Red por desarrollar en Symbiotic.

Con el objetivo de desarrollar adecuadamente el Plan de Gestión de Vulnerabilidades de Red, se pretende realizar un análisis de su situación actual desde una perspectiva tanto empresarial como de procesos y una adecuada y pertinente planificación. Al hacer esto, será posible establecer metas que mejoren la situación actual a partir de la identificación de las fortalezas y debilidades del proceso existente.

2.2. Análisis de Brecha

El concepto de análisis de brecha según (Weller, 2018) lo encuentra explicado en su artículo "Guía completa para el análisis de brecha" de la siguiente manera:

> Un análisis de brechas permite evaluar los resultados reales frente a los esperados para identificar estrategias, procesos, tecnologías o habilidades deficientes o faltantes. Utilice los resultados de un análisis de brechas para recomendar acciones que la empresa debe poner en práctica para alcanzar sus objetivos. (Weller, 2018)

El análisis de brechas proporciona una imagen realista de las deficiencias de seguridad existentes en el sistema. Sin esta evaluación, sería difícil identificar de manera efectiva las áreas específicas donde se necesita acción para cerrar la brecha entre actual y la deseada.

2.2.1. Brecha

La (Real Academia Española, 2023a) contextualiza el termino brecha de la siguiente manera: "Diferencia o distancia entre situaciones, cosas o grupos de personas, especialmente por la falta de unión o cohesión." De la misma manera, explica que una brecha se considera como: "Resquicio por donde algo empieza a perder su seguridad" o como "Rotura o abertura irregular".

De las tres definiciones brindadas por la (Real Academia Española, 2023a) se utiliza la primera, debido a que una brecha en el contexto del presente trabajo se refiere a la diferencia o distancia entre el estado actual y el nivel deseado. Tales brechas representan debilidades o deficiencias en los procesos, infraestructura o los sistemas de la organización que deben abordarse y corregirse.

2.2.2. Brecha de Seguridad

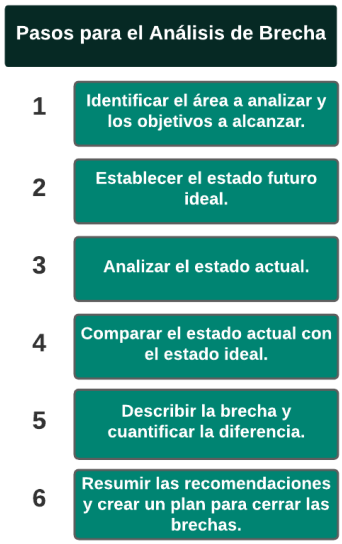
El (Instituto Nacional de Ciberseguridad de España, 2020, p. 23) explican que una brecha de seguridad es:

> Violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos. Las brechas de seguridad también afectan a la comunicación o acceso no autorizados a dichos datos.

2.2.3. Pasos para realizar un análisis de brecha

El análisis de brechas proporciona una base objetiva para la toma de decisiones y la priorización de un programa de gestión de Vulnerabilidades de Red. Esto ayuda a determinar qué aspectos de seguridad deben mejorarse primero y cuáles requieren más atención. La Figura 6 permite mostrar los pasos necesarios a considerar para la realizar un análisis de brecha.

Figura 6 Pasos del Análisis de Brechas



Fuente: Adaptado de (Weller, 2018)

A continuación, se detallan los pasos para realizar un análisis de brecha:

Identificar el área por analizar y los objetivos por alcanzar. en esta etapa primero se debe definir claramente qué aspectos, (áreas del proceso de gestión de Vulnerabilidades de Red) se desean analizar y segundo establecer los objetivos específicos que se pretenden lograr al final del análisis.

Establecer el estado futuro ideal: esta etapa busca definir cuál sería el estado idílico oportuno (*To Be*) como resultado del proceso de gestión de Vulnerabilidades de Red si se ejecutara correctamente.

Analizar el estado actual: se debe realizar una evaluación integral del estado actual del proceso de gestión de Vulnerabilidades de Red. Revisar cómo se descubren, priorizan y remedian las Vulnerabilidades de Red y la eficiencia general del proceso. Además, se debe analizar los procedimientos, la tecnología utilizada y la formación del personal implicado.

Comparar el estado actual con el estado ideal: esta etapa busca comparar las inconsistencias, áreas donde el proceso actual no cumple con los estándares deseados y posibles debilidades.

Describir la brecha y cuantificar la diferencia: aquí se detallan las áreas específicas en las que el proceso actual de gestión de Vulnerabilidades de Red no cumple con los estándares esperados. Si es posible, determina la diferencia.

Resumir las recomendaciones y crear un plan para cerrar las brechas: con base en el análisis, se compilan recomendaciones específicas para eliminar las deficiencias identificadas.

2.3. Análisis de valor añadido

Según los autores (Dumas et al., 2018, p. 213) el análisis de valor añadido consiste en:

> El análisis del valor añadido es una técnica para identificar los pasos innecesarios de un proceso con vistas a eliminarlos. con vistas a su eliminación. En este contexto, una etapa puede ser una tarea del proceso o parte de una tarea. de una tarea. A menudo, una tarea implica varios pasos. (Dumas et al., 2018, p. 213)

Según la descripción anterior, se entiende que el análisis de valor agregado es una metodología para determinar y evaluar las acciones en un proceso o sistema que, a los ojos del cliente, realmente aumentan el valor del bien o servicio terminado. Implica separar las tareas que se consideran inútiles o no esenciales de las que sí lo son.

Los autores (Dumas et al., 2018, p. 215) explican que existen tres categorías para la clasificación de las actividades, según el valor que aportan:

La primera categoría es el valor añadido (VA) son actividades o pasos que produce valor o satisfacción al cliente. Así mismo señalan una serie de preguntas las cuales se realizan para de determinar si un paso es o no VA.

- ¿Estaría dispuesto el cliente a pagar por este paso?
- ¿Valora el cliente este paso lo suficiente como para seguir haciendo negocios con nosotros?
- Y a la inversa, si eliminamos este paso, ¿percibiría el cliente que el resultado del proceso es menos valioso?

La segunda categoría es el valor añadido empresarial (VAB). Los autores Dumas et al., (2018) señalan que la actividad o el paso es necesario o útil para que la empresa funcione sin problemas, para recaudar ingresos o debido al entorno normativo de la empresa. El siguiente listado de preguntas resulta útil a la hora de determinar si una etapa ofrece valor añadido empresarial:

- ¿Es necesaria esta medida para obtener ingresos, mejorar o hacer crecer la empresa?
- ¿Sufriría (potencialmente) la empresa a largo plazo si se suprimiera esta medida?
- ¿Reduce el riesgo de pérdidas empresariales?
- ¿Es necesaria para cumplir los requisitos normativos?

La tercera categoría responde a las actividades sin valor añadido (NVA). Los autores (Dumas et al., 2018) describen estas tareas como pasos que no entra en ninguna de las otras dos categorías, por ende, no generan valor al proceso.

2.4. Análisis de desperdicios

De acuerdo con lo explicado en el libro *"Fundamentals of Business Process Management"* (Dumas et al., 2018) señalan que este análisis consiste en:

> El análisis de residuos adopta el ángulo inverso del análisis de valor añadido. Este análisis trata de encontrar residuos en todo el proceso. Algunos de estos residuos se atribuyen a pasos concretos del proceso, pero otros, como veremos, están ocultos entre los pasos o a veces en todo el proceso. (Dumas et al., 2018)

Según la descripción brindada por (Dumas et al., 2018) el análisis de desperdicio se refiere a la identificación y eliminación de actividades, procesos o recursos que no agregan valor a un producto o servicio desde la perspectiva del cliente. Así mismo, (Goldsby & Martichenko, 2005) explican que dicho análisis se fundamenta en la identificación de diversas formas de desperdicio, típicamente categorizadas en grupos como los "7 tipos de desperdicio" en *Lean Manufacturing*, y que se engloban en tres categorías mayores: movimiento, esperar y exceso:

El movimiento, se refiere residuos relacionados con el movimiento. Esta categoría incluye dos tipos de residuos: transporte y movimiento, los cuales (Goldsby & Martichenko, 2005) describen de la siguiente manera:

- Transporte innecesario: movimiento innecesario de productos o materiales.
- Movimiento excesivo del operario: movimientos adicionales o innecesarios del personal para completar una tarea.

La segunda categoría engloba los residuos derivados de esperar alguna otra acción. Los autores (Dumas et al., 2018) señalan que esta categoría incluye dos tipos de residuos: inventario y espera.

- Tiempo de espera: tiempo en el que los recursos no están en uso debido a retrasos o inactividad.
- Inventario en exceso: mantener inventario innecesario que ocupa espacio y recursos.

La última categoría está relacionada con el exceso. Son desperdicios derivados de hacer más de lo necesario para aportar valor a la empresa o al cliente. (Goldsby & Martichenko, 2005) explican que esta categoría engloba tres tipos de residuos: defectos, sobre procesamiento y sobreproducción, los cuales son descritos a continuación:

- Sobreproducción: generar antes de lo requerido o en exceso de lo requerido.
- Los errores o productos defectuosos que deben repararse o reelaborarse se denominan "defectos".
- Hacer más trabajo o procesamiento del necesario se conoce como "sobre-procesamiento".

2.5. Análisis de flujo: ciclo de tiempo vs. eficiencia del proceso

Para explicar el análisis de flujo se usan las definiciones brindadas en el libro *"Fundamentals of Business Process Management"*, en el cual (Dumas et al., 2018) señalan que este estudio está conformado por dos perspectivas la primera aborda el ciclo de tiempo del proceso y la segunda se enfoca en la eficacia del proceso.

La primera perspectiva sobre el cálculo del ciclo de tiempo del proceso se explica de la siguiente manera:

> Es el tiempo medio que transcurre entre el momento en que se inicia y el momento en que finaliza. Por extensión, decimos que el tiempo de ciclo de una tarea es el tiempo medio que transcurre entre el momento en que la tarea y el momento en que finaliza. (Dumas et al., 2018, p. 256)

El texto proporciona una base sólida para comprender y medir el tiempo requerido para completar actividades, esto es esencial en la gestión eficiente de procesos y la mejora continua. Para el cálculo del ciclo de vida se utiliza la formula descrita por (Dumas et al., 2018, p. 258)

$$Tiempo\ de\ Ciclo\ Total = Tiempo\ total\ de\ procesamiento + Tiempo\ total\ de\ espera$$

La segunda perspectiva se relaciona con la efectividad del proceso y las consideraciones para calcular dicha efectividad.

> Dumas et al., (2018) explican que el tiempo de ciclo de una tarea o de un proceso tiene la capacidad de dividirse en tiempo de espera y tiempo de procesamiento. El tiempo de espera es la parte del tiempo de ciclo en la que no se realiza ningún trabajo para hacer avanzar el proceso. trabajo para hacer avanzar el proceso. El tiempo de procesamiento, por su parte, se refiere el tiempo que los participantes dedican al trabajo real.

El análisis de flujo posibilita la comparación entre el ciclo de tiempo y la eficiencia del proceso de las actividades ejecutadas en el proceso de estudio. Además, se establecen los intervalos temporales por emplear para los cálculos. Estos intervalos permiten identificar el Tiempo Mínimo de Ejecución (Tm), el Tiempo Máximo de Ejecución (TM), y el Tiempo Promedio (TP). Para el cálculo de la efectividad del proceso se utiliza la fórmula que brinda (Dumas et al., 2018, p. 262)

$$Eficiencia\ del\ proceso = \frac{Tiempo\ total\ de\ procesamiento}{Tiempo\ de\ Ciclo\ Total}$$

2.6. Ciclo de Vida de Gestión de Vulnerabilidades

La Figura 7 permite visualizar las etapas del ciclo de vida de las Vulnerabilidades y cómo estas se gestionan.

Figura 7 Ciclo de Vida de Gestión de Vulnerabilidades de Red

Fuente: Adaptado de (Shobhit, 2020).

A continuación, se describen cada una de las actividades descritas por (Shobhit, 2020)

Fase de descubrimiento: aquí se realiza la detección proactiva de vulnerabilidades. Este paso inicial es indispensable para sentar las bases para una gestión eficaz de la vulnerabilidad. El punto de partida es identificar cualquier vulnerabilidad en el entorno lo antes posible para que pueda remediarse por completo a lo largo del ciclo.

Fase de Organización: tan vital como el descubrimiento de vulnerabilidades, esta fase busca involucrar el uso de etiquetas de activos, mantener registros, gestionar informes de incidentes y establecer una base de datos con información recurrente relevante. Esta estructura permite un enfoque más preciso en la identificación de Vulnerabilidades de Red y promueve una gestión más organizada y eficiente de los activos y procesos involucrados.

Fase de evaluación: el objetivo principal de la fase de evaluación es evaluar el impacto potencial de las vulnerabilidades identificadas y organizadas en la empresa. Esta evaluación incluye mediciones de qué procesos o funciones llegan a verse afectados negativamente por estas Vulnerabilidades de Red.

Etapa de informes. la responsabilidad de remediar las vulnerabilidades o incidentes identificados recae en el equipo de seguridad. El informe resultante ayuda a las organizaciones a comprender las implicaciones de las vulnerabilidades identificadas. Este abordaje permite desarrollar estrategias y planes para abordar estos problemas en el futuro.

Fase de remediación: la corrección de vulnerabilidades es un proceso integral que implica reparar fallas de seguridad descubiertas en una red. Esta etapa consta de varias fases, que incluyen la identificación, priorización e implementación de acciones correctivas. La solución se enfoca no solo en eliminar vulnerabilidades, sino también en implementar medidas preventivas para evitar futuros incidentes. Este enfoque integral garantiza una reparación de vulnerabilidades de exitosa y continua.

Fase de validación: La fase de prueba es fundamental para garantizar que las vulnerabilidades se remedien de manera efectiva y no representen una amenaza constante. Esta fase implica pruebas y evaluación para verificar que las medidas de mitigación implementadas estén reduciendo el riesgo con éxito. La validación garantiza que las organizaciones confíen en que las amenazas se han mitigado o contenido adecuadamente.

Shobhit, (2020) analiza la gestión de Vulnerabilidades de Red hace hincapié en el ciclo de vida de la gestión de vulnerabilidades. Dicha gestión se enfoca en identificar, evaluar y mitigar las amenazas en sistemas, aplicaciones y redes. Además, la autora enfatiza la importancia de organizar y evaluar el impacto de las Vulnerabilidades de Red en la organización.

2.6.1. Vulnerabilidad

La (Real Academia Española, 2023d) define vulnerabilidad como: “Cualidad de vulnerable”. Dicha definición no abarca mucho en contextos como la tecnología o la seguridad informática, por ende, el concepto se definirá según los marcos de referencia descritos con anterioridad.

De acuerdo con (Scarfone K & Souppaya M, 2022) en NIST Special Publication 800-40, una vulnerabilidad es “Un fallo en el diseño o la configuración del software que tiene implicaciones de seguridad. A diversas organizaciones mantienen bases de datos de Vulnerabilidades de Red de acceso público.”

Así mismo, PCI Security Standards Council, (2022, p356) afirma que la vulnerabilidad generalmente se refiere a “debilidades o fallas en sistemas, redes o aplicaciones que podrían ser explotadas por actores maliciosos para obtener acceso no autorizado a datos de titulares de tarjetas o comprometer la seguridad de las transacciones con tarjetas de pago.” El estándar enfatiza la importancia de identificar, priorizar y abordar las Vulnerabilidades de Red de manera oportuna mediante evaluaciones regulares de Vulnerabilidades de Red y pruebas de penetración.

En el marco de referencia de Information Technology Infrastructure Library (ITIL), este no contempla el concepto de vulnerabilidad, pero si aborda el concepto de gestión de Vulnerabilidades de Red como parte de su orientación sobre la gestión de servicios de tecnologías de la información. En el contexto del ITIL según (AXELOS, 2019) la vulnerabilidad generalmente se refiere a

> Debilidades o brechas en sistemas, redes o aplicaciones de tecnologías de la información que podrían ser aprovechadas por personas no autorizadas o ciber atacantes.

> Estas Vulnerabilidades de Red podrían llevar a posibles violaciones de seguridad, filtraciones de datos, interrupciones de servicios u otros impactos negativos en los servicios de tecnologías de la información y las operaciones comerciales. (AXELOS, 2019, p. 253)

Gracias a las definiciones anteriores sobre el termino de vulnerabilidad, se establece para este trabajo que el termino de vulnerabilidad se refiere a la debilidad, fragilidad o susceptibilidad de un sistema, individuo, grupo o entidad a ser afectado, dañado o explotado por factores externos o internos. En diversos contextos, existe la posibilidad de referirse a la susceptibilidad de una computadora o sistema informático a ser atacada o comprometida, la fragilidad emocional o física de una persona ante ciertas situaciones, o la exposición de un grupo social a riesgos y peligros.

En el ámbito de la tecnología y la seguridad informática, se destaca la importancia de gestionar y mitigar proactivamente las Vulnerabilidades de Red mediante diversas prácticas, como evaluaciones regulares de riesgos, controles de seguridad, gestión de accesos y procedimientos de respuesta a incidentes. Al abordar las Vulnerabilidades de Red de manera efectiva, las organizaciones mejoran la seguridad y confiabilidad general de sus servicios de tecnologías de la información, reduciendo los posibles riesgos y garantizando la continuidad de las operaciones comerciales.

2.6.2. Recurso Humano

Para (Whitman & Mattord, 2018) el recurso humano:

> Juega un papel crítico en el contexto de la gestión de Vulnerabilidades de Red, ya que son los profesionales de seguridad de la información y el equipo de TI quienes deben implementar y supervisar las prácticas de gestión de Vulnerabilidades de Red para proteger los sistemas y datos de una organización. Su experiencia y conocimientos son fundamentales para identificar y mitigar las Vulnerabilidades de Red en la infraestructura de TI y mantener un entorno seguro.

Gracias a la definición anterior se entiende que los recursos humanos son esenciales para garantizar una colaboración y comunicación efectivas entre los diferentes equipos que se encuentran dentro de la organización, como el de seguridad de la información, el de TI y otros departamentos relevantes. La colaboración entre estos equipos es fundamental para abordar adecuadamente las Vulnerabilidades de Red y tomar medidas correctivas oportunas.

En el proceso de gestión de Vulnerabilidades de Red, el equipo encargado de la seguridad de la información debe llevar a cabo diversas acciones, algunas de las cuales que se presentan en este proceso de gestión:

- Llevar a cabo escaneos periódicos de Vulnerabilidades de Red mediante el uso de herramientas de seguridad, con el propósito de analizar los resultados obtenidos para identificar posibles puntos débiles en la infraestructura.

- Realizar un análisis y priorización de las Vulnerabilidades de Red detectadas, con el objetivo de determinar su gravedad y el riesgo potencial que podrían representar para la organización.
- Implementar parches y soluciones adecuadas para corregir las Vulnerabilidades de Red identificadas, con el fin de reducir los riesgos de posibles ataques o explotaciones.
- Ejecutar pruebas de penetración y auditorías para evaluar la efectividad de las medidas de seguridad implementadas, así como para detectar las posibles brechas de seguridad que puedan existir.
- Llevar a cabo un monitoreo constante de la infraestructura de TI, con el propósito de identificar nuevas Vulnerabilidades de Red que puedan surgir y estar al tanto de cualquier cambio que afecte la seguridad del sistema.

En conjunto, estas acciones aseguran que el proceso de gestión de Vulnerabilidades de Red se lleve a cabo de manera efectiva, minimizando los riesgos y protegiendo la infraestructura y datos de la organización de posibles amenazas de seguridad.

2.7. Buenas prácticas internacionales

2.7.1. PCI DSS

(PCI Security Standards Council, 2022, p. 4) afirma que el PCI DSS (*Payment Card Industry Data Security Standard*) "es un conjunto de estándares de seguridad de la información establecido por la industria de tarjetas de pago para proteger los datos de tarjetas de crédito y débito y garantizar la seguridad de las transacciones electrónicas. Su objetivo principal es prevenir el robo o la exposición de datos confidenciales de tarjetas y salvaguardar la integridad de los sistemas de pago."

Para la realización del presente proyecto el uso del estándar permite entender las acciones necesarias para implementar medidas de seguridad que aborden varias áreas, incluida la gestión de Vulnerabilidades de Red. La regulación requiere que la empresa donde se desarrolla el trabajo realice periódicamente evaluaciones de vulnerabilidad en sus sistemas y aplicaciones, utilizando herramientas como escáneres de vulnerabilidad y pruebas de penetración. Estas evaluaciones ayudan a identificar posibles debilidades en su infraestructura de TI y le permiten tomar medidas correctivas para evitar posibles ataques y violaciones de seguridad. De esta forma el estándar hace su propia definición sobre Vulnerabilidades de Red y lo define de la siguiente manera:

> El software malicioso *(malware)* es un software o firmware diseñado para infiltrarse o dañar un sistema informático sin el conocimiento o consentimiento del propietario, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistema operativo del propietario (PCI Security Standards Council, 2022, p. 111)

Dentro de PCI DSS, la gestión en cuestión incluye la identificación, evaluación y reparación de Vulnerabilidades de Red en la infraestructura informática que los atacantes tengan la posibilidad explotar para comprometer la seguridad y la confidencialidad de los datos de la tarjeta.

El proceso de gestión de Vulnerabilidades de Red se vuelve esencial en el cumplimiento de PCI DSS, ya que permite a las organizaciones identificar y abordar rápidamente las Vulnerabilidades de Red y brechas de seguridad que podrían comprometer la confidencialidad e integridad de los datos de las tarjetas de pago.

El cumplimiento del plan de gestión de vulnerabilidades de red en el marco de PCI DSS es crucial para garantizar la seguridad de los datos de tarjetas de pago, que se trabajan en Symbiotic. Cumplir con este plan permite al departamento ayudar a identificar y abordar posibles debilidades en la red, reduciendo significativamente el riesgo de brechas de seguridad y asegurando la integridad y confidencialidad de la información financiera de los clientes. Además, el cumplimiento con los requisitos de PCI DSS es mandatorio para las organizaciones que manejan transacciones con tarjetas de pago, lo que no solo protege los datos sensibles, sino que también evita sanciones y pérdida de confianza por parte de los clientes y asociados comerciales.

2.7.2. ITIL

AXELOS, 2019) *ITIL® 4 Foundation: IT Infrastructure Library*, se presenta el concepto fundamental de "gestión de servicios", el cual es definido por (Corona, 2019). “Este término se refiere a un conjunto de capacidades organizacionales que permiten brindar valor a los clientes a través de servicios especializados.”

La versión 4 de ITIL tiene como objetivo principal de ITIL, como lo señala (Corona, 2019) es “proporcionar una guía o marco de referencia a las organizaciones para abordar los desafíos cambiantes en la gestión de servicios y aprovechar el potencial de la tecnología moderna.” A partir, de la definición anterior se proporcionará la explicación sobre el enfoque de Sistema de Valor del Servicio (SVS) que ITIL busca promover.

Sistema de Valor del Servicio (SVS)

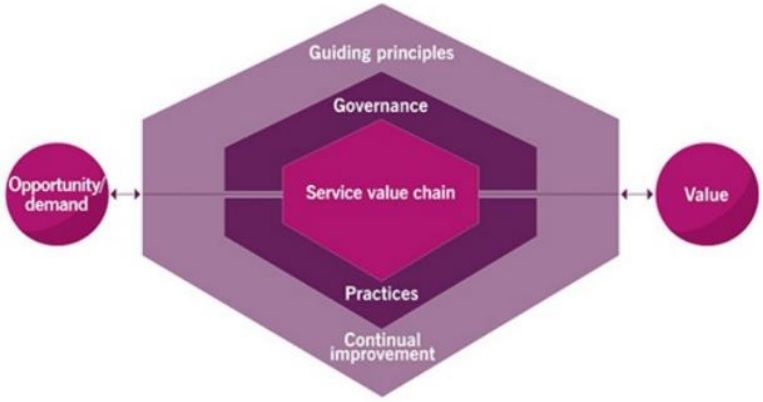
(AXELOS, 2019), explica que:

> La cadena de valor del servicio de ITIL proporciona un modelo operativo para la creación, entrega y mejora continua de servicios. Es un modelo flexible que define seis actividades clave que se combinan de diversas formas, formando múltiples flujos de valor. (AXELOS, 2019, pp. 82–83)

El enfoque innovador que ITIL presenta al crear el Sistema de Valor del Servicio (SVS) supone un cambio significativo en la perspectiva del ciclo de vida del servicio. El principal objetivo del SVS es representar de manera integral todos los componentes, factores y actividades involucrados en la gestión de servicios, con el propósito de favorecer la integración y coordinación de los valores organizacionales. Esta nueva aproximación busca proporcionar una visión más

holística y coherente de cómo los servicios se integran en la estructura de la organización y contribuyen a su éxito general. A continuación, se muestra la Figura 8

Figura 8 Cadena de Valor del Servicio



Fuente: Tomado de AXELOS. (2019). ITIL® 4 *Foundation: IT Infrastructure Library*, pagina 15.

A continuación, se detallan los componentes principales del SVS que se explican en AXELOS, (2019) en ITIL® 4 *Foundation: IT Infrastructure Library*:

- El Propósito: es el componente central del SVS y establece la razón de ser de la organización de TI. Define la dirección estratégica y los objetivos para entregar valor a los clientes y partes interesadas.
- Las Gobernanza: es responsable de la toma de decisiones y asegura que las políticas, estrategias y objetivos se cumplan en toda la organización de TI.
- La Cadena de Valor del Servicio: representa las actividades clave involucradas en la creación y entrega de servicios. Estas actividades son: planificar, mejorar, diseñar, transaccionar, entregar y apoyar.
- Las Prácticas de Gestión: son conjuntos de actividades organizadas que se emplean para llevar a cabo trabajos o lograr un objetivo particular.
- Los Resultados: representan los logros obtenidos a través de la aplicación de las prácticas de gestión. Los resultados se dividen en tres dimensiones: Resultados de rendimiento, Resultados de conformidad y Resultados de resistencia.

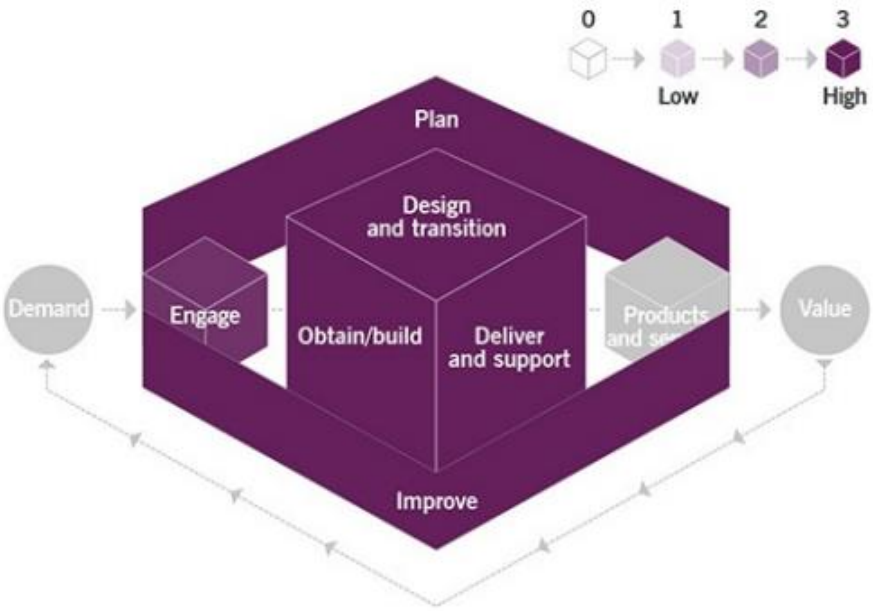
2.7.3. Práctica de Gestión de Seguridad de la Información

AXELOS, (2019) en el marco de referencia de ITIL® 4 *Foundation: IT Infrastructure Library*, habla sobre la práctica de Gestión de Seguridad de la Información. “La cual se enfoca en proteger los datos críticos que una organización necesita para llevar a cabo sus operaciones.” Esto implica la identificación y manejo de los riesgos, incidentes y Vulnerabilidades de Red asociados con la confidencialidad, integridad y disponibilidad de la información, así como otros aspectos de la seguridad de la información, como la autenticación. Para lograr una gestión efectiva, es fundamental mantener un equilibrio entre diferentes aspectos descritos por (AXELOS, 2019):

- Prevención: el objetivo es evitar que ocurran incidentes de seguridad en primera instancia. Para ello, se implementan controles y medidas de seguridad adecuadas para proteger la información de posibles amenazas y Vulnerabilidades de Red.
- Detección: aunque la prevención es crucial, no siempre existe la posibilidad de evitar todos los incidentes. Por lo tanto, es esencial detectar rápidamente cualquier actividad sospechosa o incidente de seguridad que pueda surgir para responder de manera oportuna.
- Corrección: una vez que se detecta un incidente, es necesario actuar rápidamente para corregirlo y mitigar sus efectos.

La Figura 9 permite entender cada una de las actividades de la cadena de valor relacionada a la práctica de Gestión de Seguridad. A continuación, se detallan cada una de las actividades descritas.

Figura 9 Contribución de la G. Seguridad a las actividades de la cadena de valor



Fuente: Tomado de AXELOS. (2019). ITIL® 4 *Foundation: IT Infrastructure Library*, pagina 116.

- Planificar: la seguridad de la información debe abarcar todas las actividades de planificación y debe incorporarse a todas las prácticas y servicios que se apliquen y desarrollen en la empresa.
- Mejorar: el plan busca mejorar en toda la actividad de la cadena de valor, pues permite garantizar que no se introduzcan Vulnerabilidades de Red al realizar mejoras.
- Comprometer: los requisitos de seguridad de la información para los servicios nuevos y modificados deben ser comprender y captar. Todos los niveles de compromiso, desde el operativo hasta el estratégico, deben apoyar la seguridad de la información.

- Diseño y transición: se debe tener en cuenta en toda esta actividad de la cadena de valor, el diseño de controles eficaces y su puesta en funcionamiento.
- Obtener o construir: se debe integrar en todos los componentes, basándose en el análisis de riesgos, las políticas, los procedimientos y los controles definidos por la política de seguridad de la información.
- Prestar y apoyar: la detección y corrección de los incidentes de seguridad de la información debe ser parte integrante de esta actividad de la cadena de valor

La Gestión de Seguridad de la Información se aplica en diversas áreas dentro de una organización, incluyendo:

- Procesos de Gestión de Vulnerabilidades de Red de seguridad de la información.
- Procesos de Gestión de Incidentes de seguridad de la información.
- Procesos de Gestión de Riesgos.
- Gestión de Cambios.
- Procedimientos de pruebas de penetración, escaneo de Vulnerabilidades de Red, etc.

La práctica de Gestión de cambios y la práctica de Gestión de incidentes en ITIL 4 se ocupan principalmente de los procesos de gestión de Vulnerabilidades de Red de seguridad de la información.

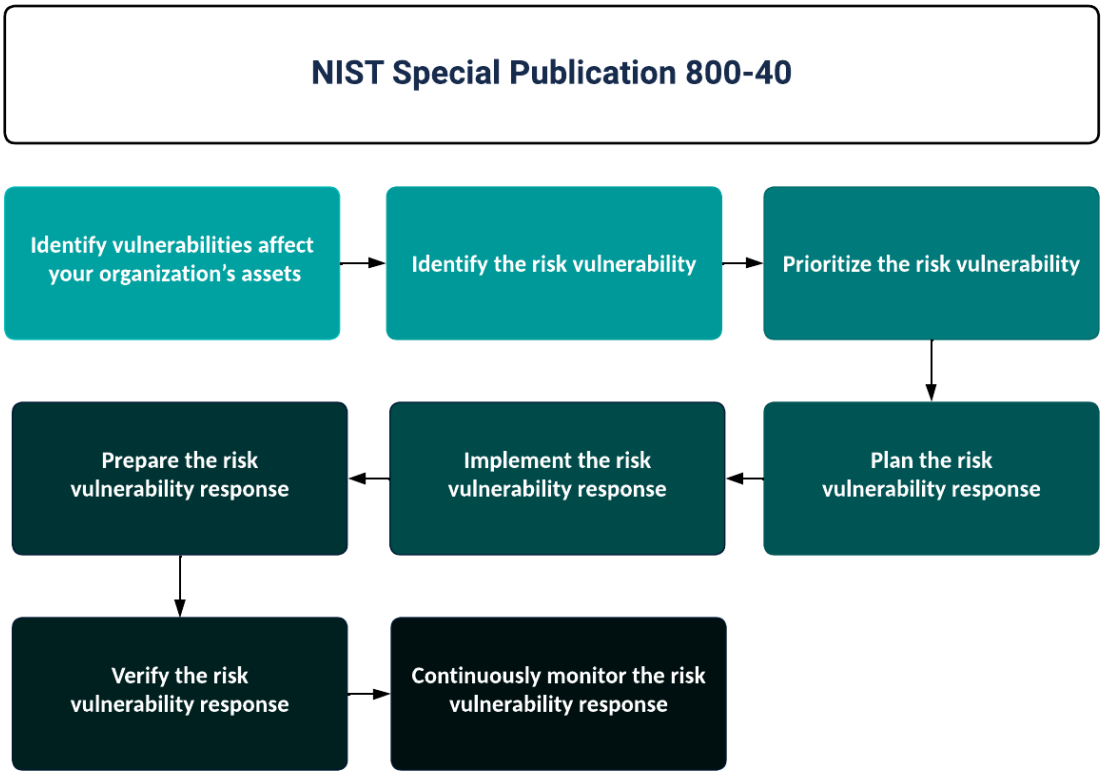
El control y la gestión de los cambios en la infraestructura y los servicios de TI se realiza para abordar las Vulnerabilidades de Red en la seguridad. La aplicación de parches, actualizaciones de software, cambios de configuración y otras acciones se incluyen en los cambios para mitigar las Vulnerabilidades de Red encontradas.

La práctica de la gestión de incidentes entra en acción cuando se encuentra una vulnerabilidad de seguridad o se produce un incidente de seguridad. Los incidentes de seguridad, incluida la gestión de las Vulnerabilidades de Red encontradas, se gestionan a través del proceso de gestión de incidentes, que también registra, categoriza, prioriza y resuelve los incidentes de seguridad. La implementación efectiva de la Gestión de Seguridad de la Información es esencial para proteger los activos más valiosos de una organización: la información y los datos confidenciales.

2.7.4. NIST SP 800-40 Creating a Patch and Vulnerability Management Program

Para definir el proceso de gestión de Vulnerabilidades de Red, la Figura 10 presenta el diagrama de actividades de este proceso. Las acciones mostradas permiten comprender desde dos niveles cuáles son las actividades del proceso contempla. Dicho proceso está descrito en la Publicación Especial 800-40 del NIST (Instituto Nacional de Estándares y Tecnología) sobre la Creación de un Programa de Gestión de Parches y Vulnerabilidades de Red.

Figura 10 NIST Special Publication 800-40



Fuente: Elaboración propia, 2023.

(Scarfone K & Souppaya M, 2022) en la NIST Special Publication 800-40. explica que la "Creación de un programa de administración de parches y Vulnerabilidades de Red, ofrece pautas y sugerencias para que las empresas establezcan procedimientos efectivos para administrar los parches de software y abordar las Vulnerabilidades de Red". El marco de *NIST Special Publication 800-40* define las pautas para la planificación, desarrollo y evaluación del proceso de gestión de Vulnerabilidades de Red. La Figura 10 se refiere a todas aquellas actividades macro que deben realizarse para garantizar el cumplimiento de la seguridad.

Así mismo, el documento hace hincapié en el método integral que emplea para desarrollar un programa de administración de parches y Vulnerabilidades de Red. Se enfoca en cuán crucial es formar el Grupo de Parches y Vulnerabilidades (PVG), un grupo a cargo de ejecutar el plan. El PVG actúa como punto focal de los esfuerzos para abordar las Vulnerabilidades de Red colaborando estrechamente con los administradores.

Por ende, el objetivo general de la publicación es ayudar a crear procedimientos eficientes para lidiar con parches y Vulnerabilidades de Red, mejorar la ciberseguridad y administrar el riesgo.

Este marco de referencia se convierte en un recurso valioso para establecer prácticas sólidas de mitigación de Vulnerabilidades de Red y administración de parches al poner en práctica el presente documento. Su adopción ayuda a las instituciones de educación superior y otras empresas a reforzar sus defensas de ciberseguridad y garantizar la seguridad de sus activos digitales e información privada. De esta forma, se logra implementar una gestión de la vulnerabilidad adecuada cuyo objetivo de reducir las posibles amenazas a la seguridad y mantener un entorno de TI seguro y fiable, siguiendo las recomendaciones proporcionadas en esta publicación.

A continuación, se pasarán a explicar cada una de las fases visualizadas en la Figura 10 para establecer una comprensión a mayor detalle.

Fase 1: Identificar las vulnerabilidades afectan los activos de su organización

(Scarfone K & Souppaya M, 2022) explican que en este periodo se recopila y documenta toda la infraestructura de sistemas, aplicaciones y activos digitales de la organización. Esto incluye servidores, equipos de red, estaciones de trabajo y otros componentes tecnológicos.

El objetivo es tener una comprensión clara y precisa de los elementos que componen el entorno tecnológico, para identificar áreas de riesgo y determinar qué activos deben monitorearse y administrarse.

Fase 2: Identificar el riesgo de la vulnerabilidad

Esta fase aborda las Vulnerabilidades de Red y amenazas identificadas en la fase anterior (Scarfone K & Souppaya M, 2022). Se contempla la implementación de las medidas de mitigación necesarias. Esto incluye parches, configuraciones de seguridad, actualizaciones de software o cualquier otra acción destinada a mejorar la seguridad y la resiliencia del sistema.

Fase 3: Priorización de la corrección de Vulnerabilidades de Red

En esta fase, se evalúan y priorizan las correcciones de Vulnerabilidades de Red. Esto se hace considerando factores como el impacto potencial de la vulnerabilidad, la gravedad de los activos afectados y la probabilidad de explotación. (Scarfone K & Souppaya M, 2022) hablan de que la priorización permite asignar recursos de manera eficiente y concentrarse en las Vulnerabilidades de Red que representan el mayor riesgo para su organización.

Fase 4: Planificar el riesgo respuesta a la vulnerabilidad

Esta fase crea la planificación sobre la información sobre correcciones específicas relevantes para la organización. Dicha planificación incluye parches, actualizaciones y correcciones específicas para las Vulnerabilidades de Red identificadas (Scarfone K & Souppaya M, 2022). Esto implica evaluar el riesgo que representa la vulnerabilidad para la organización, elegir qué forma de respuesta al riesgo (o combinación de respuestas) utilizar y decidir cómo implementar la respuesta al riesgo.

Fase 5: Preparar el riesgo respuesta a la vulnerabilidad

(Scarfone K & Souppaya M, 2022) señalan que se requieren la preparación de las pruebas que se vayan a implementar para la corrección en todo el entorno. Esta fase implica evaluar las soluciones en un entorno controlado para garantizar que no introduzcan nuevos problemas o conflictos. Las correcciones de prueba le permiten confirmar su validez y evitar fallas innecesarias en el sistema.

Fase 6: Implementar la respuesta a la vulnerabilidad

En esta etapa se explican las correcciones que se implementan en el entorno de producción (Scarfone K & Souppaya M, 2022). Esto incluye la distribución de parches, actualizaciones o configuraciones especiales a los sistemas y funciones afectados. Es importante seguir las mejores prácticas de implementación para garantizar una transición fluida y sin inconvenientes.

Los autores hacen énfasis en que se debe garantizar que la implementación constante de respuestas adecuada al riesgo de la vulnerabilidad. Además, realice diversas tareas administrativas a lo largo del ciclo de vida de la gestión de vulnerabilidades de red, incluida la actualización de la documentación, el mantenimiento de registros de auditoría y la generación de informes y conocimientos prácticos como parte de la gestión de vulnerabilidades.

Fase 7: Verificar el riesgo respuesta a la vulnerabilidad

Después de implementar una corrección en el entorno, es muy importante verificar su validez (Scarfone K & Souppaya M, 2022) . Este periodo implica el monitoreo y la evaluación continuos de los sistemas para garantizar que las vulnerabilidades de red se solucionen o mitiguen.

Fase 8: Supervisar continuamente la respuesta a la vulnerabilidad al riesgo

La etapa final según (Scarfone K & Souppaya M, 2022) afirman que la fase busca brindar seguimiento continuo del mantenimiento de los controles de seguridad, la aplicación de las respuestas de vulnerabilidades y conocer la eficacia de las mismas. Además, los autores explican que se deben realizar inspecciones periódicas para garantizar que ninguna medida crítica se haya desactivado accidentalmente.

El modelo NIST SP 800-40 descrito anteriormente por (Scarfone K & Souppaya M, 2022) muestra un proceso integral, estructurado para administrar y remediar Vulnerabilidades de Red en el entorno técnico. Cada paso es fundamental para identificar, evaluar, mitigar y validar Vulnerabilidades de Red con el fin de mejorar la seguridad y la resiliencia de una organización frente a posibles amenazas cibernéticas.

2.7.5. The Cyber Security Body of Knowledge (CyBOK)

Cybersecurity & Infrastructure Security Agency, (2016) define la importancia de la gestión de riesgos desde la perspectiva de Vulnerabilidades de Red de la siguiente manera:

> La evaluación del riesgo consta de tres componentes básicos [3]: (i) identificación y, si es posible, estimación del peligro; (ii) evaluación de la exposición y/o vulnerabilidad; y (iii) estimación del riesgo, combinando la probabilidad y la gravedad. La identificación se refiere a la determinación de los sucesos y los resultados subsiguientes, mientras que la estimación está relacionada con la fuerza relativa del resultado. La exposición se refiere a los aspectos de un sistema abiertos a los actores de amenazas (por ejemplo, personas, dispositivos, bases de datos), mientras que la vulnerabilidad se refiere a los atributos de estos aspectos que podrían ser objeto de ataques (por ejemplo, susceptibilidad a los ataques). (La estimación del riesgo puede ser cuantitativa (por ejemplo, probabilística) o cualitativa (por ejemplo, basada en escenarios) y capta el impacto esperado de los resultados. (Cybersecurity & Infrastructure Security Agency, 2016, p. 5)

El CyBOK proporciona una investigación profunda sobre una variedad de temas en ciberseguridad, incluida la gestión de Vulnerabilidades de Red. Esta última juega un papel central en la experiencia en gestión de riesgos y gobernanza, que incluye identificar, evaluar y remediar Vulnerabilidades de Red en los sistemas, aplicaciones y estructuras de red de una organización.

Para contextualizar la idea anterior Hallet & Chen, (2021) afirman que, dentro del dominio de la gestión de riesgos y el conocimiento de la gobernanza, la gestión de Vulnerabilidades de Red juega un papel fundamental para lograr una mitigación efectiva.

Así mismo, los autores establecen que las Vulnerabilidades de Red requieren una serie de actividades que sean específicamente diseñadas para abordar de manera proactiva las amenazas potenciales que tengan la posibilidad de ser explotadas por individuos o grupos malintencionados. Esto se evidencia en el Anexo III Ciclo de Gestión de Riesgos del CyBOK da una perspectiva sobre un proceso para gestionar las Vulnerabilidades de Red.

Este marco de procedimiento es fundamental para mantener la protección y la autenticidad de los activos digitales físicos y, al mismo tiempo, reducir el riesgo de intrusión y sabotaje cibernéticos. Al identificar y remediar las Vulnerabilidades de Red de manera sistemática y proactiva, las organizaciones fortalecen su postura de seguridad cibernética, pues reducen los posibles puntos de ataque y, en última instancia, ayudan a mejorar su postura de gobierno y gestión de riesgos.

2.8. Metodologías para la Mejora Continua de Procesos

2.8.1. Business Process Management

La Administración de Procesos de Negocios (*Business Process Management*) según lo que señalan (Dumas et al., 2018) afirman que:

> El objetivo de BPM (gestión de procesos empresariales), también conocida como gestión de procesos empresariales, es aumentar la eficacia y la eficiencia operativas de una organización a través de la automatización y optimización de procesos. Es una disciplina que busca identificar, diseñar, implementar, seguir y mejorar constantemente los procesos de negocio para lograr las metas y objetivos trazados por la empresa. (Dumas et al., 2018)

De acuerdo con la definición anterior, se entiende que la gestión de procesos de negocio (BPM) se ha convertido en una disciplina importante para la gestión de recursos, activos de las organizaciones. Cabe aclarar que la finalidad de esta metodología es mejorar la eficiencia y eficacia de las empresas a través de la automatización y optimización de los procesos internos.

De acuerdo con Dumas y La Rosa (2018), la disciplina es un enfoque integrado que tiene como objetivo identificar, desarrollar, implementar y monitorear y mejorar continuamente los procesos de negocios dirigidos a la realización de la organización. La gestión de procesos empresariales proporciona un enfoque eficaz para evitar que los procesos de gestión de Vulnerabilidades de Red se gestionen de forma deficiente.

La metodología, por su parte, busca crear flujos de trabajo y roles bien definidos, alineación con estándares y un enfoque en la mejora continua. De esta maneara, BPM promueve una gestión de Vulnerabilidades de Red más efectiva, mejorando la seguridad organizacional en un entorno empresarial cada vez más digital.

El marco de referencia de BPM juega un papel importante en la mitigación de las debilidades en la gestión de procesos. A medida que las empresas se vuelven más técnicas y cada vez más dependientes de los sistemas y datos digitales, la relevancia de BPM se vuelve aún más evidente en el contexto de las Vulnerabilidades de Red mal administradas.

2.8.2. Procesos BPM

Según (Bizagi, 2023) la definición de proceso se refiere a un “Grupo de acciones y pasos ejecutados para lograr un objetivo particular. En BPMN, un proceso contiene todas las formas, o elementos de modelado, que cumplen la lógica para lograr el objetivo”. Esta por esta razón, que el desarrollo del presente proyecto se utilizará la Notación de Gestión de Procesos de Negocio (BPMN 2.0) la cual define las pautas para el modelado de procesos que se acepta como la norma en la industria.

Con el fin de entender mejor la notación del marco de referencia BPMN 2.0 se utiliza el Anexo II, en donde Bizagi muestra todos los elementos necesarios para el modelo de procesos y una definición de cada uno de dichos componentes.

De la misma forma (Gartner, 2023a) describe el concepto de proceso como un "camino de procesos completo, impulsado por eventos, que inicia con una solicitud del cliente y finaliza con un resultado para el cliente. Estos procesos de negocios a menudo trascienden los límites de los departamentos e incluso de las organizaciones". El fin de usar del marco de referencia BPMN 2.0 en el presente documento es definir un marco de trabajo estructurado que permita identificar, evaluar, mitigar y gestionar las Vulnerabilidades de Red de manera eficiente y efectiva. No obstante, el uso de dicha metodología da paso a ventajas como:

- Estandarización, ya que alinea el proceso de gestión de Vulnerabilidades de Red con el marco BPMN 2.0 establece un lenguaje común y claro para describir el flujo de trabajo, que facilita el entendimiento y la comunicación entre los diferentes equipos.
- Visualización clara ya que proporciona una notación gráfica fácil de entender que le permite visualizar y analizar el proceso de gestión de Vulnerabilidades de Red con mayor claridad.
- Flexibilidad y Adaptabilidad, pues BPMN 2.0 es un marco versátil que permite personalizar el proceso de gestión de Vulnerabilidades de Red a las necesidades específicas de cada organización.

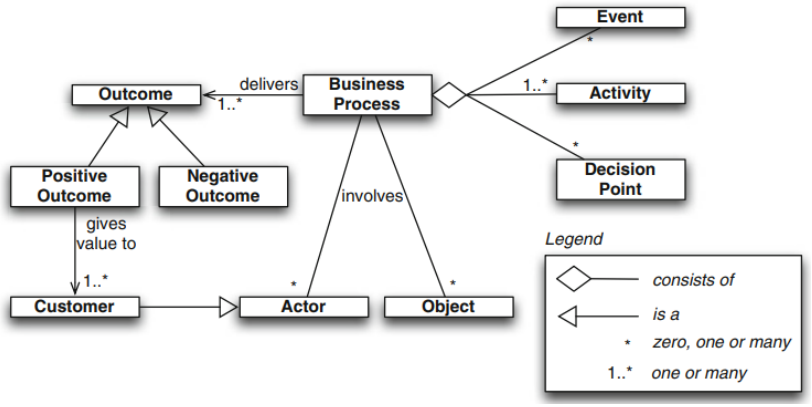
2.8.3. Procesos de Negocios

Según lo señalado por (Dumas et al., 2018, p. 30) en su libro “Fundamentos de la Gestión de Procesos de Negocios”, explican que un proceso de negocios es:

> Una secuencia de actividades coordinadas que se llevan a cabo en una organización con el propósito de lograr un resultado específico. Los procesos empresariales son lo que hacen las empresas cada vez que entregan un servicio o un producto a los clientes. (Dumas et al., 2018)

La Figura 11 brinda una serie de componentes que se deben tener en cuenta para entender el proceso de gestión de Vulnerabilidades de Red.

Figura 11 Componentes de un proceso



Fuente: Adaptado de Dumas, M. La Rosa, M (2018), pág. 34.

A continuación, se presentan las definiciones de los componentes del proceso de negocio que se visualizan en la Figura 11

Actividad: las actividades que actúan como sustitutos de diferentes trabajos o pasos que deben realizarse en el proceso general.

El flujo de control: es el componente principal que define la secuencia ordenada en la que se llevan a cabo varias actividades en un proceso. Es este flujo el que determina la cronología exacta de las acciones a lo largo del proceso, dándole coherencia y dirección.

La información: es esencial para la toma de decisiones y la operación del proceso se representa en forma de datos. Estos datos se utilizan, crean o modifican durante la ejecución del proceso y son fundamentales para la gestión y el funcionamiento operativos.

Las reglas de negocio: definen condiciones que rigen el comportamiento y la toma de decisiones en un proceso. Son estas directrices las que aseguran un funcionamiento uniforme y el cumplimiento de las políticas de la organización.

Roles: son un pilar importante que describe las responsabilidades y privilegios asignados a los individuos o grupos involucrados en el proceso. Estos roles describen las responsabilidades y funciones de cada participante en la realización del proceso.

Los eventos: son catalizadores que marcan el comienzo o el final de un paso particular en un proceso. Estos eventos se encuentran en secuencias de ejecución de procesos y momentos críticos.

Indicadores de desempeño: estas medidas permiten cuantificar y evaluar la eficiencia y eficacia de un proceso, proporcionando así una visión objetiva de su rendimiento y calidad.

Propietario del proceso: es la persona clave de gestión. Son los responsables de la dirección, seguimiento y gestión de todo el proceso, mientras velan por el cumplimiento de los objetivos de la organización y toman decisiones sobre posibles mejoras o modificaciones.

2.8.4. LEAN

Según señalan (Goldsby & Martichenko, 2005, p. 4) en su libro "*Lean Six Sigma*":

> Los conceptos "Lean" tienen sus raíces profundamente arraigadas en el Sistema de Producción Toyota. En su forma más pura, el enfoque Lean se centra en la eliminación de desperdicios y en el aumento de la velocidad y flujo. Aunque esta es una simplificación a nivel general, el objetivo último del enfoque Lean es eliminar los desperdicios de todos los procesos. (Goldsby & Martichenko, 2005, p. 4)

De acuerdo con la definición anterior, la metodología Lean se enfoca en identificar y eliminar desperdicios en los procesos. En el caso de la problemática relacionada a una inadecuada gestión de Vulnerabilidades de Red, existen ineficiencias y prácticas redundantes que son consideradas "desperdicios". Bajo esta premisa, Lean proporciona herramientas para identificar y corregir estas ineficiencias.

La metodología Lean permite optimizar el uso de los recursos, incluido el tiempo y el personal Goldsby & Martichenko, (2005). La aplicación de esta metodología a la gestión de Vulnerabilidades de Red tiene la capacidad de identificar pasos innecesarios o procesos duplicados que consumen recursos valiosos. La eliminación de estas barreras mejora la eficiencia de la identificación, evaluación y mitigación de Vulnerabilidades de Red.

Otra razón para considerar el uso de esta metodología recae en promover la mejora continua de los procesos. Aplicar este pensamiento a la gestión de Vulnerabilidades de Red significa que la organización, no solo aborda las Vulnerabilidades de Red existentes, sino que también se esfuerza por mejorar continuamente el proceso en sí, anticipando las amenazas futuras y adaptándose a los cambios en el entorno de ciberseguridad.

2.8.5. Six Sigma

La metodología Six Sigma es un enfoque altamente estructurado para la mejora continua, (Goldsby & Martichenko, 2005) explican que esta metodología se basa en:

> Six Sigma es una metodología de gestión que busca comprender y eliminar los efectos negativos de la variación en nuestros procesos. Basada en una infraestructura de profesionales capacitados (cinturones negros), Six Sigma ofrece un modelo de resolución de problemas respaldado por herramientas de "voz del cliente" y control estadístico de procesos. (Goldsby & Martichenko, 2005, p. 5)

El objetivo de la metodología alrededor de la eliminación los efectos negativos en los procesos habilita y promueve la estandarización de estos. Lo anterior permite diseñar e implementar procedimientos claros y consistentes para cada etapa del ciclo de vida de la gestión de Vulnerabilidades de Red.

La metodología descrita por Goldsby & Martichenko, (2005) proporciona herramientas para la priorización basadas en el impacto y la probabilidad. En la gestión de Vulnerabilidades de Red, esto ayuda a identificar las amenazas más críticas, es decir que requieren atención inmediata. Esto ayuda a evitar Vulnerabilidades de Red y asegurar que siga un conjunto de actividades sistemáticas que permitan el manejo de manera correcta y consistente de dichas Vulnerabilidades de Red.

No obstante, Six Sigma también destaca la importancia de medir y cuantificar. En el contexto de la gestión de Vulnerabilidades de Red, esto requiere el uso de métricas precisas para evaluar la eficacia del procedimiento, tales como: tiempo de detección y control de daños, tasa de resolución, etc. Los autores añaden que el uso de métricas establece un enfoque basado en datos para la mejora utilizando datos confiables y análisis perspicaces. En la gestión de Vulnerabilidades de Red, esto se traduce en tomar decisiones basadas en datos fácticos en lugar de intuiciones o suposiciones.

3. Marco Metodológico

La importancia de definir un marco metodológico la explica Arias, (2012, p. 110) como "La metodología del proyecto que incluye el tipo o tipos de investigación, las técnicas y los instrumentos que serán utilizados para llevar a cabo la indagación. Es el "cómo" se realizará el estudio para responder al problema planteado."

Con base en la definición anterior se afirma que la creación de un marco metodológico sirve como una estructura sistemática para recopilar, organizar y analizar información, de modo que los resultados permitan tener una interpretación en términos del problema descrito. Por ende, este capítulo se encarga de brindar una explicación detallada de los diversos elementos que constituyen el marco metodológico empleado durante el desarrollo del presente documento.

Por otro lado, el capítulo presenta información sobre el tipo de investigación seleccionado, el enfoque adoptado, el alcance del estudio, el diseño utilizado, las fuentes de información consultadas, los sujetos y variables de investigación; así como las técnicas empleadas para la recolección de datos. Además, se describen las diferentes etapas que conformaron el proceso de investigación realizado para el trabajo de graduación.

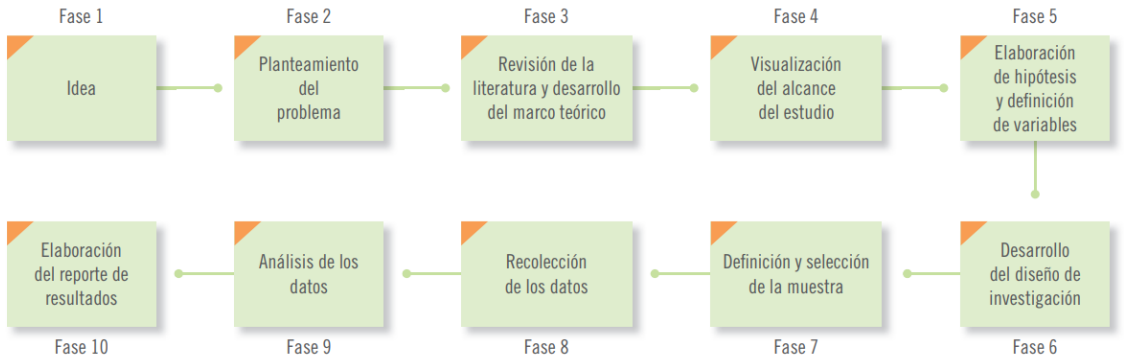
3.1. Enfoque de investigación

En el siguiente apartado se define el enfoque de investigación que se desarrollará en el presente documento, Arias, (2012, p. 23) afirma que el tipo de investigación es: "Se refiere al grado de profundidad con que se aborda un fenómeno u objeto de estudio."

Para esto se utilizará las definiciones brindadas por Hernández et al., (2010) en su libro Metodología de la investigación acerca de los enfoques de investigación con el objetivo de definir la mejor opción para el desarrollo del presente proyecto.

3.1.1. Cuantitativo

Figura 12 Definición del Enfoque Cuantitativo



Fuente: Tomado de Metodología de la investigación. McGRAW-HILL, p 45.

La Figura 12 permite entender las fases de desarrollo de un proyecto de investigación bajo el enfoque cuantitativo. Este enfoque según Hernández et al., (2010). es:

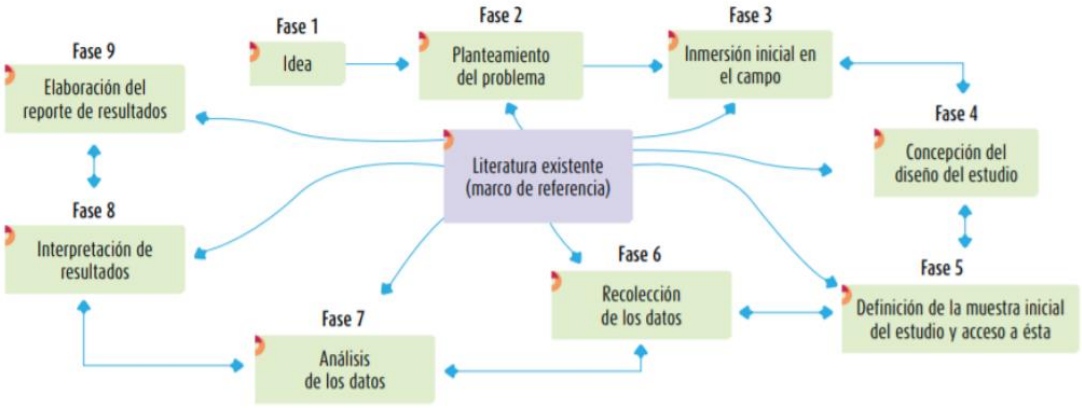
> Secuencial y probatorio. Cada etapa precede a la siguiente y no podemos "brincar o eludir" pasos, el orden es riguroso, aunque, desde luego, podemos redefinir alguna fase. Parte de una idea, que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica. (p. 46)

Al utilizar la investigación cuantitativa se aborda un enfoque sistemático y secuencial elaborado por etapas que permite que las preguntas específicas empleadas para obtener resultados numéricos se sustenten en los argumentos y contribuyan al conocimiento en el campo de estudio del problema.

Para esto se debe hacer una selección adecuada de los métodos de recopilación de datos, el análisis estadístico apropiado y la presentación clara y precisa de los resultados que son importantes para la validez y confiabilidad de la investigación.

3.1.2. Cualitativo

Figura 13 Definición del Enfoque Cualitativo



Fuente: Tomado de METODOLOGÍA de la investigación. McGRAW-HILL, p. 50.

La Figura 13 permite explicar las fases de desarrollo de un proyecto de investigación bajo el enfoque cualitativo. (Hernández et al., 2010). afirman que el enfoque cualitativo:

> Utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación. En la investigación cualitativa con frecuencia es necesario regresar a etapas previas. Por ello, las flechas de las fases que van de la inmersión inicial en el campo hasta el reporte de resultados se visualizan en dos sentidos. (pág. 49)

El uso de la investigación cualitativa facilita una comprensión profunda y enriquecida de los fenómenos sociales o humanos que se estudian. Dicha investigación permite a los participantes tener voz y explorar sus propias experiencias, creencias y perspectivas, brindando una perspectiva más completa y contextualizada del tema de estudio. Por esta razón, es fundamental presentar los resultados de forma clara y detallada, para que la investigación sea válida y tenga un impacto significativo en el campo.

Así mismo, es importante definir en qué consisten los datos cualitativos los cuales Hernández et al., (2010, p. 49) como: "Descripciones detalladas de situaciones, eventos, personas, interacciones, conductas observadas y sus manifestaciones."

3.1.3. Mixto

El último enfoque mixto, también conocido como investigación combinada o híbrida Hernández et al., (2010), busca integrar los elementos de investigación cuantitativa y cualitativa con el objetivo de explotar las fortalezas de ambos enfoques para obtener una comprensión más completa y holística del fenómeno en estudio.

> Los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (meta inferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (Hernández Sampieri y Mendoza, 2008, como se citó en Hernández, R., Fernández, C., y Baptista, M, 2010, p. 588).

La combinación de ambos enfoques permite obtener resultados más robustos y significativos, de modo que enriquece el valor y el impacto de la investigación. Para esto, es importante que el diseño y la realización de investigaciones mixtas se realicen con cuidado y conciencia para asegurar la calidad y validez de los resultados obtenidos.

3.1.4. Selección del tipo de metodología aplicada para este proyecto

Según la explicación de los enfoques anteriores se determina que se utilizará uno cualitativo para esta investigación. Esto se debe a que busca comprender las perspectivas de las diferentes partes involucradas en el proyecto con respecto al problema del proyecto y el entorno que le rodea. Además, se pretende llegar a una conclusión satisfactoria a de base de las opiniones y datos recolectados de los involucrados. Otra razón por la cual es un estudio cualitativo es que se utilizan técnicas de recolección de datos no estándarizados, reuniones con personas, discusiones y entrevistas para obtener la información necesaria. Además, el estudio no utiliza datos numéricos exactos para obtener los resultados deseados, al contrario, se consultan documentos organizacionales, opiniones, comentarios y características del proceso de gestión de Vulnerabilidades de Red para desarrollar la investigación y obtener el resultado deseado.

3.2. Diseño de la investigación

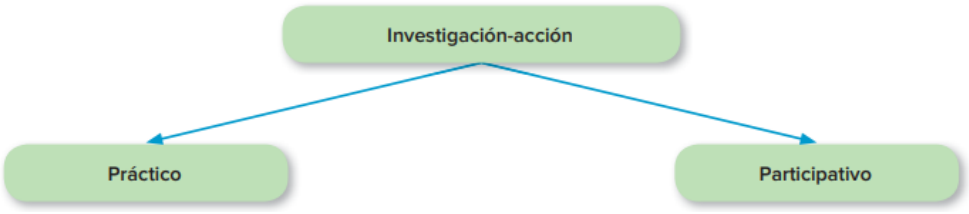
En el siguiente apartado se busca definir el diseño de la presente investigación, para esto se utilizarán los diseños de investigación cualitativa definidos por Hernández et al., (2010) los cuales tienen cinco perspectivas o abordajes diferentes; la teoría fundamentada, etnográfico, narrativo, fenomenológico y por último la investigación/acción. A continuación, se define la descripción de cada diseño que brinda el autor:

- Teoría fundamentada: se encarga de explicar el proceso o fenómeno de investigación. Este enfoque se utiliza para conocer objetos de estudio como procesos, acciones o interacciones entre individuos.
- Etnográfico: busca estudiar un sistema social como un todo, con el fin de brindar descripciones y justificaciones de la composición de elementos y grupos de la estructura social de estudio.
- Narrativo: pretende definir el objeto de estudio alrededor de una o más personas y sus biografías o contemplar varios relatos de un evento.
- Fenomenológico: este diseño se encarga de estudiar individuos que hayan compartido la experiencia o el fenómeno de estudio.
- Investigación/acción: la finalidad de la investigación-acción es comprender y resolver problemáticas específicas de una colectividad vinculadas a un ambiente. Su principio fundamental es que debe influir en el cambio y, como resultado, este cambio debe incorporarse al propio proceso de investigación.

La selección del diseño de investigación cualitativo para el desarrollo del presente trabajo se basa en el uso del abordaje investigación-acción que, de acuerdo con Hernández et al. (2010) está respaldado por la capacidad inherente para identificar y abordar problemas prácticos que sean contextualmente relevantes, como la gestión insuficiente del proceso de gestión de Vulnerabilidades de Red.

La Figura 14 permite entender los diseños básicos para aplicar el enfoque del abordaje investigación-acción. Así mismo, Hernández et al., (2010, p. 595) afirma que “Los diseños investigación-acción también representan una forma de intervención y algunos autores los consideran diseños mixtos, pues normalmente recolectan datos cuantitativos y cualitativos, y se mueven de manera simultánea entre el esquema inductivo y el deductivo.”

Figura 14 Diseños básicos de la investigación-acción.



Fuente: Tomado de METODOLOGÍA de la investigación. McGRAW-HILL, p. 592.

La Figura 14 respalda la selección del diseño de investigación-acción por su capacidad para abordar de manera completa y exitosa el proceso inadecuado de gestión de Vulnerabilidades de Red. Este método permite una comprensión profunda del problema desde una perspectiva práctica que apoya la participación de las partes interesadas y la implementación de soluciones viables y flexibles que mejoran significativamente la seguridad y la gestión de la organización.

3.3. Alcance de la Investigación

(Hernández et al., (2010) señalan que la delimitación del alcance de la investigación posibilita definir los límites en términos conceptuales y metodológicos de la indagación y, como consecuencia, identificar cuatro categorías de delimitación, a saber: exploratoria, descriptiva, correlacional y explicativa. A continuación, se detallan las categorías mencionadas:

- Investigaciones exploratorias: cumplen la función de preparar el terreno al establecer el precedente para investigaciones que poseen alcances descriptivos, correlacionales o explicativos. Se desarrollan cuando la intención es examinar fenómenos y dilemas que sean novedosos, desconocidos o apenas investigados.
- Investigaciones descriptivas: conforman el fundamento para investigaciones de naturaleza correlacional, proveyendo la información necesaria para la realización de estudios explicativos.
- Estudios explicativos: abarcan investigaciones cuyo objetivo radica en identificar las causas subyacentes de los eventos, problemas o fenómenos bajo estudio.
- Estudios correlacionales: engloban investigaciones que buscan establecer relaciones entre conceptos, fenómenos, hechos o variables. Estos análisis cuantifican las variables y sus conexiones mediante análisis estadísticos.

Para el presente trabajo se decide usar el alcance explicativo, debido que permite responder preguntas fundamentales como "¿por qué está ocurriendo la gestión inadecuada de Vulnerabilidades de Red?" y "¿cuáles son los factores que están contribuyendo a esta situación?". Al explorar las causas y relaciones más profundas, el alcance explicativo ayuda a proporcionar una visión integral de los elementos que afectan negativamente el problema de estudio.

3.4. Fuentes de datos e información

A lo largo del desarrollo del proyecto, se requiere emplear diversas fuentes de información que contribuyen a identificar la situación presente de la problemática y a plantear la solución correspondiente. A partir de esta necesidad, este apartado busca definir las medidas requeridas con el propósito de garantizar información pertinente para el proyecto.

Para definir en qué consiste el concepto de fuente de información Arias, (2012, p. 27) lo explica de la siguiente manera: una fuente es todo lo que suministra datos o información.

Según su naturaleza, las fuentes de información son documentales (proporcionan datos secundarios), o vivas (sujetos que aportan datos primarios). Así mismo, los autores Hernández et al., (2010, p. 29) brinda una clasificación para las fuentes de información en dos categorías:

- Fuentes de información Viva: personas que no son parte de la muestra, pero que suministran información en una investigación de campo.
- Fuentes de información Documentales: son documentos impresos, digitales, audiovisuales o audio, que están autorizados o validados.

3.4.1. Fuentes de Información Primaria

Las fuentes de información primarias son aquellas donde se encuentran la información original. La fuente primaria suele ser el resultado del trabajo intelectual; normalmente contiene información que no ha sido alterada o analizada, lo que significa que son datos puros que, no se han puesto en uso.

Hernández et al., (2010, p. 503) afirman que:

> Siempre y cuando el tiempo y los recursos te lo permitan, es conveniente tener varias fuentes de información y métodos para recolectar los datos. En la indagación cualitativa posees una mayor riqueza, amplitud y profundidad de datos si provienen de diferentes actores del proceso, de distintas fuentes y de una mayor variedad de formas de recolección.

Las fuentes de información primaria que se pretenden usar en el documento son publicaciones académicas, libros, marcos de referencia, diccionarios, enciclopedias y otros medios que contengan esta información. A continuación, se explica mediante la Tabla 2 la importancia de las fuentes primarias seleccionadas para el desarrollo del presente documento.

Tabla 2 Fuentes Primarias

Fuentes	Tipo de documento	Importancia
Contenidos en el repositorio interno de *Confluence*	Directrices de políticas. Documentos técnicos. Manuales técnicos.	Dichos documentos ofrecen una base de conocimiento esencial para comprender la problemática. Además, proporcionan información sobre las políticas, procesos, medidas técnicas y mejores prácticas relacionadas con la seguridad de la información y la gestión de Vulnerabilidades de Red en la organización.

Fuentes	Tipo de documento	Importancia
NIST Special Publication 800-40	Buenas prácticas de la industria	Este documento brinda las instrucciones para desarrollar un programa de administración de parches y Vulnerabilidades de Red para ayudar a las organizaciones a administrar las Vulnerabilidades de Red del software y aplicar parches de manera rápida y eficiente. El presente documento brinda recomendaciones para desarrollar políticas y procedimientos, seleccionar herramientas, realizar campañas de capacitación y concientización, y los pasos necesarios para establecer un programa de administración de parches, como la identificación, priorización, remediación y validación de Vulnerabilidades de Red.
Cybok Risk Management Governance Issue	Buenas prácticas de la industria	El documento se centra en la gestión de riesgos y Vulnerabilidades de Red con un enfoque especial referencia en la gestión de riesgos y Vulnerabilidades de Red en el contexto de la ciberseguridad. El documento proporciona un marco conceptual y una estructura sobre cómo abordar y reducir los riesgos asociados con la gestión insuficiente de Vulnerabilidades de Red.
PCI-DSS-v4_0	Buenas prácticas de la industria	El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago, versión 4.0 es un recurso clave para gestión de Vulnerabilidades de Red, particularmente en el contexto de las transacciones con tarjetas de pago. Además, el documento se alinea a las mejores prácticas para administrar la seguridad de los datos.
Fundamentals of Business Process Management	Marco de referencia	El documento permite dar una perspectiva holística, que se centra en la eficiencia, la calidad y la mejora continua en las operaciones organizacionales. Además, el libro ayuda a localizar posibles flujos de procesos relacionados con la gestión de Vulnerabilidades de Red dentro de una organización.

Fuentes	Tipo de documento	Importancia
ITIL Foundation 4	Marco de referencia	ITIL *(Information Technology Infrastructure Library*) es un marco de trabajo ampliamente reconocido para la gestión de servicios de tecnología de la información. Aunque no se enfoca específicamente en la ciberseguridad, ITIL ofrece principios y prácticas que ayudan a aplicar las mejores prácticas de la gestión de Vulnerabilidades de Red en un entorno tecnológico.
Instrumentos de investigación	Instrumentos de investigación	Las herramientas de investigación son fundamentales, son los dispositivos y procedimientos que se emplean para recopilar datos y conocer los detalles pertinentes sobre el problema que está investigando.

Fuente: Elaboración propia, 2023.

3.4.2. Fuentes de Información Secundaria

En relación con las fuentes de información secundarias, (Arias, 2012) señala que estas constituyen resúmenes o registros que expanden los datos adquiridos de las fuentes primarias. Las fuentes secundarias comprenden análisis, evaluaciones y otros contenidos que enriquecen la comprensión de las fuentes primarias. La Tabla 3 permite describir todo este tipo de documentos.

Tabla 3 Fuentes de Información Secundaria

Fuentes	Tipo de documento	Importancia
Repositorio Académicos TEC	Tesis Universitarias y Trabajos de graduación	Con el propósito de asegurar un documento de calidad y que cumpla con los contenidos requeridos, se recurre a consultas sobre materiales de referencia en la creación de un Trabajo de Fin de Grado.
Sitios web con artículos y revistas tecnológicas	Artículos	Las tendencias, innovaciones y desarrollos más recientes en los campos de la ciberseguridad y la gestión de Vulnerabilidades de Red se tratan en revistas de tecnología y sitios web de artículos. Esto es necesario para abordar un problema que está en constante evolución.

Fuentes	Tipo de documento	Importancia
Libros sobre terminología referente a la problematica	Libros	Para establecer definiciones precisas, construir una base teórica sólida y sustentar sus argumentos en una tesis sobre el tema de Gestión Inadecuada del Proceso de Vulnerabilidad, los diccionarios son fuentes cruciales. Al ofrecer una comprensión profunda y autoridad en el uso de términos clave en el campo de estudio, estos libros mejoran la investigación.

Fuente: Elaboración propia, 2023.

3.5. Sujetos de investigación

En este apartado se proporcionará una descripción detallada de los individuos involucrados en la investigación, como por ejemplo colaboradores y otros actores cruciales, que se buscan para obtener información sobre la problemática.

En virtud de esta razón, en esta parte del trabajo se identificarán todas las entidades, tanto individuales como legales, que desempeñen un rol en la administración del proyecto. Esto incluye a personas que tienen la posibilidad de verse directamente afectadas por el proyecto, así como aquellas que no tengan un impacto directo.

La Tabla 4 tiene como finalidad ofrecer una descripción exhaustiva de los sujetos que serán objeto de estudio. Además, se introducen tres niveles de evaluación, los cuales representan indicadores que facilitan una comprensión y visualización más claras de la información disponible.

Tabla 4 Sujetos de Investigación

Rol	Resumen de responsabilidades	Conocimientos
Security and Monitoring Agent	• Supervisión de la seguridad y respuesta a incidentes. • Operaciones de seguridad. • Detección y análisis de amenazas. • Cumplimiento e informes. • Documentación y comunicación de incidentes.	• Conocimientos de tecnologías y herramientas de seguridad, como cortafuegos, antivirus, SIEM y sistemas de detección de intrusiones. • Familiaridad con amenazas de seguridad comunes, Vulnerabilidades de Red y vectores de ataque.

Rol	Resumen de responsabilidades	Conocimientos
Security and Monitoring Manager	• Supervisión del cumplimiento de la protección de datos. • Supervisión y evaluación de alertas de seguridad. • Investigación y Resolución de Incidentes. • Mantenimiento de registros y documentación. • Privacidad desde el diseño. • Responsabilidad de supervisar y controlar el acceso a los datos.	• Conocimientos de las leyes y normativas de protección de datos, como el GDPR, CCPA u otras leyes de privacidad de datos aplicables. • Familiaridad con los principios de privacidad, incluido el consentimiento informado. • Gestión de Riesgos y Evaluación de Impacto.
IT Ops and Compliance Manager	• Supervisar y gestionar las operaciones tecnológicas y el cumplimiento de la normativa. • Dirigir el equipo de operaciones informáticas y agentes de cumplimiento. • Aplicar y mantener políticas y procedimientos de seguridad. • Evaluar y mitigar los riesgos de seguridad y cumplimiento. • Mantenerse al día sobre las mejores prácticas y normativas de seguridad. • Autorizar el acceso a los distintos componentes del sistema.	• Experiencia en la gestión efectiva de proyectos y operaciones de tecnología de la información para garantizar la eficiencia y la entrega exitosa de los servicios. • Habilidad para identificar riesgos y llevar a cabo auditorías internas para garantizar el cumplimiento normativo y la seguridad de la información. • Conocimiento profundo de regulaciones y estándares relevantes en la industria, como GDPR, PCI-DSS, y cómo asegurar el cumplimiento de los requisitos.

Rol	Resumen de responsabilidades	Conocimientos
IT Ops and Compliance Agent	• Mantener y gestionar la infraestructura tecnológica de la empresa. • Garantizar el cumplimiento de las políticas y normativas de seguridad y privacidad. • Supervisar y solucionar problemas relacionados con la red y los sistemas. • Aplicar y mantener medidas de seguridad y protección.	• Certificaciones de Seguridad de la información y cumplimiento normativo. • Conocimiento de estándares y normas de seguridad. • Gestión de riesgos informáticos. • Gestión de incidentes de seguridad. • Concienciación y educación en materia de seguridad.
Programador jefe	• Diseñar, implantar y mantener la infraestructura de la empresa. • Configurar y gestionar servicios en la nube como almacenamiento, redes y máquinas virtuales. • Automatizar procesos y tareas utilizando herramientas y servicios en la nube. • Optimizar el rendimiento y la escalabilidad de los sistemas en la nube. • Garantizar la seguridad y continuidad de los servicios en la nube.	• Experiencia previa en el diseño, implementación y administración de infraestructuras. • Conocimiento de plataformas en la nube populares como Amazon Web Services (AWS), Google Cloud Platform (GCP). • Experiencia en el uso de herramientas de automatización y orquestación de la nube como Terraform, Ansible o Kubernetes.

Fuente: Elaboración propia, 2023.

3.6. Variables o categorías de la investigación

En esta sección, se detalla cada una de las variables que serán empleadas en el contexto de este documento. Para esto Arias, (2012, p. 58) explica el concepto de variable de la siguiente manera: “una variable es una característica o cualidad; magnitud o cantidad, que puede sufrir cambios, y que es objeto de análisis, medición, manipulación o control en una investigación.”

Las variables de investigación son establecidas considerando los objetivos específicos del documento, ya que contribuyen a determinar qué aspectos evaluar para lograr el alcance de dichos objetivos. La Tabla 5 permite supervisar y gestionar las variables utilizadas, las cuales se emplearán para analizar las fluctuaciones del proceso de medición del trabajo.

Tabla 5 Variables de la investigación

Objetivo especifico	Variables	Contextualización	Indicadores
Analizar la situación actual de la gestión de Vulnerabilidades de Red para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria.	Situación actual de la gestión de Vulnerabilidades de Red.	**Capacidad de identificación** de las Vulnerabilidades de Red: Se refiere a la habilidad de un sistema, organización o individuo para detectar y reconocer posibles debilidades, en un sistema, proceso o infraestructura. **Nivel de Conformidad con Estándares de la Industria**: evalúa qué tan bien las prácticas y procedimientos actuales de gestión de Vulnerabilidades de Red cumplen con los estándares y recomendaciones de seguridad aceptados por la industria. **Contexto organizacional:** hace referencia a la forma en cómo las personas piensan y realizan las actividades relacionadas con el proceso de gestión de Vulnerabilidades de Red. **Documentación del proceso**: Documentación existente del proceso de gestión riesgos y Vulnerabilidades de Red.	Número de Vulnerabilidades de Red identificadas. Grado de evaluación de la puesta en práctica recomendada de los controles de seguridad. Cantidad de mejoras identificadas. Grado de conocimiento de la temática. Cantidad de documentos existentes relacionados con el proceso.

Objetivo especifico	Variables	Contextualización	Indicadores
Diseñar un marco de trabajo de la Gestión de Vulnerabilidades de Red para la Estandarización de las actividades de su ciclo de vida basado en las buenas prácticas internacionales.	Marco de trabajo de la Gestión de Vulnerabilidades de Red.	La variable hace referencia a: **Definición de roles y responsabilidades** en la gestión de Vulnerabilidades de Red: Según las buenas prácticas se debe tener una clara definición de roles y responsabilidades para asignar los recursos adecuados a cada rol. **Alineación con Estándares de Seguridad Reconocidos**: esta variable se refiere a la adaptabilidad del proceso de gestión de Vulnerabilidades de Red a los estándares y marcos de seguridad definidos internacionalmente.	Políticas existentes relacionadas a la gestión de Vulnerabilidades de Red. Procedimientos operativos existentes. Cantidad de responsabilidades definidas por rol. Nivel de conocimiento de los roles. Cantidad de controles y prácticas específicos de seguridad incorporadas en el proceso.
	Componentes del plan de gestión del marco de trabajo	La variable mide la amplitud y profundidad la de lista de componentes que el proceso de diseño aborda para cubrir las fases del ciclo de vida de la vulnerabilidad. Además, se analiza la asignación de recursos en la Gestión de Vulnerabilidades de Red.	Lista de componentes del plan de gestión del proceso. Grado de estandarización de las actividades pertenecientes al proceso. Cantidad de recursos asignados al proceso de Vulnerabilidades de Red.

Objetivo especifico	Variables	Contextualización	Indicadores
Definir indicadores de desempeño (KPI) para la medición del rendimiento del proceso de gestión de Vulnerabilidades de Red en términos de las fases de su ciclo de vida.	Modelo de indicadores claves de desempeño (KPI)	La variable contextualiza: Indicadores de desempeño: ofrece una perspectiva más completa y detallada para medir y evaluar el desempeño del proceso de gestión de Vulnerabilidades de Red desde diferentes perspectivas. Cumplimiento de Políticas y Normativas: evalúa la capacidad del proceso de gestionar Vulnerabilidades de Red en concordancia con políticas y regulaciones internas y externas.	Lista de indicadores claves seleccionados para el proceso de gestión de Vulnerabilidades de Red. Lista de indicadores que cumplen con las Políticas y Normativas.

Fuente: Elaboración propia, 2023.

3.7. Técnicas e instrumentos de recolección de datos

La siguiente sesión permite definir los instrumentos de recolección de datos que se utilizarán para el desarrollo del presente proyecto de graduación. Estas herramientas se consideran los medios a través de los cuales se obtendrá la información requerida, con el propósito de lograr un análisis pertinente a la situación problemática de la organización.

Hernández et al., (2010, p.443) explican que la "recolección de datos cualitativos es el acopio de datos narrativos en los ambientes naturales y cotidianos de los participantes o unidades de muestreo." La Tabla 6 proporciona una descripción detallada de cada uno de los instrumentos que serán empleados en el proceso.

Tabla 6 Instrumentos de recolección de datos

Instrumento	Justificación del uso del instrumento	Apéndice de referencia
Revisión Documental	Las investigaciones documentales contribuyen a comprender el núcleo fundamental del tema de estudio. Este tipo de análisis resulta útil para conocer los orígenes de un contexto, así como las experiencias o circunstancias que ocurren en él y su funcionamiento diario y excepcional". Hernández et al., (2010, p. 76) En el marco de este proyecto, se llevará a cabo un análisis y observación de los informes y documentos relacionados con proyectos.	Apéndice H Bitácora Revisión Documental

Instrumento	Justificación del uso del instrumento	Apéndice de referencia
Observación	Miles et al., (2014, citados por (Hernández et al., 2010) los explican que el objetivo de la técnica de la observación es "Comprender procesos, vinculaciones entre personas y sus situaciones, experiencias o circunstancias, los eventos que suceden al paso del tiempo y los patrones que se desarrollan" (p.25)	Apéndice I Bitácora de Observación
Encuesta	Las autoras Ulate & Vargas, (2016, p.79) describen este instrumento como "un método empleado para recopilar las opiniones de las personas sobre una situación o tema en particular en el que están involucradas. Por otro lado, también resaltan "la importancia de definir con precisión la muestra encuestada debido a su influencia sustancial en los resultados a obtener."	Apéndice L Encuesta Situación Actual del Proceso
Análisis de Brecha	El análisis de brechas proporciona una imagen realista de las deficiencias de seguridad existentes en el sistema. Sin esta evaluación, sería difícil identificar de manera efectiva las áreas específicas donde se necesita acción para cerrar la brecha entre la seguridad actual y la deseada.	Apéndice J Plantilla Análisis de Brecha
Entrevista	Así mismo Ulate & Vargas, (2016) explican que las entrevistas cualitativas posibilitan explorar experiencias individuales, perspectivas, valores, creencias, emociones, sentimientos, hechos concretos, narrativas de vida y otras dimensiones subjetivas y contextuales.	Apéndice N Entrevista: Diseño del Proceso de Gestión de Vulnerabilidades de Red y Componentes del Plan Apéndice Q Factores Críticos de Éxito de los KPIs Apéndice R Entrevista Sobre Definición de Indicadores

Fuente: Elaboración propia, 2023.

3.8. Matriz de cobertura de las variables

En relación con el desafío planteado en el apartado de la Situación problemática, la Tabla 7 garantiza que las variables identificadas en el apartado Variables o categorías de la investigación tengan asignado un instrumento de recolección de información, que permita realizar el análisis de cada una de ellas.

Tabla 7 Matriz de cobertura de las variables

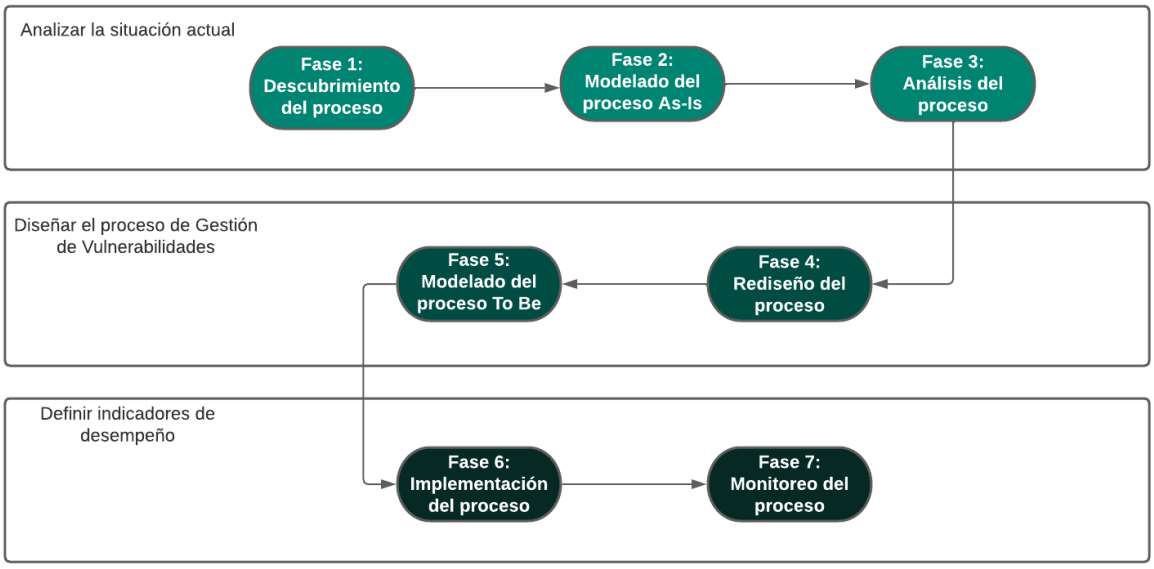
Variable	Encuesta	Entrevista	Observación	Revisión Documental	Análisis Brecha
Situación actual de la gestión de Vulnerabilidades de Red.	X		X	X	
Diseño del proceso de Gestión de Vulnerabilidades de Red.		X	X	X	X
Componentes del plan de gestión del proceso		X		X	
Modelo de indicadores claves de desempeño (KPI)	X	X	X		
Análisis de costos beneficio		X			

Fuente: Elaboración propia, 2023.

3.9. Procedimiento metodológico de la investigación

En esta sección, se desglosan minuciosamente las distintas etapas que se van a llevar a cabo para alcanzar el cumplimiento del objetivo general del proyecto. Conforme a lo expuesto en la sección del Alcance, estas etapas están estrechamente vinculadas con los objetivos específicos. La Figura 15 permite visualizar cada objetivo y las etapas que se engloban y alinean con el proceso de investigación para la solución del presente trabajo de graduación.

Figura 15 Fases de la metodología del proyecto



Fuente: Elaboración propia, 2023.

3.9.1. Etapa 1: Analizar la situación actual

En esta primera fase se realizó el análisis de la situación actual con relación al problema de la gestión insuficiente del proceso de Vulnerabilidades de Red, esta fase consta de tres subetapas básicas, las cuales son descritas a continuación:

Fase 1: Descubrimiento del proceso: en esta fase se procedió a investigar y descubrir en detalle el proceso actual de gestión de Vulnerabilidades de Red en la organización. Esto se llevó a cabo a partir de los instrumentos de recolección de información definidos en la Tabla 7. El proceso implicó identificar los componentes, las interacciones y los actores involucrados en el proceso existente.

Fase 2: Modelado del proceso As Is: una vez que se descubrió el proceso, se modeló en su estado actual, es decir, *As Is* o en español, el "proceso tal cual". En esta etapa, se buscó una representación gráfica del flujo de trabajo, los puntos de entrada y salida, así como los procedimientos y las decisiones tomadas en el proceso actual de gestión de Vulnerabilidades de Red.

Fase 3: Análisis del proceso: en esta fase, se realizó un análisis exhaustivo del proceso actual de gestión de Vulnerabilidades de Red, a partir de los instrumentos de recolección de información definidos en la Tabla 7 así como instrumentos de análisis específicos descritos por Dumas et al., (2018) en el capítulo relacionado al Análisis Cualitativo de Procesos, en donde se evaluaron las fortalezas, y debilidades del proceso, así como se identificaron áreas potenciales de mejora y optimización.

Estas tres etapas dentro de la Fase 1 fueron esenciales para comprender completamente el panorama actual de gestión de Vulnerabilidades de Red en la organización y sentar las bases para realizar mejoras en el proceso de metodología de investigación.

3.9.2. Etapa 2: Diseñar el marco de trabajo de Gestión de Vulnerabilidades de Red

Esta fase de la metodología de investigación se centró en el diseño general del proceso mejorado de gestión de la temática descrita con el objetivo de abordar el problema de la gestión insuficiente del proceso de Vulnerabilidades de Red en la organización. Esta fase incluyó dos específicas que crearon un proceso más eficiente:

Fase 4: Rediseño del proceso: se realizó el rediseño del proceso de gestión de Vulnerabilidades de Red basado en el análisis realizado en la fase 3. En esta fase se definieron los pasos, roles, responsabilidades y flujos de trabajo en el nuevo proceso. Se consideraron las lecciones aprendidas de la etapa anterior y se buscaron soluciones efectivas para solventar los problemas identificados.

Fase 5: Modelado del proceso To Be: se modelo el nuevo proceso de gestión de Vulnerabilidades de Red en su forma ideal, denominada *To Be*, teniendo en cuenta las mejores prácticas de la industria y los hallazgos encontrados en la sección 3.9.1 de modo que permite definir los objetivos de mejora.

3.9.3. Etapa 3: Definir indicadores claves de desempeño

Esta fase del procedimiento metodológico de investigación se centró en la definición de indicadores clave de desempeño para evaluar la efectividad y eficiencia del proceso de Gestión de Vulnerabilidades de Red.

Fase 6: Implementación del proceso: en este paso se realizó una estrategia de implementación para la propuesta además de ejecutar simulación el proceso definido en la Etapa 2: Diseñar el marco de trabajo de Gestión de Vulnerabilidades de Red, para esto se han implementado todas las actividades, funciones y secuencias de tareas definidas en el proceso rediseñado. Así mismo se diseñó la estrategia de implementación de la solución.

Durante esta fase de la simulación, los respectivos equipos adaptaron y adoptaron el proceso, asegurando una transición suave y fluida al proceso anterior descrito en el apartado Fase 2: Modelado del proceso As Is. Esta simulación, permitió probar nuevas técnicas y probar su aplicabilidad en un entorno controlado antes de la implementación completa en operaciones reales.

Fase 7: Monitoreo del proceso: durante esta etapa, se establecieron métricas de rendimiento clave para evaluar la efectividad y eficiencia del proceso de Gestión de Vulnerabilidades de Red. Se recolectaron datos pertinentes sobre la identificación, mitigación, evaluación y comunicación de Vulnerabilidades de Red, con el propósito de evaluar el grado de cumplimiento de los objetivos establecidos según lo mencionado en etapas anteriores.

La fase 3 del proceso metodológico de investigación permitió definir indicadores clave de desempeño para medir la efectividad del nuevo proceso de gestión de Vulnerabilidades de Red, encaminado a solucionar el problema de la gestión insuficiente del proceso de vulnerabilidad en el marco de la organización de estudio.

3.10. Operacionalización de las variables o categorías.

En esta sección se describe la relevancia de comprender cómo se relacionan y se ponen en práctica las variables en el contexto de este estudio. El enfoque de este trabajo se basa en la observación para lograr una contextualización adecuada de la función de estas variables. Más adelante, en la Tabla 8 presentan las etapas y el funcionamiento de estas variables.

Tabla 8 Operacionalización de las variables

Objetivo especifico	Variables	Definición	Indicadores	Instrumento
Analizar la situación actual de la gestión de Vulnerabilidades de Red para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria.	Situación actual de la gestión de Vulnerabilidades de Red.	La variable se refiere a la: **Capacidad de identificación de las Vulnerabilidades de Red**: es la habilidad que tiene el sistema, la organización o un individuo para detectar y reconocer posibles debilidades, en un sistema, proceso o infraestructura. **Nivel de Conformidad con Estándares de la Industria:** evalúa qué tan bien las prácticas y procedimientos vigentes de gestión de Vulnerabilidades de Red cumplen con los estándares y recomendaciones de seguridad aceptados por la industria. **Contexto organizacional**: hace referencia a la forma en cómo las personas piensan y realizan las actividades relacionadas con el proceso de gestión de Vulnerabilidades de Red. **Documentación del proceso**: documentación existente del proceso de gestión riesgos y de Vulnerabilidades de Red.	Número de Vulnerabilidades de Red identificadas. Grado de evaluación de la implementación recomendada de los controles de seguridad. Cantidad de problemas identificados en la situación actual. Grado de conocimiento de la temática. Cantidad de documentos existentes relacionados con el proceso.	Encuesta a los sujetos de investigación definidos. (Apéndice L Encuesta Situación Actual del Proceso) Revisión Documental: • Directrices de políticas. • Documentos técnicos. (Apéndice H Bitácora Revisión Documental) Observación: • Procesos y actividades relacionadas a la gestión de Vulnerabilidades de Red. (Apéndice I Bitácora de Observación)

Objetivo especifico	Variables	Definición	Indicadores	Instrumento
Diseñar un marco de trabajo de la Gestión de Vulnerabilidades de Red para la Estandarización de las actividades de su ciclo de vida basado en las buenas prácticas internacionales.	Marco de trabajo de la Gestión de Vulnerabilidades de Red.	La variable hace referencia a: **Definición de roles y responsabilidades en la gestión de Vulnerabilidades de Red:** según las buenas prácticas, se debe tener una clara definición de roles y responsabilidades para de asignar los recursos adecuados a cada rol. **Alineación con Estándares de Seguridad Reconocidos**: esta variable se refiere a la adaptabilidad del proceso de gestión de Vulnerabilidades de Red a los estándares y marcos de seguridad definidos internacionalmente.	Políticas existentes relacionadas a la gestión de Vulnerabilidades de Red. Procedimientos operativos existentes. Cantidad de responsabilidades definidas por rol. Nivel de conocimiento de los roles. Cantidad de controles y prácticas específicas de seguridad incorporadas en el proceso.	Análisis de brecha del proceso existente contra las buenas prácticas de la industria. (Apéndice J Plantilla Análisis de Brecha) Entrevista a los sujetos de investigación definidos. (Apéndice N Entrevista: Diseño del Proceso de Gestión de Vulnerabilidades de Red y Componentes del Plan) Revisión Documental: • Directrices de políticas. • Documentos técnicos. • Manuales técnicos. • Matriz de roles y responsabilidades. • Estándares de buenas prácticas. (Apéndice H Bitácora Revisión Documental)

Objetivo especifico	Variables	Definición	Indicadores	Instrumento
				Observación: • Procesos y actividades relacionadas a la gestión de Vulnerabilidades de Red. (Apéndice I Bitácora de Observación)
	Componentes del plan de gestión del marco de trabajo	La variable mide la amplitud y profundidad de la lista de componentes que el proceso de diseño aborda en las fases del ciclo de vida de la vulnerabilidad. Además, se analiza la asignación de recursos en la Gestión de Vulnerabilidades de Red.	Lista de componentes del plan de gestión del proceso. Grado de estandarización de las actividades pertenecientes al proceso. Cantidad de recursos asignados al proceso de Vulnerabilidades de Red. Porcentaje de la utilización de recursos en relación con la cantidad de Vulnerabilidades de Red tratadas y su influencia.	Entrevista a los sujetos de investigación definidos. (Apéndice N Entrevista: Diseño del Proceso de Gestión de Vulnerabilidades de Red y Componentes del Plan) Revisión Documental: • Estándares de buenas prácticas. • Directrices de políticas. (Apéndice H Bitácora Revisión Documental)

Objetivo especifico	Variables	Definición	Indicadores	Instrumento
Definir indicadores de desempeño (KPI) para la medición del rendimiento del proceso de gestión de Vulnerabilidades de Red en términos de las fases de su ciclo de vida.	Modelo de indicadores claves de desempeño (KPI)	Indicadores de desempeño: ofrece una perspectiva más completa y detallada para medir y evaluar el desempeño del proceso de gestión de Vulnerabilidades de Red desde diferentes perspectivas. Cumplimiento de Políticas y Normativas: evalúa la capacidad del proceso de gestionar Vulnerabilidades de Red en concordancia con políticas y regulaciones internas y externas.	Lista de indicadores claves seleccionados para el proceso de gestión de Vulnerabilidades de Red. Lista de indicadores que cumplen con las Políticas y Normativas.	Entrevista a los sujetos de investigación definidos. (Apéndice Q Factores Críticos de Éxito de los KPIs) (Apéndice R Entrevista Sobre Definición de Indicadores) Revisión Documental: • Estándares de buenas prácticas. • Documentos técnicos. (Apéndice H Bitácora Revisión Documental) Observación: • Procesos y actividades relacionadas a la gestión de Vulnerabilidades de Red. (Apéndice I Bitácora de Observación)

Fuente: Elaboración propia, 2023.

3.11. Tabla Resumen del Procedimiento Metodológico

Esta sección resume los métodos utilizados en el desarrollo del proyecto. La Tabla 9 permite vincular describir los pasos metodológicos, las herramientas utilizadas para recopilar datos para cada paso, los anexos asociados con cada paso y, finalmente, los productos o entregables asociados con cada paso.

Tabla 9 Resumen del Procedimiento Metodológico

Objetivo	Fase	Conclusiones	Recomendaciones	Desarrollado en	Apéndice / Anexo
Analizar la situación actual de la gestión de Vulnerabilidades de Red para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria.	Descubrimiento del proceso	Capítulo 6 Sección 6.1	Capítulo 7 Sección 7.1	Análisis de la situación actual	Apéndice L Apéndice M
	Modelado del proceso			Modelado de Procesos *As Is*	Apéndice S Apéndice T Apéndice U
	Análisis del proceso			Análisis de los Procesos Análisis de Brechas	Apéndice V Apéndice W Apéndice X
Diseñar un marco de trabajo de la Gestión de Vulnerabilidades de Red para la Estandarización de las actividades de su ciclo de vida basado en las buenas prácticas internacionales.	Rediseño del proceso	Capítulo 6 Sección 0	Capítulo 7 Sección 7.2	Componentes de la Solución	Apéndice J Apéndice N Apéndice P Anexo IV Anexo V

Objetivo	Fase	Conclusiones	Recomendaciones	Desarrollado en	Apéndice / Anexo
					Anexo VI Anexo X Anexo XI
	Modelado de proceso To Be			Identificación de las oportunidades de mejoras de los procesos Rediseño y Modelado de los Procesos	Anexo VII Anexo VIII Anexo IX
Definir indicadores de desempeño (KPI) para la medición del rendimiento del proceso de gestión de Vulnerabilidades de Red en términos de las fases de su ciclo de vida.	Implementación del proceso	Capítulo 6 Sección 6.2.11	Capítulo 7 Sección 0	Estrategia de Implementación	Apéndice Z Apéndice AA
	Monitoreo del proceso			Catálogo de KPI's Métricas de Control y Seguimiento de la Implementación	Apéndice Q Apéndice R Apéndice Y Anexo VI Anexo XI

Fuente: Elaboración propia, 2023.

4. Análisis de Resultados

En este capítulo se presenta el análisis de resultados de las variables de investigación del proyecto. Dicha sección detalla los resultados de la puesta en práctica de los instrumentos de recolección de información desarrollados para cada variable descrita en el apartado de Matriz de cobertura de las variables, de modo que permita conocer la situación actual y la deseada para el cumplimiento de Symbiotic en la implementación de la propuesta del Programa de gestión de Vulnerabilidades de Red. La propuesta del programa en cuestión va a emplear un enfoque riguroso y exhaustivo que permite, evaluar la efectividad y presentar los beneficios de una iniciativa para identificar, analizar, mitigar y eliminar Vulnerabilidades de Red en el entorno tecnológico de la organización.

Las autoras (Ulate & Vargas, 2016, p. 92) mencionan que en el análisis de datos “es importante determinar la mejor manera de analizar la información y definir las herramientas para racionalizar los datos recolectados, a fin de dilucidar y exponer las relaciones existentes entre las variables estudiadas”. Los datos recopilados tienen como objetivo obtener una comprensión integral de cómo el programa fortalece la postura de seguridad de la organización y optimizar su capacidad para abordar las necesidades actuales y futuros en el entorno digital.

4.1. Análisis de la situación actual

En la fase inicial del estudio, se presenta un análisis exhaustivo del estado actual del proceso de gestión de Vulnerabilidades de Red en el contexto organizacional. Para obtener una visión completa, se implementaron diferentes técnicas de recolección de información, que engloban entrevistas con los miembros encargados del proceso, revisión detallada sobre la documentación existente que explica los procedimientos, y la observación directa de la ejecución concreta de este procedimiento.

A través de los instrumentos aplicados, se recolecto información acerca de la forma en que las Vulnerabilidades de Red son abordadas en el entorno del departamento de *IT Operations and Compliance* de Symbiotic en la actualidad. Para entender el contexto de la situación actual se aborda a partir de la contextualización definida para dicha variable, en donde se analiza la capacidad de identificación de las Vulnerabilidades de Red, el nivel de Conformidad con Estándares de la Industria, el contexto organizacional y la documentación del proceso.

4.1.1. Capacidad de identificación de las Vulnerabilidades de Red

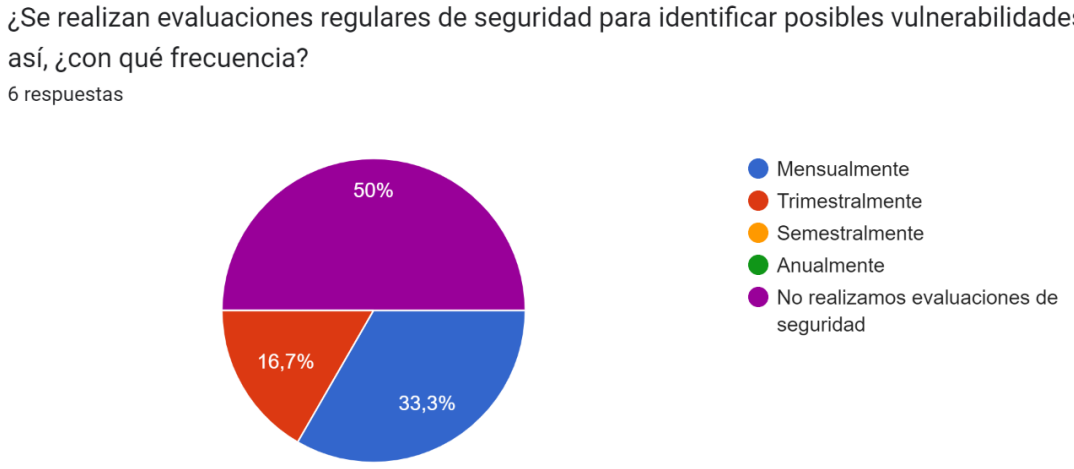
En esta sección, se aborda específicamente la habilidad de la organización para identificar de manera eficaz las Vulnerabilidades de Red en sus sistemas y operaciones. A través del Apéndice L, permite realizar el análisis de la perspectiva de la capacidad de identificación de las Vulnerabilidades de Red sobre la variable de situación actual.

Figura 16 Resultados sobre la identificación de Vulnerabilidades de Red

Fuente: Elaboración propia, 2023.

La Figura 16 busca comprender cómo la organización aborda la capacidad de identificación de Vulnerabilidades de Red como se muestra un 66.7% de los encuestados afirman que la efectividad de la etapa de identificación es moderada, los encuestados hacen ver que tener una eficiencia moderada impacta en las etapas de mitigación y prevención de amenazas. Además, señala que una persona afirma que la etapa de identificación es poco efectiva, lo cual cataloga como un individuo aún más crítico en alrededor del proceso.

Figura 17 Resultados sobre evaluaciones regulares de seguridad



Fuente: Elaboración propia, 2023.

Los resultados de Figura 17 muestran que el 50% de los encuestados aseguran que no se realizan evaluaciones regulares sobre la identificación de Vulnerabilidades de Red. No obstante, para entender la respuesta en cuestión cabe resaltar que los entrevistados que marcaron la opción de "mensualmente" equivalente al 33% son el *Security and Monitoring Agent* y *IT Ops and Compliance Manager*, los cuales son los dueños del proceso actual y estos afirman que, aunque estas evaluaciones están calendarizadas para ser mensuales no se realizan de esta manera, sino que se llevan a cabo por peticiones de los clientes o solicitudes de procesos de auditorías.

Los hallazgos encontrados en la Figura 16 y Figura 17 implican que los procesos de detección de Vulnerabilidades de Red y evaluación de seguridad de la organización requieren una valoración exhaustiva. A partir de estos hallazgos, el presente documento busca tomar medidas para aumentar la eficiencia de la detección de las amenazas dadas las implicaciones directas para la mitigación y prevención de amenazas. Esto permite a la organización fortalecer su postura de seguridad y mitigar proactivamente los riesgos potenciales.

4.1.2. Contexto organizacional

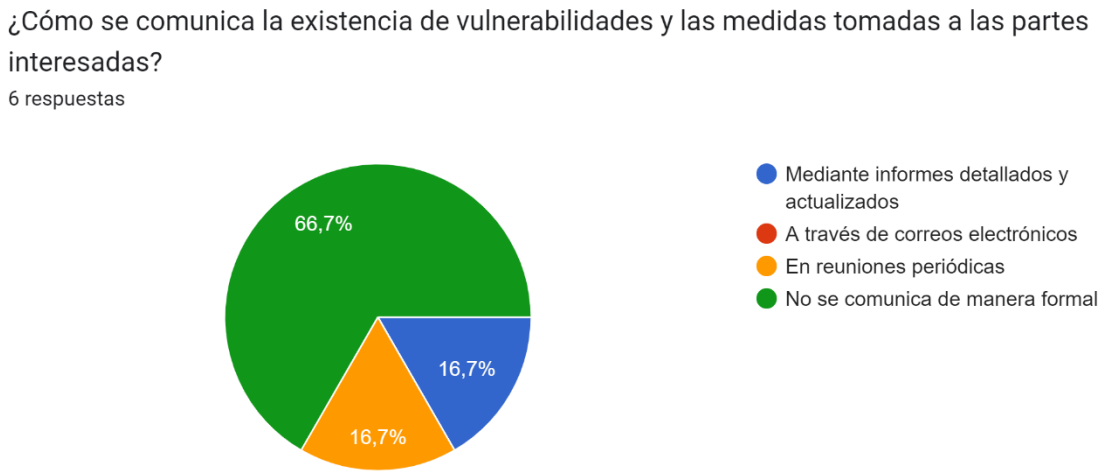
Dentro de este apartado se realiza un análisis de la contextualización de la variable "Situación actual del proceso de gestión de la vulnerabilidad", específicamente enfocado desde una perspectiva del contexto organizacional. A través del Apéndice L Encuesta Situación Actual del Proceso se busca comprender en detalle cómo el entorno, las estructuras y las prácticas organizacionales influyen en la forma en que se maneja la identificación y mitigación de Vulnerabilidades de Red en sistemas y procesos. Por otro lado, el Apéndice M Minuta recolección de información Encuesta Situación Actual permite realizar el análisis de la perspectiva del contexto organizacional sobre la variable de situación actual.

Figura 18 Resultados sobre el conocimiento de las etapas de mitigación y resolución

Fuente: Elaboración propia, 2023.

Según la Figura 18 muestra que la etapa de mitigación y resolución no cumple con los pasos establecidos, pues los encuestados afirman que en estas etapas se realiza reproceso haciendo que se gaste tiempo de operación en otras actividades, al no tener plazos de tiempo definidos, esto evidencia que los responsables no tienen claro la ejecución del proceso.

Figura 19 Resultados sobre el conocimiento de la comunicación de Vulnerabilidades de Red



Fuente: Elaboración propia, 2023.

La Figura 19 muestra los resultados obtenidos en la encuesta sobre el conocimiento de la comunicación de Vulnerabilidades de Red que se identifican en la organización. Según el gráfico anterior un 66.7% de los encuestados afirma que no hay un protocolo formal de comunicación sobre las amenazas, lo cual, en consecuencia, generan que no todos los involucrados o personal de diferentes departamentos que tengan que ser notificados no sean informados de manera correcta.

En conclusión, los resultados presentados en las Figura 18 y Figura 19 resaltan aspectos relevantes que requieren atención en la organización. En el contexto organizacional es esencial implementar medidas para mejorar la eficiencia de las etapas de mitigación y resolución, de manera que reduzca los reprocesos y en su lugar establezcan plazos de tiempo definidos. Asimismo, la creación de un protocolo formal de comunicación de Vulnerabilidades de Red es importante para garantizar que todas las partes interesadas pertinentes al proceso estén informadas de manera adecuada y oportuna.

4.1.3. Nivel de Conformidad con Estándares de la Industria

En esta sección mediante el uso del Apéndice L Encuesta Situación Actual del Proceso se examina en detalle si el personal de la organización conoce sobre los estándares y prácticas de gestión de Vulnerabilidades de Red reconocidos por la industria.

Figura 20 Resultados sobre el uso de estándares internacionales

Fuente: Elaboración propia, 2023.

Las respuestas proporcionadas en la Figura 20 ofrecen una visión de cómo la organización se relaciona con los estándares de seguridad en su enfoque de gestión de Vulnerabilidades de Red. Según el gráfico anterior, se muestra como la mitad (50%) de los encuestados indica que la organización se está adaptando actualmente para cumplir con estándares internacionales reconocidos, enfocados en la gestión de Vulnerabilidades de Red. Esto demuestra que la organización está trabajando en la implementación gradual de los estándares y que es consciente de la necesidad de mejora.

Figura 21 Resultados sobre conocimiento de estándares internacionales

Fuente: Elaboración propia, 2023.

Los resultados obtenidos en la Figura 21 muestran el nivel de conocimiento que tiene el personal del departamento sobre las regulaciones internacionales. Los encuestados afirman conocer "moderadamente" los requisitos de seguridad, lo que lleva a representar un 66.7% de las respuestas totales. Esto indica que una mayoría de los encuestados tiene un nivel aceptable de conocimiento y comprensión de los requisitos de seguridad propuestos por estos estándares.

Figura 22 Resultados sobre el nivel de priorización de cumplimiento

Fuente: Elaboración propia, 2023.

La Figura 22 y sus resultados ejemplifican la relevancia que tiene el acoplamiento de las buenas prácticas internacionales en los procesos de la organización. El 66.7% de los encuestados afirman que el porcentaje de prioridades “muy altas” se debe al compromiso que tiene la empresa por cumplir con las certificaciones que aplican al nicho de mercado la organización, que permiten adherirse a las mejores prácticas de seguridad.

El gráfico muestra que las respuestas obtenidas son un reflejo de la importancia que la organización otorga a la seguridad y el cumplimiento de los estándares aceptados, los cuales permiten definir la línea base que sirve para desarrollar la propuesta de plan de gestión de Vulnerabilidades de Red.

Los resultados descubiertos a partir de las preguntas anteriores ayudan a establecer los cimientos esenciales para la elaboración del plan de gestión de Vulnerabilidades de Red propuesto. La combinación entre el firme compromiso hacia la adaptación a estándares, el nivel moderado de conocimiento del equipo y la alta relevancia concedida al cumplimiento y la seguridad, señalan que la organización se encuentra en una posición que requiere mejoras para avanzar hacia una gestión de Vulnerabilidades de Red más eficaz y alineada con las mejores prácticas de la industria.

4.1.4. Documentación del proceso

En esta sección se llevó a cabo un análisis con el fin de examinar cómo la capacidad de identificar Vulnerabilidades de Red se refleja y registra en la documentación del proceso. La Tabla 10 permite una comprensión completa del modo en que la organización documenta y monitorea sus iniciativas de protección de ciberseguridad, proporcionando una visión holística de los esfuerzos en esta área crítica.

Tabla 10 Bitácora de Revisión Documental sobre la Situación Actual

Bitácora de Revisión Documental sobre la Situación Actual			
Id	Fecha	Documento	Hallazgo
RevD-01	29 agosto 2023	*Vulnerability Management Plan*	El documento presenta en el procedimiento actual de la gestión de Vulnerabilidades de Red algunos aspectos importantes dentro de los que se encuentran: • El documento no tiene definido una categorización de Vulnerabilidades de Red. • No se encuentran definidos los aspectos de priorización para los diferentes componentes del sistema. • No se encuentra un plan o procedimiento de comunicación sobre las diferentes etapas del ciclo de vida de las Vulnerabilidades de Red, específicamente para la etapa de la mitigación y control. • No existe una política que contemple y respalde el procedimiento descrito en el documento. • No se cuentan con instructivos que enseñen cómo se usan las herramientas tecnológicas que apoyan al sistema. • Los roles y responsabilidades no están documentados en control del proceso. • La metodología de mitigación no se alinea con las buenas prácticas internacionales. • No se encuentran plazos definidos de respuesta a las actividades.

Fuente: Elaboración propia, 2023.

Según lo encontrado en la columna de hallazgos de la Tabla 10 se descubren puntos de mejora a partir de los aspectos que definen limitantes en la documentación que fueron encontrados en el proceso de observación documental.

El primer aspecto para tomar en cuenta está relacionado con la ausencia de categorización de las Vulnerabilidades de Red, lo cual impide una evaluación sobre la gravedad y/o riesgo potencial que la vulnerabilidad generaría. Esta carencia dificulta la asignación de recursos o priorizaciones de acciones en función de las Vulnerabilidades de Red. Otra razón para considerar son los aspectos de priorización en donde una falta de claridad al establecer prioridades para diferentes componentes del sistema limita la capacidad de centrar los esfuerzos en las Vulnerabilidades de Red más críticas.

Así mismo, se encuentra una laguna relacionada al tema de comunicación debido a no poseer un plan o proceso formal para comunicarse durante las fases del ciclo de vida de la vulnerabilidad, especialmente la fase de mitigación y control, en donde existe la posibilidad que ocurra confusión o retrasos. Otro aspecto para considerar es la ausencia de políticas únicas que respalden el procedimiento actual que genera incertidumbre en relación con la autoridad y legitimidad del proceso gestión de Vulnerabilidades de Red. Lo mismo pasa con la definición de los roles y responsabilidades, debido al claro desconocimiento respecto a los encargados, dueños y demás actores pertenecientes al proceso.

La carencia de manuales que detallen cómo emplear las herramientas tecnológicas requeridas obstaculiza la implementación eficaz de la herramienta. Así mismo, se reconoce en el proceso de observación documental la falta de una metodología integral que incorpore evaluaciones minuciosas de las medidas correctivas que tengan la posibilidad de ocasionar lagunas en el sistema de seguridad. Una metodología robusta desempeña un papel esencial en asegurar un abordaje efectivo y completo de las Vulnerabilidades de Red, pues garantizan así la integridad de los procesos de seguridad.

Las limitaciones encontradas en la Tabla 10 resaltan la necesidad de llevar a cabo una evaluación minuciosa y de aplicar mejoras pertinentes al proceso. Estas mejoras ayudarían a hacer frente a los diferentes aspectos encontrados, los cuales se toman como línea base para la construcción del rediseño del proceso de gestión de Vulnerabilidades de Red con mayor eficiencia, organización y capacidad para identificar, mitigar y prevenir Vulnerabilidades de Red en el contexto tecnológico de la entidad.

4.2. Modelado de Procesos *As Is*

En esta sección se ejecuta la fase 2 de la primera etapa del procedimiento metodológico descrito en la sección 0 del documento.

4.2.1. Proceso de Identificar Vulnerabilidades de Red

La Tabla 11 sirve como insumo para realizar el diagrama del proceso As Is. Dicho instrumento permite mostrar la información recolectada en el Apéndice S sobre el proceso de identificar Vulnerabilidades de Red que se ejecuta actualmente en la organización.

Tabla 11 Perfil de Proceso de Identificar Vulnerabilidades de Red

Perfil de Proceso de Identificar Vulnerabilidades de Red	
Objetivo	Actualmente no existe un objetivo claro para la identificación de Vulnerabilidades de Red.
Dueño del proceso	Actualmente no existe una persona o entidad responsable de garantizar que el proceso cumpla.
Cliente	Departamento de *IT Operations and Compliance*.
Expectativas del cliente	Garantizar una identificación rigurosa sobre la alerta de seguridad identificada.
Disparador	Señal de actividad sospechosa generada por la herramienta de monitoreo.
Actividades del proceso	1. El proceso inicia cuando la herramienta de monitoreo IDS genera una señal de actividad sospechosa. 2. El *Security and Monitoring Agent* recibe una señal de actividad sospechosa de la herramienta de monitoreo IDS. 3. El *Security and Monitoring Agent* se encarga de generar un informe específico sobre la señal de actividad sospechosa identificada. a. El informe debe contener: el nombre del evento, tipo de evento, fecha del evento, descripción del evento, y ambiente donde se generó la señal de alerta. 4. El *Security and Monitoring Agent* envía el informe al *Security and Monitoring Manager*. 5. El *Security and Monitoring Manager* genera una aprobación del informe. 6. El *Security and Monitoring Manager* envía el informe al Programador jefe para reportar la actividad sospechosa. 7. El Programador jefe genera una respuesta de aprobación sobre el informe. 8. El Programador jefe envía la respuesta generada. 9. El *Security and Monitoring Manager* recibe la respuesta del Programador jefe.

Perfil de Proceso de Identificar Vulnerabilidades de Red	
	a. Si no se recibe una respuesta de aprobación, se vuelve a enviar el correo al Programador jefe. 10. El *Security and Monitoring Manager* valida las dos aprobaciones del informe generado sobre la señal de actividad sospechosa. 11. El proceso termina cuando el reporte de detección queda validado.
Interfases de entrada	No existen procesos que antecedan al proceso en cuestión.
Interfases de salida	Proceso de Analizar Vulnerabilidades de Red.
Recursos requeridos	Recursos humanos: • *Security and Monitoring Agent.* • *Security and Monitoring Manager*. • Programador jefe. Información, Documentos y Conocimientos: • Informe de la señal de actividad sospechosa. Entorno de Trabajo, Materiales e Infraestructura: • Herramienta *Google Cloud Intrusion Detection System IDS*.
KPIs	No existen métricas relacionadas al proceso.
Observaciones	Datos adicionales: se encuentra en la documentación del proceso, con el nombre Proceso de Identificar y Priorizar Vulnerabilidades de Red, a pesar de que en la ejecución no existe ninguna actividad relacionada con la priorización.

Fuente: Elaboración propia, 2023.

La Tabla 11 permite describir los principales hallazgos a partir del análisis de observación realizado al proceso en el Apéndice S. Los resultados de la observación del proceso establecen que existe un protocolo documentado para identificar Vulnerabilidades de Red. Además, se encuentran brechas con relacionadas a la coordinación entre los participantes del proceso en cuestión. Esto afecta directamente la seguridad de la información, debido a que la falta de coordinación lleva a la duplicación de esfuerzos, retrasos en la detección y respuesta a amenazas, y a la posibilidad de que incidentes de seguridad pasen desapercibidos.

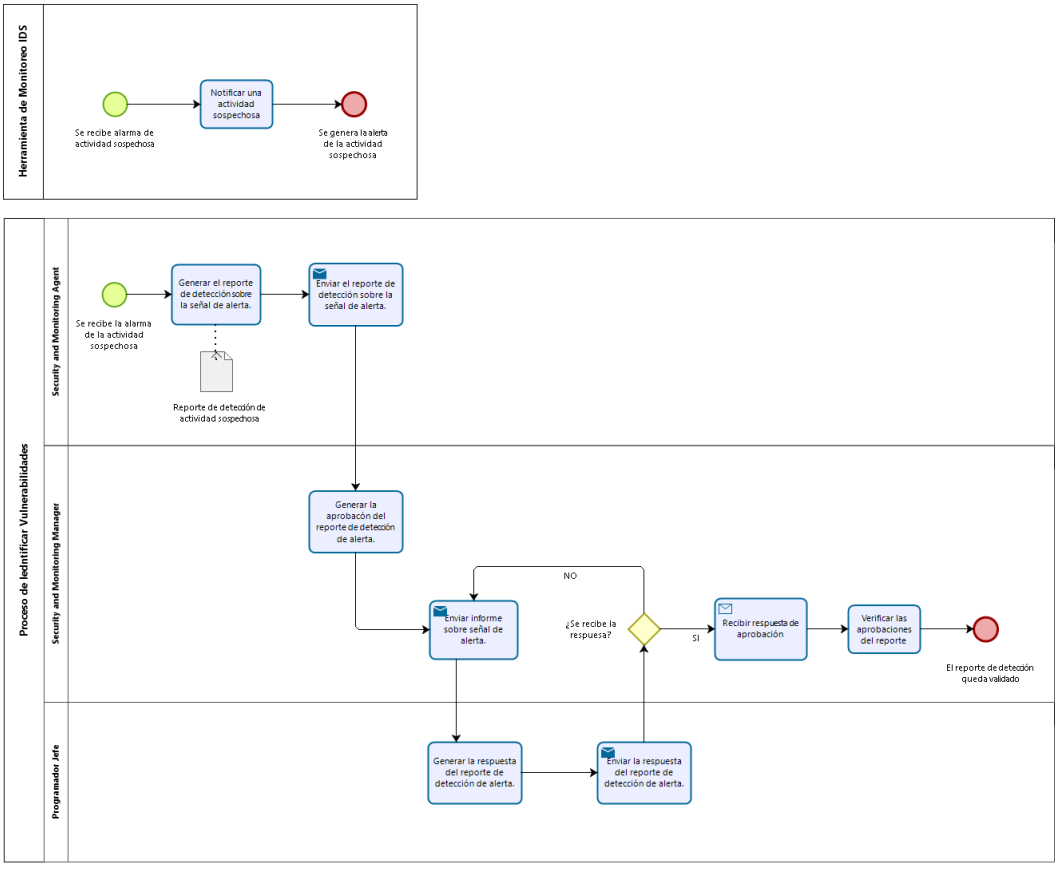
La falta de plazos definidos tiende a dar lugar a retrasos, ambigüedades haciendo una gestión ineficiente del recurso del tiempo. En el contexto del proyecto el retraso en la identificación de Vulnerabilidades de Red aumenta la posibilidad de que la amenaza se concreta o materializa, además dificulta la planificación de etapas posteriores. Otro hallazgo encontrado a partir del instrumento de recolección aplicado en la Tabla 11 al proceso está relacionado con no poseer una definición de criterios de priorización documentada.

Esto genera que al ejecutar el proceso los responsables no sepan qué Vulnerabilidades de Red se deban abordar primero, lo que conlleva a que se desconozca cuáles eventos son menos críticos que otros. Así mismo, este descubrimiento afecta la toma de decisiones para la mitigación, debido a que las Vulnerabilidades de Red que no sean priorizadas adecuadamente tengan la posibilidad de no ser atendidas con los recursos adecuados, de modo que la organización no tiene una asignación de recursos pertinente a cada vulnerabilidad.

Las evidencias encontradas permiten demostrar que la definición de documentos o artefactos relacionados con el proceso no ayuda a crear una visión clara a medida que se ejecuta el proceso, lo que implica un desvío de los lineamientos desarrollados por las buenas prácticas de la industria como lo son NIST, CyBOK, ITIL o PCI.

El análisis de observación aplicado en la Tabla 11 permitió a enriquecer la comprensión sobre las razones detrás de la falta de coordinación entre los responsables del proceso. Según los datos analizados respecto al proceso de identificar y priorizar Vulnerabilidades de Red, se realiza una representación gráfica del proceso utilizando la notición de BPMN 2.0 (Bizagi, 2023), en la Figura 23 para indicar los pasos actuales que se ejecutan.

Figura 23 Proceso As Is Identificar Vulnerabilidades de Red



Fuente: Elaboración propia, 2023.

4.2.2. Proceso de Analizar Vulnerabilidades de Red

La Tabla 12 sirve como entrada para realizar el diagrama del proceso As Is, con el fin de analizar Vulnerabilidades de Red. Los datos para completar dicha tabla se obtuvieron en el Apéndice T.

Tabla 12 Perfil de Proceso de Analizar Vulnerabilidades de Red

Perfil de Proceso de Analizar Vulnerabilidades de Red	
Objetivo	Analizar los componentes del sistema que son afectados directamente por la vulnerabilidad identificada por la herramienta *Google Cloud Intrusion Detection System IDS.*
Dueño del proceso	Actualmente no existe una persona o entidad responsable de garantizar que el proceso cumpla.
Cliente	Departamento de *IT Operations and Compliance*.
Expectativas del cliente	Garantizar un análisis adecuado de los componentes afectados por Vulnerabilidades de Red identificadas.
Disparador	Se recibe el informe aprobado sobre la señal de actividad sospechosa.
Actividades del proceso	1. El proceso inicia cuando *Security and Monitoring Manager* afirma la validación de aprobaciones sobre el informe generado. 2. El *Security and Monitoring Manager* agenda una reunión con Programador jefe y *IT Ops and Compliance Manager* para realizar el análisis de la vulnerabilidad. 3. El Security and Monitoring Manager notifica sobre la reunión. 4. El Programador jefe y *IT Ops and Compliance Manager* reciben la notificación de la reunión. 5. El *Security and Monitoring Manager* se agrupa con el Programador jefe y *IT Ops and Compliance Manager* para realizar el análisis de la vulnerabilidad. a. El informe de análisis consta de investigar a qué componente del sistema afecta de forma directa la vulnerabilidad y definir si afecta o no la operación de la aplicación. 6. El *Security and Monitoring Manager* envía el informe de análisis de la vulnerabilidad al *Chief Technology Officer*, para tener una aprobación. 7. El *Chief Technology Officer* se encarga de tomar la decisión de aprobación. a. En caso de no tener el visto bueno, se solicita una reunión con el *Security and Monitoring Manager* para obtener información con el fin de generar la respuesta. 8. El proceso termina cuando el *Chief Technology Officer* la comunica la respuesta de aprobación.

Perfil de Proceso de Analizar Vulnerabilidades de Red	
Interfases de entrada	Proceso de Identificar Vulnerabilidades de Red.
Interfases de salida	Proceso de Mitigar Vulnerabilidades de Red.
Recursos requeridos	Recursos humanos: • *Security and Monitoring Manager*. • *IT Ops and Compliance Manager* • *Chief Technology Officer*. Información, Documentos y Conocimientos: • Informe aprobado de la señal de actividad sospechosa. Entorno de Trabajo, Materiales e Infraestructura: • Herramienta *Google Cloud Intrusion Detection System IDS.*
KPIs	El proceso no cuenta con KPI´s definidos para su monitoreo.
Observaciones	Datos adicionales: se encuentra que para el análisis se utiliza la herramienta de IDS para encontrar el componente del ambiente afectado.

Fuente: Elaboración propia, 2023.

Según los datos obtenidos con respecto al proceso realizado para analizar Vulnerabilidades de Red demostrados en la Tabla 12, se determina que en dicho protocolo no existe una categorización adecuada de las Vulnerabilidades de Red. Según las recomendaciones de NIST SP 800-40 (Guía de gestión de Vulnerabilidades de Red) explica que:

> El NIST enfatiza la importancia de evaluar y categorizar las Vulnerabilidades de Red en función de su gravedad y urgencia. Esta categorización permite a las organizaciones comprender el impacto potencial de una vulnerabilidad en sus sistemas y datos. (Scarfone K & Souppaya M, 2022, p. 26).

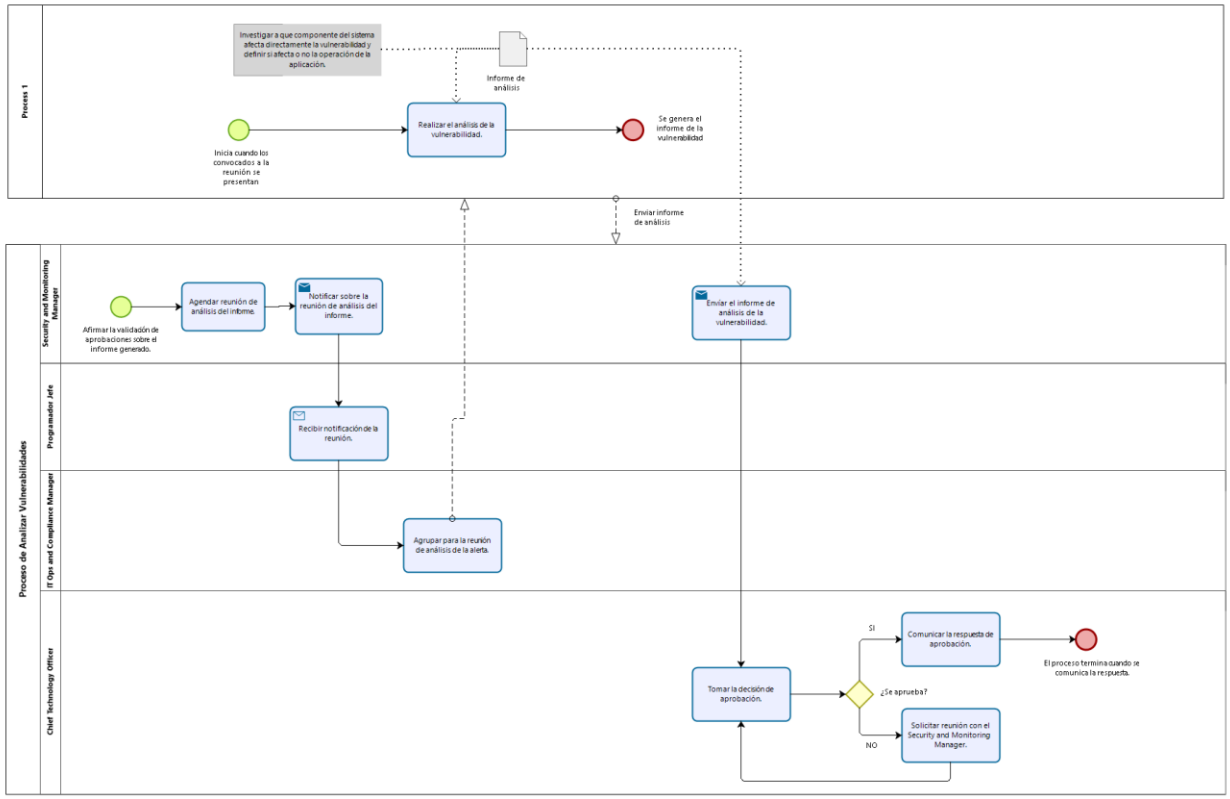
El primer hallazgo permite evidenciar que; sin una categorización adecuada, a la organización le resultará difícil distinguir entre las Vulnerabilidades de Red más urgentes, que deben solucionarse de inmediato y aquellas que no tienen una prioridad de abordarse con urgencia. El segundo es la ausencia de aspectos de priorización de Vulnerabilidades de Red, según los datos obtenidos en el Apéndice T, donde se muestra la falta de documentación sobre los criterios de priorización que la NIST hace referencia.

Esto da como resultado que no se detallen adecuadamente los pasos y aspectos de relevancia necesarios para priorizar los diferentes componentes del sistema que se ven afectados por Vulnerabilidades de Red y que tendrían la oportunidad de poner en riesgo la operación de los procesos críticos de la empresa.

La Tabla 12 refleja el tercer hallazgo el cual se relaciona con la evaluación de las Vulnerabilidades de Red, ya que el proceso sigue un conjunto de pasos que involucran la revisión de alertas, la identificación de los componentes afectados en el sistema, la solicitud de aprobación y la comunicación de la decisión final de la solicitud de aprobación. No obstante, es crucial destacar que la carencia de una adecuada clasificación y priorización de las Vulnerabilidades de Red en este proceso podría llevar a que el *Chief Technology Officer* tome decisiones de aprobación que no sean pertinentes para resolver las Vulnerabilidades de Red que han sido identificadas. Esto, a su vez, podría generar una falta de alineación en la asignación de recursos y en la gestión de riesgos de seguridad de la información dentro de la empresa.

Basándose en la información proporcionada sobre el análisis de datos relacionados con la evaluación y análisis de Vulnerabilidades de Red, la Figura 24 es representación visual del proceso actual utilizando la notación BPMN 2.0.

Figura 24 Proceso As Is de Analizar Vulnerabilidades de Red



Fuente: Elaboración propia, 2023.

4.2.3. Proceso de Mitigar Vulnerabilidades de Red

La Tabla 13 sirve como entrada para realizar el diagrama del proceso As Is de analizar Vulnerabilidades de Red. Los datos para completar la tabla se encuentran en el Apéndice U.

Tabla 13 Perfil de Proceso de Mitigar Vulnerabilidades de Red

Perfil de Proceso de Mitigar Vulnerabilidades de Red	
Objetivo	Mitigar las Vulnerabilidades de Red identificadas por la herramienta *Google Cloud Intrusion Detection System IDS.*
Dueño del proceso	Actualmente no existe una persona o entidad responsable de garantizar que el proceso cumpla.
Cliente	Departamento de *IT Operations and Compliance*.
Expectativas del cliente	Garantizar una mitigación adecuada sobre las Vulnerabilidades de Red identificadas.
Disparador	Se recibe la respuesta de aprobación del *Chief Technology Officer.*
Actividades del proceso	1. El proceso inicia una vez se recibe la respuesta de aprobación del *Chief Technology Officer*. 2. El *Security and Monitoring Manager* y el Programador jefe desarrollan una estrategia de pruebas para la vulnerabilidad. 3. El Programador jefe se encarga de realizar las pruebas de mitigación. 4. El *IT Ops and Compliance Manager* se encarga de supervisor las pruebas de mitigación. 5. El *IT Ops and Compliance Manager* se encarga de crear un reporte de mitigación sobre los puntos clave obtenidos en las pruebas realizadas. a. El reporte contiene: nombre de la vulnerabilidad, componente que fue afectado, estrategia establecida, herramienta utilizada, fecha de pruebas y hallazgos. 6. El Programador jefe valida que se haya mitigado la vulnerabilidad. a. Si no, se vuelve a generar las pruebas de mitigación. b. Si se mitiga, se informa al *Security and Monitoring Manager* con el reporte de pruebas de mitigación realizado. 7. El *Security and Monitoring Manager* aprueba el reporte y lo envía al *IT Ops and Compliance Manager.* 8. El proceso termina cuando *IT Ops and Compliance Manager*, el reporte de pruebas de mitigación se sube al gestor de conocimiento de la empresa (Confluence).
Interfases de entrada	Proceso de Analizar Vulnerabilidades de Red.
Interfases de salida	No existe un proceso consecuente al proceso en cuestión.

Perfil de Proceso de Mitigar Vulnerabilidades de Red	
Recursos requeridos	Recursos humanos: • *Security and Monitoring Manager*. • *IT Ops and Compliance Manager* • *Programador Jefe.* Información, Documentos, Conocimientos: • Informe aprobado de la señal de actividad sospechosa. • Informe de análisis sobre los componentes afectos por Vulnerabilidades de Red identificadas. Entorno de Trabajo, Materiales, Infraestructura: • Gestor de conocimiento de la empresa (*Confluence*)
KPI's	El proceso actualmente no cuenta con KPI´s definidos para su monitoreo.
Observaciones	Datos adicionales:

Fuente: Elaboración propia, 2023.

La Tabla 13 sirve como insumo para describir los resultados obtenidos de la aplicación del instrumento en el Apéndice U. Con base en los resultados de la situación actual del proceso de mitigar Vulnerabilidades de Red, se encuentran una serie de problemas relacionados con la ejecución de dicho proceso en la organización.

El primer hallazgo está relacionado con la falta de una metodología alineada con las buenas prácticas de la industria (NIST, CyBOK, PCI e ITIL) que complete y abarque las pruebas de corrección. Esta carencia implica que la organización no cuenta con un enfoque estructurado para abordar las Vulnerabilidades de Red, lo que podría dar lugar a enfoques improvisados y menos eficientes en el proceso de corrección. Esto, a su vez, aumenta el riesgo de pasar por alto pasos esenciales o que las soluciones implementadas no se evalúen adecuadamente, lo que podría resultar en la persistencia de Vulnerabilidades de Red no abordadas o en soluciones incompletas.

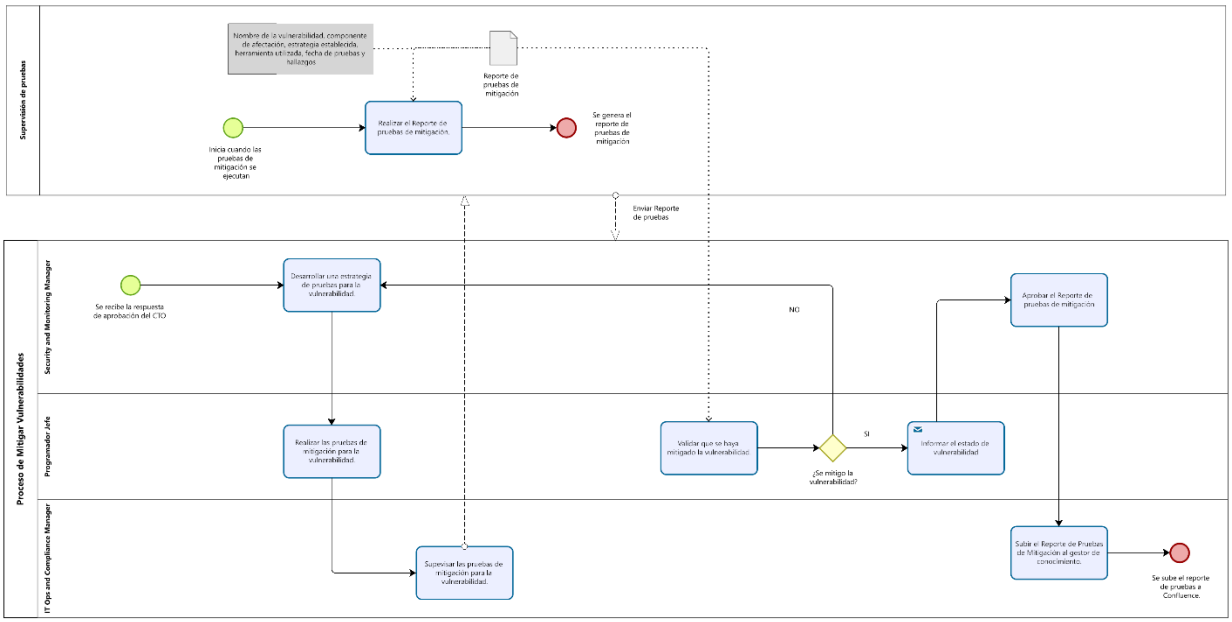
La segunda evidencia encontrada se relaciona con la ausencia de documentación esencial, como manuales de usuario o guías técnicas, referente al manejo de las herramientas disponibles en la organización para el trato de Vulnerabilidades de Red. Este hallazgo es un aspecto importante que afecta el conocimiento del personal. Sin la debida orientación y capacitación, existe la posibilidad de que los miembros del equipo utilicen estas herramientas de manera errónea, lo que podría tener un impacto negativo en la precisión de las pruebas y en la eficacia global del proceso de mitigación.

El tercer hallazgo encontrado se encuentra relacionado con el anterior y se ejemplifica en la utilización incorrecta de la herramientas o técnicas de exploración de Vulnerabilidades de Red que tienen la posibilidad ocasionar la aparición de resultados incorrectos, ya sean falsos positivos o falsos negativos. Esto tiene un impacto directo en la gestión de recursos de la organización.

Por último, se destaca que la falta de un enfoque en la implementación de parches de seguridad es otro aspecto para tomar en consideración. La omisión de la puesta en práctica de parches de seguridad durante el proceso de mitigación da lugar a incoherencias en la seguridad de los componentes de los sistemas. Aplicar parches es un paso esencial para cerrar Vulnerabilidades de Red que ya son conocidas y para mantener los sistemas en un estado actualizado y seguro.

Utilizando los datos obtenidos en la Tabla 13, se elabora una representación gráfica del proceso actual de mitigación. Para este propósito, se utiliza la notación BPMN 2.0, como se muestra en la Figura 25. Esta representación visual detalla las etapas que actualmente se implementan en el proceso.

Figura 25 Proceso As Is de Mitigar Vulnerabilidades de Red



Fuente: Elaboración propia, 2023.

4.3. Análisis de los Procesos

En este apartado, se establece la aplicación de análisis cualitativos y cuantitativos de los procesos elegidos.

4.3.1. Análisis del Proceso de Identificar Vulnerabilidades de Red

Para comprender mejor los aspectos que se deben considerar para la propuesta de solución, se explorarán tres enfoques esenciales el análisis de valor añadido, el análisis de desperdicios y el análisis de flujo.

4.3.1.1 Análisis de valor añadido

Para realizar el análisis se utilizarán las actividades descritas en la Figura 23.

Tabla 14 Análisis Valor Agregado Proceso de Identificar

ID	Actividad	VA	BVA	NVA
1	La herramienta de monitoreo IDS detecta actividad sospechosa.	X		
1.1	La herramienta de monitoreo notifica una actividad sospechosa.		X	
1.2	La herramienta de monitoreo IDS genera una señal de actividad sospechosa	X		
2	El *Security and Monitoring Agent* recibe una señal de la actividad sospechosa.	X		
3	El *Security and Monitoring Agent* se encarga de generar informe de la actividad sospechosa.	X		
4	El *Security and Monitoring Agent* se encarga de enviar el informe de la activada sospechosa al *Security and Monitoring Manager*.	X		
5	El *Security and Monitoring Manager* genera una aprobación del informe.	X		
6	El *Security and Monitoring Manager* envía el informe al Programador jefe para reportar la actividad sospechosa.	X		
7	El Programador jefe genera una respuesta de aprobación sobre el informe.	X		
8	El *Security and Monitoring Manager* recibe la respuesta del Programador jefe.	X		
9.1	El *Security and Monitoring Manager* recibe la respuesta del Programador jefe.	X		
9.2	Si no se recibe una respuesta de aprobación, se vuelve a enviar el correo al Programador jefe.	X		
10	El *Security and Monitoring Manager* validan las dos aprobaciones del informe generado sobre la señal de actividad sospechosa.	X		
11	El proceso termina cuando el reporte de detección queda validado.	X		

Fuente: Elaboración propia, 2023.

La Tabla 14 revela que varias etapas en este proceso de identificación de Vulnerabilidades de Red son esenciales para garantizar una respuesta efectiva ante las amenazas de seguridad.

- Las actividades marcadas como "VA" son esenciales y contribuyen significativamente al proceso de identificar Vulnerabilidades de Red al agregar valor real.

- Las actividades marcadas como "VBA" son tareas que agregan valor, pero se podría eliminar o simplificarse para aumentar la eficiencia del proceso de identificación de Vulnerabilidades de Red.
- No se identifican etapas como "NAV" en el flujo del proceso de identificación de Vulnerabilidades de Red, ya que todas las etapas parecen contribuir de alguna manera al proceso.

4.3.1.2 Análisis de desperdicios

Para realizar el análisis de desperdicios se utilizan las actividades de la Figura 23.

Tabla 15 Análisis de Desperdicios Proceso de Identificar

Act	Transporte innecesario	Movimiento	Tiempo de Espera	Inventario	Errores	Sobreproducción	Sobre procesar
1							
1.1		X					
1.2							
2	X						
3				X			
4		X					
5				X			
6		X					
7				X			
8		X					
9			X				
9.1			X				
9.2							X
10			X				
11				X			

Fuente: Elaboración propia, 2023.

La Tabla 15 muestra los hallazgos sobre el proceso de identificación de Vulnerabilidades de Red en relación con los principios Lean descritos por (Goldsby & Martichenko, 2005) sobre la reducción de desperdicios:

- Transporte innecesario: se evidencia en la actividad dos del procedimiento muestra este tipo de desperdicio. Esto sugiere que existen formas de mover información o documentos que podrían ahorrar tiempo y recursos al reducir la necesidad de transporte.
- Movimiento: las actividades uno, cuatro, seis y ocho evidencian este tipo de desperdicio, como hallazgo se evidencia que existe la posibilidad reducir el movimiento innecesario de personas o información, las tareas podrían simplificarse o eliminarse.

- Tiempo de espera: las evidencias nueve y diez detectan el tiempo de espera. Esto muestra que existen tiempos de espera para aprobaciones o respuestas que podrían acortarse mejorando la comunicación o los flujos de trabajo.
- Inventario: la información que espera la aprobación se acumula en las actividades tres, cinco y siete como inventario.
- Sobre procesamiento: la actividad nueve punto uno genera reproceso del trabajo en caso de no recibir una respuesta.

Según el análisis realizado en la Tabla 15, se revela numerosas oportunidades para reducir el desperdicio y aumentar la efectividad del proceso de identificación de vulnerabilidad .

4.3.1.3 Análisis de flujo

El propósito de este análisis es explorar en detalle la comparación entre el tiempo de ciclo y la eficiencia en el proceso de identificación de Vulnerabilidades de Red; para esto se utiliza la herramienta de simulación de Bizagi con el fin de realizar el análisis de flujo se utilizarán los hallazgos descritos en el Apéndice S.

Tabla 16 Análisis de Flujo del Proceso de Identificar

Name	Type	Instances completed	Instances started	Min. time	Max. time	Avg. time	Total time	Total fixed cost
Proceso de Iedntificar Vulnerabilidades	Process	100	100	11h 45m	1d 21h 45m	15h 58m 30s	66d 13h 30m	17,432.46
Se recibe la alarma de la actividad sospechosa	Start event	100						
Generar el reporte de detección sobre la señal de alerta.	Task	100	100	3h 10m	3h 10m	3h 10m	13d 4h 40m	1,600
El reporte de detección queda validado	End event	100						
Generar la aprobacón del reporte de detección de alerta.	Task	100	100	3h	3h 20m	3h 24s	12d 12h 40m	1,227
Enviar el reporte de detección sobre la señal de alerta.	Task	100	100	15m	15m	15m	1d 1h	4,000
Enviar informe sobre señal de alerta.	Task	198	198	30m	1h 20m	30m 56s	4d 6h 5m	2,429.46
Generar la respuesta del reporte de detección de alerta.	Task	198	198	3h	5h 30m	3h 3m 1s	25d 4h	3,168
¿Se recibe la respuesa?	Gateway	198	198					
Verificar las aprobaciones del reporte	Task	100	100	1h 15m	1h 45m	1h 15m 18s	5d 5h 30m	1,227
Enviar la respuesta del reporte de detección de alerta.	Task	198	198	30m	3h 30m	34m 14s	4d 17h	3,168
Recibir respuesta de aprobación	Task	100	100	5m	1h 5m	6m 21s	10h 35m	613
ExclusiveGateway	Gateway	198	198					

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

Con base en los datos recopilados en la Tabla 16, se efectuarán los cálculos necesarios para analizar el ciclo de vida del proceso de identificación de Vulnerabilidades de Red y evaluación de su eficacia. Según la Tabla 16 muestra que el tiempo mínimo de identificar Vulnerabilidades de Red sea de 11h 45m haciendo que se tome más de un día laboral en el mejor de los casos. Esto hace que la eficiencia del tiempo no respalde la asignación de costos de los recursos utilizados en el proceso ya que según lo mostrado en la Tabla 16 se tiene un costo fijo aproximado del proceso de $17,432.46.

4.3.2. Análisis del Proceso de Analizar Vulnerabilidades de Red

Para comprender mejor los aspectos que se deben considerar para la propuesta de solución del proceso de analizar Vulnerabilidades de Red, se explorarán tres enfoques esenciales el análisis de valor añadido, el análisis de desperdicios y el análisis de flujo.

4.3.2.1 Análisis de valor añadido

Para realizar el análisis de valor añadido se usan las actividades descritas en la Figura 24.

Tabla 17 Análisis Valor Agregado Proceso de Analizar

ID	Actividad	VA	BVA	NVA
1	El proceso inicia cuando *Security and Monitoring Manager* afirma la validación de aprobaciones sobre el informe generado.	X		
2	El *Security and Monitoring Manager* agenda una reunión con el Programador jefe y el *IT Ops and Compliance Manager* para realizar el análisis de la vulnerabilidad.		X	
3	El *Security and Monitoring Manager* notifica sobre la reunión.		X	
4	El Programador jefe y el *IT Ops and Compliance Manager* reciben la notificación de la reunión.			X
5	El *Security and Monitoring Manager* se reúne con el Programador jefe y el *IT Ops and Compliance Manager* para realizar el análisis de la vulnerabilidad.	X		
5.1	El informe de análisis consta de investigar a qué componente del sistema afecta directamente la vulnerabilidad y definir si afecta o no la operación de la aplicación.	X		
6	El *Security and Monitoring Manager* envía el informe de análisis de la vulnerabilidad al *Chief Technology Officer*, para tener una aprobación.	X		
7	El *Chief Technology Officer* se encarga de tomar la decisión de aprobación.	X		
7.1	En caso de no tener aprobación, se solicita una reunión con el *Security and Monitoring Manager* para obtener información con el fin de generar la respuesta.		X	

ID	Actividad	VA	BVA	NVA
8	El proceso termina cuando el *Chief Technology Officer* comunica la respuesta de aprobación.	X		

Fuente: Elaboración propia, 2023.

La Tabla 17 contempla los resultados del análisis realizado basado en el flujo del proceso de analizar Vulnerabilidades de Red. De esta manera, se encuentra que:

- Las etapas uno, cinco, cinco punto uno, seis, siete y ocho marcadas como "VA" son actividades que son esenciales y contribuyen significativamente al proceso al agregar valor real.
- Las etapas dos, tres y siete punto uno marcadas como "VBA" son tareas que agregan valor, pero que se podrían eliminar o simplificarse para aumentar la eficiencia del proceso.
- La etapa cuatro se identifica como etapa "NAV" (No Agrega Valor) en este flujo.

4.3.2.2 Análisis de desperdicios

Para realizar el análisis en cuestión se ejecutan las actividades descritas en la Figura 24.

Tabla 18 Análisis de Desperdicios Proceso de Analizar

Act	Transporte innecesario	Movimiento	Tiempo de Espera	Inventario	Errores	Sobreproducción	Sobre procesar
1			X				
2	X	X	X				
3	X		X				
4							
5	X	X	X			X	
5.1				X			
6		X					
7			X				
7.1		X				X	
8			X				

Fuente: Elaboración propia, 2023.

Según los resultados obtenidos en la Tabla 18 sobre los desperdicios del proceso de analizar Vulnerabilidades de Red en relación con los principios Lean descritos por (Goldsby & Martichenko, 2005) se evidencia que:

- Transporte innecesario: se demuestra que las etapas dos, tres y cinco del proceso presentan este tipo de desperdicio, al hacer referencia al uso alternativo de formas de mover información o documentos que podrían ahorrar tiempo.

- Movimiento: las etapas dos, cinco, seis puntos uno muestra un movimiento innecesario de personas o información; las tareas podrían automatizarse o simplificarse para evitar el desperdicio.
- Tiempo de espera: las etapas uno, dos, tres, cinco, siete y ocho están relacionadas con tiempos de espera para aprobaciones o respuestas que podrían acortarse implementando estrategias de comunicación efectivas.
- Inventario: la etapa cinco punto uno genera el informe de análisis, esta implica que sea información que debe esperar la aprobación.
- Sobre procesamiento: las etapas cinco y siete generan reproceso del trabajo en caso de no recibir una respuesta.

El análisis realizado en la Tabla 18 identificó múltiples áreas en donde existe la posibilidad de reducir desperdicios y mejorar la eficiencia del proceso de análisis de Vulnerabilidades de Red.

4.3.2.3 Análisis de flujo

El propósito de este análisis es evidenciar el contraste entre el ciclo temporal y tiempo de espera para el proceso en cuestión. El Apéndice T permite evaluar los tiempos del flujo de trabajo.

Tabla 19 Tabla Análisis de Flujo del Proceso de Analizar

Name	Type	Instances completed	Instances started	Min. time	Max. time	Avg. time	Total time	Total fixed cost
Proceso de Analizar Vulnerabilidades	Process	173	174	6h 50m	2d 18h 20m	11h 37m 11s	83d 18h 15m	9,767.66
Afirmar la validación de aprobaciones sobre el informe generado.	Start event	100						
Agendar reunión de análisis del informe.	Task	100	100	1h 10m	1h 30m	1h 14m	5d 3h 20m	1,227
Notificar sobre la reunión de análisis del informe.	Task	100	100	3h 35m	3h 35m	3h 35m	14d 22h 20m	122
Recibir notificación de la reunión.	Task	100	100	5m	5m	5m	8h 20m	133
Agrupar para la reunión de análisis de la alerta.	Task	100	100	2h	2h	2h	8d 8h	3,600
Envíar el informe de análisis de la vulnerabilidad.	Task	73	74	20m	20m	20m	1d 20m	302.66
Tomar la decisión de aprobación.	Task	140	140	7h	7h	7h	40d 20h	2,520
¿Se aprueba?	Gateway	140	140					
Comunicar la respuesta de aprobación.	Task	73	73	2h	2h	2h	6d 2h	657
Solicitar reunión con el Security and Monitoring Manager.	Task	67	67	2h 30m	4h 55m	2h 32m 9s	7d 1h 55m	1,206
El proceso termina cuando se comunica la respuesta.	End event	73						

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

Según los resultados obtenidos de la Tabla 19 se encuentra que, el proceso de análisis de Vulnerabilidades de Red tiene la posibilidad de finalizar en promedio 11 horas y 37 minutos en completarse. El costo fijo aproximado del proceso es $9,767.66 y representa una métrica crucial para la gestión de recursos y presupuesto.

4.3.3. Análisis del Proceso de Mitigar Vulnerabilidades de Red

Para obtener una comprensión más profunda de los elementos que deben ser tenidos en cuenta al proponer una solución, se investigarán tres enfoques clave: el análisis del valor agregado, la evaluación de las ineficiencias y el estudio del flujo de trabajo.

4.3.3.1 Análisis de valor añadido

Para realizar el análisis de valor añadido se usan las actividades descritas en la Figura 25.

Tabla 20 Análisis Valor Agregado Proceso de Mitigar

ID	Actividad	VA	BVA	NVA
1	Recibir la respuesta de aprobación del *Chief Technology Officer*		X	
2	El *Security and Monitoring Manager* y el Programador jefe desarrollan una estrategia de pruebas para la vulnerabilidad	X		
3	El Programador jefe realiza las pruebas de mitigación.	X		
4	El *IT Ops and Compliance Manager* supervisa las pruebas de mitigación.	X	X	
5	El *IT Ops and Compliance Manager* crea un reporte sobre los puntos clave obtenidos en las pruebas realizadas.	X		
6	El Programador jefe valida que se haya mitigado la vulnerabilidad.	X		
6.1	Si no, se vuelve a generar las pruebas de mitigación.	X		
6.2	Si se mitiga, se informa al *Security and Monitoring Manager* con el reporte de pruebas de mitigación realizado.	X		
7	El *Security and Monitoring Manager* aprueba el reporte y lo envía al *IT Ops and Compliance Manager*.		X	
8	El proceso termina cuando *IT Ops and Compliance Manager*, sube el reporte de pruebas de mitigación al gestor de conocimiento de la empresa (Confluence).	X		

Fuente: Elaboración propia, 2023.

Según los resultados obtenidos en la Tabla 20 sobre el análisis de valor añadido se encuentra que el proceso tiene las siguientes actividades:

- La activad uno demuestra que el valor agregado es mínimo porque el proceso simplemente se inicia sin exposición directa a la vulnerabilidad.

- La actividad dos sí agrega valor al proceso, ya que planifica una estrategia de acción concreta para abordar la vulnerabilidad.
- La actividad tres implica una acción directa para abordar las Vulnerabilidades de Red, en cuanto que agrega un valor significativo al proceso y al negocio.
- La actividad cuatro se identifica que, aunque esta fase no agrega valor directo a la mitigación de Vulnerabilidades de Red, es importante desde una perspectiva de gobernanza y cumplimiento.
- La actividad cinco aporta valor, ya que documenta los resultados y proporciona información importante para la toma de decisiones.
- La actividad seis es importante, en la medida en la que asegura que la vulnerabilidad se haya abordado de manera efectiva. Si no se ha mitigado, se vuelve a la etapa 2 para desarrollar una nueva estrategia de pruebas, lo que suma valor al proceso de mejora continua.
- La actividad siete aporta valor al garantizar que los resultados estén disponibles para futuras referencias y aprendizaje organizacional.

4.3.3.2 Análisis de desperdicios

Las actividades presentes en la Figura 25 serán empleadas en el análisis de ineficiencias.

Tabla 21 Análisis de Desperdicios Proceso de Mitigar

Act	Transporte innecesario	Movimiento	Tiempo de Espera	Inventario	Errores	Sobreproducción	Sobre procesar
1							
2			X				
3			X				
4			X				
5			X				
6			X				
6.1			X				
6.2			X				
7	X						
8	x			X			

Fuente: Elaboración propia, 2023.

Con base en los resultados obtenidos en la Tabla 21 respecto al desperdicio en los procesos de análisis de vulnerabilidad relacionados con los principios Lean (Goldsby & Martichenko, 2005), queda claro que:

- La actividad uno no genera desperdicios significativos, ya que el proceso arranca de forma lógica después de obtener la aprobación necesaria.

- Las actividades de dos a siete (planificación y ejecución de pruebas) se caracterizan por períodos de espera largos y movimientos innecesarios.
- La actividad cinco a pesar de agregar valor al proceso al crear un informe detallado sobre los aspectos claves de las pruebas, podría generar un inventario innecesario de informes o su mala gestión.
- La actividad seis, muestra que es importante para validar las restricciones de vulnerabilidad, esta etapa tiene la posibilidad de realizar transiciones innecesarias.

4.3.3.3 Análisis de flujo

La aplicación de este análisis a partir de los datos del Apéndice U, muestra la comparación entre el tiempo de ciclo y el tiempo de espera del proceso de mitigación de Vulnerabilidades de Red.

Tabla 22 Análisis de Flujos Proceso de Mitigar

Name	Type	Instances completed	Instances started	Min. time	Max. time	Avg. time	Total time	Total fixed cost
Proceso de Mitigar Vulnerabilidades	Process	465	466	1h 35m	19h 30m	9h 53m 22s	191d 14h 40m	23,850.72
Se recibe la respuesta de aprobación del CTO	Start event	100						
Supevisar las pruebas de mitigación para la vulnerabilidad.	Task	276	276	4h 10m	4h 10m	4h 10m	47d 22h	9,936
Realizar las pruebas de mitigación para la vulnerabilidad.	Task	276	276	5h 30m	7h 30m	5h 49m 33s	67d	4,416
Desarrollar una estrategia de pruebas para la vulnerabilidad.	Task	276	276	3h 30m	7h	4h 22m 21s	50d 6h 50m	6,773.04
Validar que se haya mitigado la vulnerabilidad.	Task	365	366	50m	50m	50m	12d 16h 10m	1,950.78
¿Se mitigo la vulnerabilidad?	Gateway	365	365					
Informar el estado de vulnerabilidad	Task	189	189	5m	5m	5m	15h 45m	251.37
Aprobar el Reporte de pruebas de mitigación	Task	189	189	35m	4h	1h 34m 39s	12d 10h 10m	230.58
Subir el Reporte de Pruebas de Mitigación al gestor de conocimiento.	Task	189	189	5m	5m	5m	15h 45m	292.95
Se sube el reporte de pruebas a Confluence.	End event	189						

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

Estos datos sugieren una relación potencial con la cantidad y complejidad de las Vulnerabilidades de Red. La duración promedio de la actividad es de aproximadamente 9 horas y 53 minutos, lo que indica un enfoque cuidadoso en cada paso del proceso. El rango de tiempos de

espera es de 40 minutos hasta y 1 hora 25 minutos, apunta a posibles cuellos de botella o retrasos en la asignación de recursos. Los costos fijos aproximados asociados son $23,850.72 y cubren diversos recursos.

4.4. Análisis de Brechas

El presente apartado se examina las brechas presentes en la situación actual, a fin de comprender a fondo la dinámica de la gestión de Vulnerabilidades de Red y sus implicaciones. Mediante el uso del Apéndice J, el cual fue aplicado al *IT Ops and Compliance Manager* y al *Security and Monitoring Manager* en la Tabla 23, se definen las brechas existentes entre la situación actual de la gestión de Vulnerabilidades de Red y los estándares internacionales.

Este análisis aborda diversos aspectos cruciales, entre ellos: la evaluación de la situación actual de la gestión de Vulnerabilidades de Red, el diseño del proceso de gestión de Vulnerabilidades de Red en uso, los componentes que conforman el plan de gestión del proceso y el desarrollo de un modelo de indicadores clave de desempeño (KPI) que permita medir y monitorear eficazmente la efectividad de las prácticas implementadas.

Tabla 23 Tabla Análisis de Brecha

Variable	Contextualización	Estado Actual	Estado Ideal
Variable 1 Situación actual de la gestión de Vulnerabilidades de Red.	Capacidad de identificar Vulnerabilidades de Red.	Como se evidenció en la sección 4.1.1 la organización tiene dificultades para identificar y evaluar de manera efectiva las Vulnerabilidades de Red en sus sistemas y aplicaciones.	Según lo indicado por el *IT Ops and Compliance Manager* y el *Security and Monitoring Manager* se deben implementar procedimientos y entrenamiento adecuado para el personal encargado de la identificación de Vulnerabilidades de Red.
	Contexto organizacional.	Según los hallazgos descubiertos en la sección 4.1.2, se muestra que gestión de Vulnerabilidades de Red no cuenta con un protocolo claro de comunicación en la organización, lo que genera a una falta de apoyo y recursos.	En cuanto a los estándares de la industria mencionan, se debe desarrollar un programa de concienciación en seguridad cibernética que informe a los empleados sobre los riesgos y la importancia de la gestión de Vulnerabilidades de Red en el contexto de la

Variable	Contextualización	Estado Actual	Estado Ideal
			organización. (Hallet & Chen, 2021; Scarfone K & Souppaya M, 2022)
	Nivel de conformidad de los estándares.	De acuerdo con los resultados obtenidos en la sección 4.1.3 se establece que la organización no cumple completamente con los estándares de seguridad reconocidos, lo que pone en riesgo la integridad de la información.	(Hallet & Chen, 2021; Scarfone K & Souppaya M, 2022) establecen que de acuerdo con las buenas prácticas de la industria se debe llevar a cabo un análisis para identificar las áreas de no conformidad con los estándares reconocidos y tomar medidas de acción.
	Documentación del proceso.	Como se observó en la sección 4.1.4 se demuestra que la documentación actual es limitada y no proporciona una guía completa para el proceso de gestión de Vulnerabilidades de Red.	De acuerdo con los autores Burnap, (2019); Scarfone K., Souppaya M, (2022) es necesario crear una documentación que incluya descripciones detalladas de cada fase del proceso, procedimientos paso a paso y formularios de para cada etapa.
Variable 2 Marco de trabajo de la Gestión de Vulnerabilidades de Red.	Definición de roles y responsabilidades en la gestión de Vulnerabilidades de Red.	Los resultados obtenidos en la sección 4.1.2 demuestran que existe interacción entre diferentes actores en el proceso, estos no se encuentran debidamente documentados, lo que genera que ninguno de los procesos analizados tenga un dueño del proceso.	Según el CyBOK y NIST SP 800-40 respectivamente mencionan que es necesario establecer funciones concretas que se alineen a la ejecución de cada una de las etapas del ciclo de vida de las Vulnerabilidades de Red.

Variable	Contextualización	Estado Actual	Estado Ideal
	Alineación con Estándares de Seguridad Reconocidos.	Los resultados que se obtuvieron de la aplicación del Apéndice P sección 4.1.3, evidencian que dentro la organización, se está pasando por un proceso de certificación por ende se busca que el proceso de Vulnerabilidades de Red se adapte o se cumpla según las mejores prácticas internacionales.	Según lo indicado por el *IT Ops and Compliance Manager y al Security and Monitoring Manager* se debe realizar una revisión completa del proceso para garantizar su alineación con estándares internacionales, esto implica que se tenga una base de conocimiento propio sobre las Vulnerabilidades de Red.
Variable 3 Componentes del plan de gestión del proceso.	Componentes del plan de gestión del proceso.	De acuerdo con los hallazgos del Apéndice P, pregunta 4 la organización enlista el conjunto de componentes esenciales que se deben incorporar en el plan de gestión de Vulnerabilidades de Red.	De acuerdo con las buenas prácticas de la industria se deben desarrollar, métricas de rendimiento claras y alineadas con los objetivos específicos para evaluar el éxito de los componentes pertenecientes al proceso de gestión de Vulnerabilidades de Red. (Hallet & Chen, 2021; Scarfone K & Souppaya M, 2022)
Variable 4 Modelo de indicadores claves de desempeño (KPI).	Indicadores de desempeño	En el Apéndice P, pregunta 2 y 7 se evidencia la actual presentada de la organización sobre este tema no dispone de un conjunto de indicadores de rendimiento para evaluar y medir el proceso de gestión de Vulnerabilidades de Red.	(Organización de los Estados Americanos (OEA), 2019; PCI Security Standards Council, 2022; Scarfone K & Souppaya M, 2022) definen que la gestión de Vulnerabilidades de Red enfatiza la importancia de establecer KPI's que se adecuen a su ciclo de vida.

Fuente: Elaboración propia, 2023.

5. Propuesta de Solución

En el presente capitulo se busca poner en práctica la propuesta de la solución al problema presentado en el primer capítulo. Además, este capítulo pretende abordar todas las oportunidades de mejora encontradas en el Análisis de Resultados. De esta forma, el capítulo en cuestión permite ejecutar las fases cuatro, cinco, seis y siete definidas en el Procedimiento metodológico de la investigación, con el objetivo de definir un proceso de Gestión de Vulnerabilidades de Red que se alinee a las buenas prácticas de la industria y que sirva como línea base y herramienta a la organización para solventar las amenazas que vayan a ser tratadas.

5.1. Diseño de la Solución

En este apartado se presenta la ejecución de la fase cuatro y cinco definidas en el apartado 3.9 referente al Procedimiento metodológico de la investigación las cuales buscan crear el rediseño del proceso de Gestión de Vulnerabilidades de Red que se ejecuta actualmente en la organización. En este contexto, se identificarán las oportunidades de mejoras, para definir los perfiles de procesos “To Be”. Estas mejoras también tienen como propósito considerar las herramientas con las que cuenta la organización, así como una correcta definición de roles y responsabilidades para garantizar la alineación de este proceso con los estándares de la industria pertinentes.

5.1.1. Identificación de las oportunidades de mejoras de los procesos

El insumo obtenido de los hallazgos de los apéndices S, T, U se encuentra en la Tabla 24, la cual determina los puntos que son considerados para el rediseño del proceso de Gestión de Vulnerabilidades de Red.

Tabla 24 Oportunidades de Mejoras

Proceso	Hallazgo	Oportunidad de Mejora
Identificar Vulnerabilidades de Red	El Apéndice S evidencia los siguientes hallazgos: No existe coordinación entre los dueños del proceso y las actividades. No hay una definición de plazos de respuesta en el proceso. No existen objetivos claros que definan el proceso. Desperdicios se centran en inventario y movimiento.	A continuación, se muestran las oportunidades de mejora: Establecer plazos de respuesta, para la reducción de tiempos de espera. Establecer pasos para una comunicación más efectiva, de las actividades del proceso. Definir el dueño del proceso además de los roles y responsabilidades de los actores.

Proceso	Hallazgo	Oportunidad de Mejora
Analizar Vulnerabilidades de Red	El Apéndice T evidencia los hallazgos sobre el proceso en cuestión: El documento no tiene definido una categorización de Vulnerabilidades de Red, por ende, dicho proceso no se concreta en su ejecución. No se encuentran fijados los aspectos de priorización de Vulnerabilidades de Red para los diferentes componentes del sistema. Actualmente no existe una persona o entidad responsable de garantizar que el proceso cumpla. El proceso no cuenta con KPI´s definidos para su monitoreo. Se encuentran desperdicios relacionados con el tiempo de espera.	A continuación, se definen las oportunidades de mejora en relación con las evidencias de la columna de hallazgos: Instaurar una categorización que se adecua a las necesidades de la empresa. Añadir el sistema de priorización de Vulnerabilidades de Red, para definir la estrategia de abordaje según el nivel de prioridad asignado. Definir el dueño del proceso además de los roles y responsabilidades de los actores. Determinar KPIs.
Mitigar Vulnerabilidades de Red	El Apéndice U muestra los hallazgos sobre el proceso en cuestión: No existe una metodología alineada a las buenas prácticas de la industria para la mitigación que englobe las pruebas de mitigación. No hay documentación (manuales de usuario o guías técnicas) acerca del uso de las herramientas con las que cuenta la organización. El uso inadecuado de las herramientas. Desperdicio de reprocesos y tiempo de espera.	A continuación, se definen las oportunidades de mejora en relación con las evidencias de la columna de hallazgos: Crear un proceso de Mitigación alineado a las buenas prácticas. Desarrollar documentación detallada que brinde orientación sobre cómo aprovechar la documentación de herramientas. Mejorar los conocimientos y las habilidades en el uso de herramientas de exploración de Vulnerabilidades de Red. Consideración de parches de seguridad. Definir el dueño del proceso además de los roles y responsabilidades.

Fuente: Elaboración propia, 2023.

5.1.2. Componentes de la Solución

En la presente sección se describen los componentes que debe poseer la propuesta de la solución y que fueron mencionados por el CTO y el *IT Ops and Compliance Manager* en la pregunta cuatro del Apéndice P. Según las especificaciones brindadas por los sujetos de investigación sobre los elementos que se deben considerar se encuentra que dichos elementos forman parte de las fases del ciclo de vida de la gestión de Vulnerabilidades de Red detallada en el Marco Conceptual.

Bajo esta premisa, la solución que se propone en este apartado se origina como resultado no solo del periodo ejecución del trabajo final de graduación, sino también las experiencias vividas trabajando en proyectos anteriores de Symbiotic, y de las necesidades descritas en el primer capítulo, junto con los hallazgos de mejoras evidenciados en apartados anteriores.

La propuesta busca definir un marco de trabajo que sirva como una base sólida para la gestión de Vulnerabilidades de Red de TI y que se alinee con las buenas prácticas de la industria descritas en el Marco Conceptual. Dicho marco de trabajo aborda las oportunidades de mejora encontradas en el análisis de los procesos pertenecientes a las fases del ciclo de vida de Vulnerabilidades de Red que se ejecutan actualmente en la organización, así como la asignación de los recursos humanos, la definición de un plan de comunicación y por último la definición de un catálogo de KIP's para el control y seguimiento de los procesos que se ejecutan en dichas fases.

5.1.2.1. Política de Gestión de Vulnerabilidades de Red

El apartado se presenta la creación del documento referente la política para la gestión de Vulnerabilidades de Red desarrollada para Symbiotic (ver Anexo IV). Este documento tiene como objetivo establecer las bases de trabajo, las cuales el departamento de IT Operations and Compliance junto con el equipo de seguridad a cargo de Symbiotic define como los planes y mecanismos de acción para el control de Vulnerabilidades de Red.

Con la implementación de este marco de trabajo la organización busca que se ejecute un modelo genérico de gestión de Vulnerabilidades de Red alineado a las buenas prácticas de la industria, alineado con los estándares de NIST SP 800-40 y el CyBOK. Este documento presenta varias secciones relativas a la gestión de la temática, las cuales van a ser abordadas detalladamente para el proceso de cumplimiento.

Así mismo, el marco de trabajo definido en este documento busca simplificar la toma de decisiones efectivas en circunstancias en las que podría ser difícil alcanzar los objetivos de tecnología de la información que se vean afectados por la presencia de Vulnerabilidades de Red, lo que en última instancia podría perjudicar el logro de los objetivos comerciales. A continuación, se presenta la Tabla 25, la cual permite dar descripciones a los apartados de la política que se abordan en el Anexo IV., y ver cómo estas posibilitan la alineación con las buenas prácticas de la industria relacionadas con la gestión de Vulnerabilidades de Red.

Tabla 25 Apartados de la Política

Apartado	Descripción
Objetivo	En esta sección se establece el objetivo del marco de trabajo para la gestión de Vulnerabilidades de Red en Symbiotic, así mismo se marca el estándar de la industria por seguir.
Alcance	Esta sección refuerza la importancia que tienen las prácticas de ciberseguridad de la organización, mientras aplica las recomendaciones de los estándares de la industria.
Definiciones	Se detallan términos claves relacionados con la gestión.
Roles y Responsabilidades	Detalla los roles y responsabilidades para la Gestión de Vulnerabilidades de Red, incluyendo el *Security and Monitoring Manager*, *IT Ops and Compliance Manager*, y otros.
Capacitación en Conciencia de Seguridad	Describe las medidas que Symbiotic considera importante para capacitar a los empleados en seguridad.
Revisión de la Política	En esta sección se establecen los periodos de tiempo para las revisiones de la política o aplicación de cambios relacionados con esta.
Cumplimiento de la Política	El apartado define las acciones disciplinarias por incumplimiento.
Reconocimiento de la Política	El apartado detalla cómo los trabajadores y partes interesadas deben declarar formalmente que conocen y están de acuerdo con la política.
Niveles de Disponibilidad	Especifica los niveles de disponibilidad del servicio de su aplicación. Los niveles de disponibilidad que Symbiotic considera relevantes como bajo, medio y alto.
Sistema de Categorización	En esta sección, se establece un sistema de categorización basado en la evaluación de la importancia de los componentes del sistema de Symbiotic (Ver Anexo IV, Tabla I)
Sistema de Priorización	En este apartado se definen los criterios de impacto y probabilidad para priorizar Vulnerabilidades de Red (Ver Anexo IV, Tablas II y III)
Estatutos aplicables al Procedimiento de la Gestión	Define regulaciones internas y aspectos por considerar para la ejecución de los procedimientos que pertenecen a la gestión de Vulnerabilidades de Red en Symbiotic.

Fuente: Elaboración propia, 2023.

La Tabla 25 resume los aspectos que se desarrollaron para definir la normativa interna de Symbiotic relacionada con la gestión de Vulnerabilidades de Red. Este documento facilita establecer un marco estructurado que abarque las etapas del ciclo de vida de las Vulnerabilidades de Red y las causas de la problemática en el apartado 1.3.1.

Así mismo, se establecen secciones que permiten ayudar a solventar la problemática relacionada con el desconocimiento alrededor de los niveles de disponibilidad, la categorización de componentes y los criterios de priorización de Vulnerabilidades de Red.

5.1.2.2. Plan de Comunicación de Gestión de Vulnerabilidades de Red

El documento definido en el Anexo V hace referencia al plan de comunicación de Vulnerabilidades de Red de Symbiotic. Dicho documento es un componente importante para una estrategia eficaz de gestión ya que ayuda a comunicar los riesgos asociados a las Vulnerabilidades de Red del software.

Dicho documento ayuda a solventar la causa de la problemática relacionada con los desafíos de comunicación y coordinación existentes en el proceso de gestión de Vulnerabilidades de Red, descrito en la sección 1.3.1.. La Tabla 26 proporciona a modo resumen los apartados que se consideraron para el desarrollo del plan.

Tabla 26 Resumen Plan de Comunicación

Apartado	Descripción
Resumen del Plan	En este apartado se define el plan de comunicación de Vulnerabilidades de Red de Symbiotic para mitigar riesgos asociados al software.
Enfoque de Comunicación	La sección define la importancia de la comunicación en las etapas del ciclo de vida de las Vulnerabilidades de Red y define el enfoque de comunicación que Symbiotic desea utilizar para esta práctica.
Planificación de la Estrategia	El apartado establece las diferentes estrategias de comunicación que se deben utilizar según el tipo de información que se debe compartir con los involucrados ya sean altos mandos, colaboradores o departamentos.
Roles y Responsabilidades	Detalla los roles y responsabilidades para la Gestión de Vulnerabilidades de Red, incluyendo el personal clave.
Proceso de Manejo de Comunicación	Este apartado permite detallar las actividades que se consideran en el proceso de manejo de comunicación de Vulnerabilidades de Red, desde la notificación hasta la resolución.
Canales de Comunicación	La sección permite definir los canales de comunicación oficiales que se utilizarán de manera interna en Symbiotic para la notificación de las Vulnerabilidades de Red. Así mismo, se establece que tipo de comunicación se enviará de acuerdo con el canal definido.
Plan de Reuniones	El plan de reuniones permite enumerar las reuniones incluidas en la gestión de Vulnerabilidades de Red, sus asistentes y la finalidad de cada una de ellas.
Plazos de Respuesta	El apartado establece cuáles son los plazos de respuesta de ciertas actividades que se contemplan en los procedimientos establecidos para la gestión de Vulnerabilidades de Red, desde la notificación hasta la aprobación.
Políticas de Divulgación	La sección plantea las normas para la divulgación de información relacionada con la gestión de Vulnerabilidades de Red.

Fuente: Elaboración propia, 2023.

5.1.2.3. Material de Entrenamiento para el Personal

El siguiente apartado establece el material de entrenamiento diseñado para fortalecer el proceso de gestión de Vulnerabilidades de Red en Symbiotic. Dicho material incluye varios elementos esenciales que garantizan una formación integral.

En primer lugar, está la Política de Gestión de Vulnerabilidades de Red, que sirve como línea base para todas las actividades relacionadas con el proceso en cuestión. El Anexo Xmuestra la presentación realizada para la política permite al personal de Symbiotic visualizar los principios y pautas que se deben seguir para mantener la integridad y confidencialidad de los datos y garantizar la disponibilidad de los servicios ofrecidos por Symbiotic.

Figura 26 Material de Entrenamiento de la Política

Fuente: Elaboración propia, 2023.

En línea con la Política de Gestión de Vulnerabilidades de Red, el material de formación incluye la presentación relacionada con el catálogo de KPI, definido en el Anexo XI. Este material busca garantizar que el personal de Symbiotic tenga consciencia de que las prácticas de seguridad implementadas se miden y evalúan por los indicadores de desempeño establecidos.

La presentación ofrece una visión concisa y cuantitativa de la situación de seguridad de la información de la empresa, lo que permite la toma de decisiones informadas y la detección temprana de oportunidades de mejora.

Figura 27 Material de Entrenamiento Catálogo de KPI's

Fuente: Elaboración propia, 2023.

El último material de entrenamiento realizado se encuentra relacionado con el plan de comunicación de Vulnerabilidades de Red. El Anexo XII busca detallar al personal involucrado en el proceso en la estrategia para informar de manera efectiva y rápida las Vulnerabilidades de Red identificadas.

Figura 28 Material de Entrenamiento Plan de Comunicación

Fuente: Elaboración propia, 2023.

Los materiales de entrenamiento desarrollados desempeñan un papel crucial en la gestión de vulnerabilidades al proporcionar una estructura educativa y un conjunto de recursos que fortalecen la comprensión y la ejecución efectiva de los procesos de seguridad. En conclusión, los materiales educativos diseñados para mejorar el proceso de gestión de las vulnerabilidades de red de Symbiotic son un conjunto completo de materiales que abordan aspectos clave.

5.1.2.4. Rediseño y Modelado de los Procesos

En esta sección se detallan las acciones propuestas para el rediseño y modelado de los procesos, las cuales representan las fases cuatro y cinco del procedimiento metodológico descrito en la sección 0, así mismo, abarcan el ciclo de vida de la gestión de Vulnerabilidades de Red que se ejecutan actualmente en la organización.

Para el rediseño de los procesos que se realizan en el departamento *de IT Operations and Compliance* de Symbiotic, se toman en consideración las buenas prácticas de la industria, las herramientas de la organización, la asignación del personal y la documentación pertinente a estos procesos. De modo que, para el desarrollo de este componente de la solución, se han examinado los siguientes aspectos:

- Revisión documental y literaria realizada en el Capítulo II de este proyecto, que hace referencia al Marco Conceptual, sobre las buenas prácticas de la gestión de Vulnerabilidades de Red.
- La situación actual de la gestión que se analizó en el Capítulo IV el cual detalla el Análisis de Resultados obtenidos sobre el estudio de la problemática de la organización.
- Retroalimentación por parte de los Sujetos de investigación que formaron parte del presente proyecto.
- Áreas de mejora las cuales fueron identificadas en la sección 0.

A continuación, se detallan las directrices sugeridas para cada una de las actividades pertenecientes para el ciclo de vida de Vulnerabilidades de Red. Estos aspectos permiten indicar las acciones que los responsables definidos en la sección 5.1.2 Política de Gestión de Vulnerabilidades de Red, deben seguir con el fin de ejecutar de manera estándar las actividades.

5.1.2.2.1 Proceso de Identificación

En esta sección se detallan todas aquellas actividades relacionadas con el proceso de identificación de Vulnerabilidades de Red. Para el rediseño del proceso toma en consideración la sección 4.3.1 la cual hace referencia al análisis del proceso en cuestión, así mismo se usa el Apéndice S como puntos de inicio para establecer el rediseño del proceso y su respectiva representación gráfica.

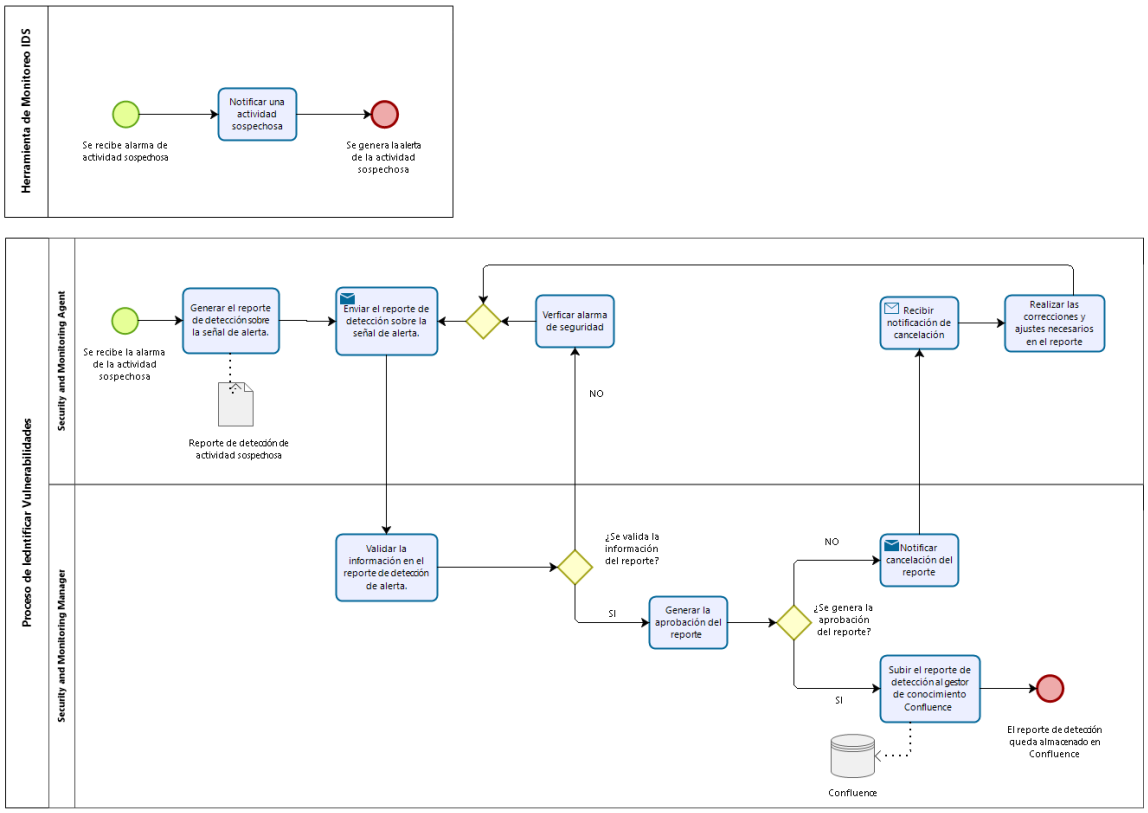
Rediseño del proceso

En este apartado, se propone el flujo de trabajo para el proceso de identificación de Vulnerabilidades de Red a partir del uso de la herramienta de *Intrusion Detection System (IDS)* de Google. El flujo se ha diseñado con la idea de asegurar que todas las señales de actividad sospechosa sean identificadas, documentadas y comunicadas de manera oportuna.

El Anexo VII presenta la documentación del procedimiento tomando en cuenta aspectos relevantes definidos en la Tabla 12 vinculada al perfil del proceso de Identificación de Vulnerabilidades de Red y la Tabla 24 la cual permite evidenciar las oportunidades de mejoras específicas para el proceso. El documento descrito en el Anexo VII permite describir un método organizado para identificar y manejar las alertas de seguridad enviadas por las herramientas del Sistema de Detección de Intrusiones en la nube (IDS) de Google.

La Figura 29, muestra una representación visual simplificada de las actividades del proceso basado en el uso de en BPMN 2.0.

Figura 29 Proceso "To Be" Identificación



Fuente: Realización propia 2023.

Simulación del proceso To Be

En este apartado se ejecuta la simulación del proceso To Be bajo las mismas condiciones del proceso As Is de Identificar Vulnerabilidades de Red.

Figura 30 Resultados Simulación To Be Identificación Vulnerabilidades de Red

Name	Type	Instances completed	Instances started	Min. time	Max. time	Avg. time	Total time
Proceso de Iedntificar Vulnerabilidades	Process	100	100	1h 52m	2d 52m	10h 47m 40s	44d 23h 27m
Se recibe la alarma de la actividad sospechosa	Start event	100					
Generar el reporte de detección sobre la señal de alerta.	Task	100	100	37m	3h 32m	44m 46s	3d 2h 38m
Generar la aprobación del reporte	Task	175	175	25m	55m	26m 54s	3d 6h 30m
Subir el reporte de detección al gestor de conocimiento Confluence	Task	100	100	15m	40m	16m 12s	1d 3h
Verficar alarma de seguridad	Task	205	205	2h	4h 30m	2h 1m 29s	17d 7h 6m
¿Se valida la información del reporte?	Gateway	380	380				
¿Se genera la aprobación del reporte?	Gateway	175	175				
El reporte de detección queda almacenado en Confluence	End event	100					
Notificar cancelación del reporte	Task	75	75	5m	35m	6m 20s	7h 55m
Recibir notificación de cancelación	Task	75	75	5m	2h	9m 44s	12h 10m
Realizar las correcciones y ajustes necesarios en el reporte	Task	75	75	3h	3h 5m	3h 16s	9d 9h 20m
Validar la información en el reporte de detección de alerta.	Task	380	380	30m	55m	30m 38s	8d 2h 3m
Enviar el reporte de detección sobre la señal de alerta.	Task	380	380	5m	2h 5m	7m 3s	1d 20h 45m
ExclusiveGateway	Gateway	280	280				

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

Como se muestra en la Figura 30, el tiempo mínimo requerido para completar una instancia es de 1 hora y 52 minutos, mientras que el tiempo máximo es de 2 días y 52 minutos, y el tiempo promedio es de aproximadamente 10 horas, 47 minutos y 40 segundos por instancia. Los resultados obtenidos de los tiempos mínimos, máximos, promedios y total del proceso disminuyo en comparación con los resultados obtenidos en la Tabla 16.

Tabla 27 Costos del Proceso To Be Identificación de Vulnerabilidades de Red

Nombre	Tiempo Mínimo	Tiempo Máximo	Tiempo Promedio	Tiempo Total	Costos fijo total
Proceso de Identificación de Vulnerabilidades de Red	1h 52m	2d 52m	10h 47m 40s	44d 23h 27m	$8,046.08

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

La Tabla 27 muestra que el costo fijo aproximado es de $8,046.08, mientras que la Tabla 28 recalca la disminución de tiempos entre el proceso As Is y el proceso To Be de la siguiente manera:

Tabla 28 Comparación de Tiempos Identificación de Vulnerabilidades de Red

Tiempo	As Is	To Be	Diferencia	Porcentaje
Mínimo	11h 45m	1h 52m	9h 53m de ahorro	Ahorro del 84.68%
Máximo	1d 21h 45m	2d 0h 52m	0d 3h 7m aumento de tiempo	Aumento del 6.52%
Promedio	15h 58m	10h 47m	5h 11m de ahorro de tiempo	Ahorro del 32.38%
Total	66d 13h 30m	44d 23h 27m	21d 14h 3m de ahorro de tiempo	Ahorro del 34.58%

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

Creación del reporte de detección

En esta sección se establece el proceso para completar el Apéndice Z *Symbiotic Vulnerability Detection Report* el cual define la plantilla para el reporte de detección creado para dar una descripción detallada de los eventos de identificación de Vulnerabilidades de Red. Este informe sirve como medio para registrar y difundir información sobre incidentes o posibles amenazas a la seguridad que deben abordarse. La plantilla descrita en el Apéndice Z consta de varios apartados los cuales serán descritos a continuación:

Información de alerta de vulnerabilidad: esta sección contiene datos sobre la alerta de vulnerabilidad, por ejemplo: el nombre o título único que identifica el evento, el tipo de alerta que indica la categoría o clasificación del evento (incidente de seguridad, error del sistema, violación de acceso), la fecha y hora exacta del evento, así como el lugar preciso donde se generó la alerta.

Descripción de la alerta: este apartado proporciona una descripción detallada del incidente con el objetivo de comprender la naturaleza y el alcance de la vulnerabilidad o incidente.

Información sobre los involucrados: se enumeran las personas involucradas en el hecho. Además, incluye información de contacto de los participantes, lo que facilita la comunicación y la colaboración para resolver el problema.

Aprobación: Finalmente, esta sección se utiliza para obtener la aprobación y firma del supervisor o gerente correspondiente; esto indica que el informe ha sido revisado y se han tomado las medidas adecuadas para abordar la vulnerabilidad o el incidente.

En resumen, el propósito del informe establecido en el Apéndice Z es registrar y reportar eventos relacionados con la detección de Vulnerabilidades de Red, brindando a los gerentes de seguridad de la información una perspectiva integral de los eventos, las personas involucradas y las medidas implementadas o necesarias para abordar el control de la situación.

Comunicación con el equipo del trabajo

En este apartado se define cómo se llevará a cabo la comunicación entre los responsables del proceso de identificación de Vulnerabilidades de Red. Para esto se utilizará como base el protocolo establecido en la política de gestión definida en el Anexo V, perteneciente al Plan de Comunicación de Vulnerabilidades de Red definido en apartados anteriores.

Es por ello que se establece el uso de la estrategia de envío de información. El Apéndice Z *Symbiotic Vulnerability Detection Report* permite a los responsables del proceso conocer cómo notificar la actividades de relacionadas a la identificación de Vulnerabilidades de Red entre los involucrados. Este enfoque tiene como objetivo facilitar la implementación de cambios y el uso de herramientas para los empleados.

Alineación con los estándares de la industria

Para realizar la alineación con los estándares de la industria se toma como base lo evidenciado en la sección 5.1.1, que presenta las oportunidades de mejora el proceso de Identificación de Vulnerabilidades de Red, además, para esto (Scarfone K & Souppaya M, 2022, p. 23) explican que;

> Las organizaciones utilizar al menos uno de los siguientes tipos de recursos para monitorear Vulnerabilidades de Red y amenazas:
>
> 1. Herramienta de gestión de parches empresarial para obtener todos los parches disponibles de proveedores compatibles.
> 2. Sitio de seguridad de proveedores y lista de correo para obtener todos los parches disponibles de proveedores que no son compatibles con las herramientas de administración de parches empresariales.
> 3. Una base de datos de Vulnerabilidades de Red o lista de correo que proporciona información actualizada sobre todas las Vulnerabilidades de Red conocidas y soluciones recomendadas. (Scarfone K & Souppaya M, 2022, p. 23)

A partir de lo explicado por (Scarfone K & Souppaya M, 2022) y lo analizado en el capítulo de Análisis de Resultados se encuentra que Symbiotic utiliza la herramienta de Google IDS. Esta herramienta permite que el proceso siga lo establecido con la fase de identificación y monitoreo de NIST SP 800-40. La herramienta realiza un monitoreo continuo de la infraestructura en busca de Vulnerabilidades de Red u otras actividades inusuales que tengan la posibilidad ser una amenaza a la seguridad.

Según Google (2023) explica que la herramienta *Intrusion Detection System* desempeña un papel fundamental ya que permite la detección inmediata de posibles intrusiones o comportamientos inusuales y emite alertas sobre las amenazas identificadas. Además, la funcionalidad de la herramienta examina el tráfico de la red y los registros de actividad en los diferentes componentes del sistema de Symbiotic para identificar patrones y eventos inusuales que tienen la posibilidad de indicar amenazas a la seguridad.

Además de manejar alertas de seguridad y validar datos de las amenazas, el proceso To Be definido para la solución está estructurado y documentado, esto permite aplicar las mejores prácticas recomendadas de la industria proporcionando un enfoque integral para la gestión de Vulnerabilidades de Red.

5.1.2.2.2 Proceso de Análisis y Priorización

En esta sección se detallan los aspectos que fueron encontrados en el proceso de análisis de Vulnerabilidades de Red. Para ello se toma en consideración la sección 4.3.2 la cual hace referencia al análisis del proceso en cuestión, así mismo se usa el Apéndice T como puntos de inicio para establecer el rediseño del proceso y su respectiva representación gráfica.

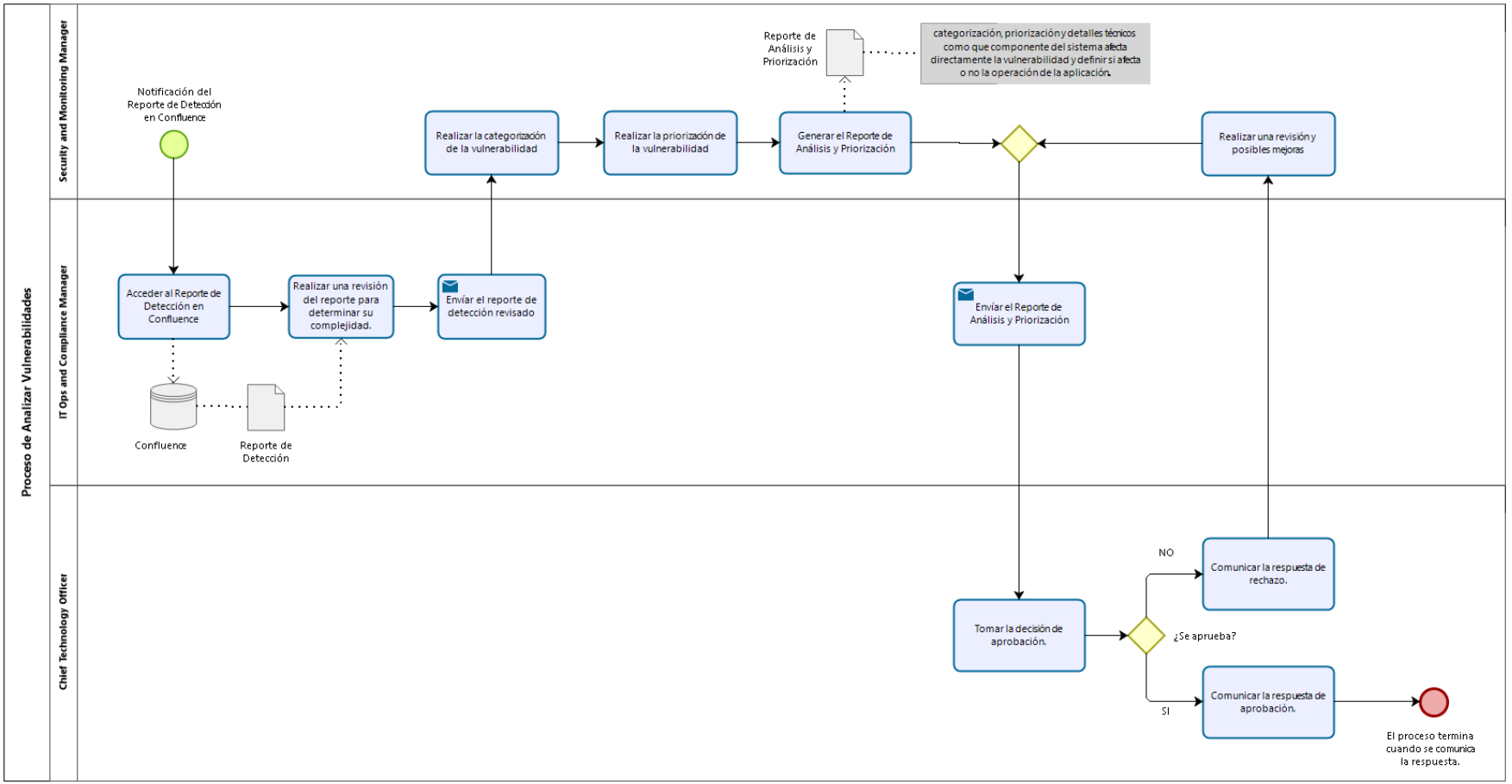
Rediseño del proceso

El flujo del proceso To Be de Analizar y Priorizar se ha diseñado con la idea de asegurar que todos los reportes de las señales de actividad sospechosa sean categorizados, priorizados, documentados y comunicados de manera oportuna. La Tabla 24 evidencia las oportunidades de mejoras específicas para el proceso.

El documento presentado en el Anexo VIII categoriza y prioriza los componentes del sistema que se ven directamente afectados por las Vulnerabilidades de Red descubiertas mediante la herramienta de IDS. El archivo presenta un sistema que garantice que todos los informes de actividades sospechosas se clasifiquen, prioricen, documenten completamente y se comuniquen de manera oportuna.

Este proceso está diseñado para mejorar la capacidad de Symbiotic para abordar de manera proactiva las Vulnerabilidades de Red y fortalecer su postura de ciberseguridad. La Figura 31, es una representación visual de las actividades proceso de Analizar y Priorizar Vulnerabilidades de Red basado en el uso de la notación de BPMN 2.0.

Figura 31 Proceso "To Be" Analizar y Priorizar



Fuente: Elaboración propia, 2023.

Simulación del proceso

En este apartado se ejecuta la simulación del proceso To Be bajo las mismas condiciones del proceso As Is de Analizar Vulnerabilidades de Red.

Figura 32 Resultados Simulación To Be Analizar y Priorizar Vulnerabilidades de Red

Name	Type	Instances completed	Instances started	Min. time	Max. time	Avg. time	Total time
Proceso de Analizar Vulnerabilidades	Process	100	100	5h 45m	1d 55m	8h 42m 6s	36d 6h 10m
Acceder al Reporte de Detección en Confluence	Task	100	100	10m	10m	10m	16h 40m
Envíar el Reporte de Análisis y Priorización	Task	177	177	5m	5m	5m	14h 45m
Tomar la decisión de aprobación.	Task	177	177	2h 30m	2h 30m	2h 30m	18d 10h 30m
¿Se aprueba?	Gateway	177	177				
Comunicar la respuesta de rechazo.	Task	77	77	15m	15m	15m	19h 15m
Comunicar la respuesta de aprobación.	Task	100	100	15m	15m	15m	1d 1h
El proceso termina cuando se comunica la respuesta.	End event	100					
Generar el Reporte de Análisis y Priorización	Task	100	100	40m	40m	40m	2d 18h 40m
Realizar una revisión del reporte para determinar su complejidad.	Task	100	100	1h	1h	1h	4d 4h
Envíar el reporte de detección revisado	Task	100	100	5m	5m	5m	8h 20m
Realizar la categorización de la vulnerabilidad	Task	100	100	45m	45m	45m	3d 3h
Realizar la priorización de la vulnerabilidad	Task	100	100	15m	15m	15m	1d 1h
Realizar una revisión y posibles mejoras	Task	77	77	1h	1h	1h	3d 5h
ExclusiveGateway	Gateway	177	177				
Notificación del Reporte de Detección en Confluence	Start event	100					

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

Los resultados de la figura anterior demuestran que el tiempo mínimo requerido para completar una instancia es de 5 horas y 45 minutos, mientras que el tiempo máximo es de 1 día y 55 minutos, mientras que el tiempo promedio es de aproximadamente 8 horas, 42 minutos y 6 segundos por instancia.

Así mismo, la Tabla 29 permite realizar los cálculos correspondientes al costo fijo aproximado siendo un total de $8,514.03.

Tabla 29 Costos del Proceso To Be Análisis y Priorización de Vulnerabilidades de Red

Nombre	Tiempo Mínimo	Tiempo Máximo	Tiempo Promedio	Tiempo Total	Costos fijo total
Proceso de Analizar de Vulnerabilidades de Red	5h 45m	1d 55m	8h 42m 6s	36d 6h 10m	$8,514.03.

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

El uso de la Tabla 30 describe la comparación de Tiempos Análisis y Priorización de Vulnerabilidades de Red entre el modelo As Is y el modelo To Be.

Tabla 30 Comparación de Tiempos Análisis y Priorización de Vulnerabilidades de Red

Tiempo	As Is	To Be	Diferencia	Porcentaje
Mínimo	6h 50m	5h 45m	1h 5m de ahorro	Ahorro del 15.94%
Máximo	2d 18h 20m	1d 0h 55m	1d 17h 25m de ahorro	Ahorro del 53.09%
Promedio	11h 37m	8h 42m	2h 55m de ahorro de tiempo	Ahorro del 25.06%
Total	83d 18h 15m	36d 6h 10m	47d 12h 5m de ahorro de tiempo	Ahorro del 57.05%

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

Creación del Reporte de Análisis

La siguiente sección detalla el instructivo para rellenar la propuesta del reporte de análisis presentado en el

Apéndice AA. Este informe sirve como medio para categorizar, priorizar y distribuir la información sobre las Vulnerabilidades de Red que deben abordarse. La plantilla descrita en el

Apéndice AA consta de varios apartados, los cuales serán descritos a continuación:

Análisis de la vulnerabilidad: en esta sección el reporte define datos relacionados con la vulnerabilidad como el "nombre de alerta". El "tipo de alerta" describe la clasificación o categoría bajo el cual se categoriza la vulnerabilidad ya sea, como incidente de seguridad, error del sistema, violación de acceso u otro. Posteriormente la "descripción de la alerta" concluye dando un relato breve de la vulnerabilidad tomado del Reporte de Detección de Señal de Alerta.

Categorización de la vulnerabilidad: este apartado establece el uso del sistema de categorización que se definió en la sección 5.1.2 Política de Gestión de Vulnerabilidades de Red, el cual se fundamenta en la comprensión del nivel de importancia de los componentes del sistema, de modo que permite a las partes responsables del proceso priorizar de manera más rápida y eficiente.

Priorización de la vulnerabilidad: dicha sección realiza el proceso de priorización, definido en el apartado 5.1.2 Política de Gestión de Vulnerabilidades de Red, el cual utiliza el estándar "*ASINZS 4360: 1999 Risk Management*" del Council of Standards Australia (2003) como base.

Información adicional: este apartado brinda comentarios o información extra relevante sobre la vulnerabilidad para etapas posteriores.

Aprobación: Por último, pero no menos importante, esta sección se utiliza para obtener la aprobación y firma del gerente o supervisor correspondiente. Esto procedimiento demuestra que el informe ha sido examinado y que se han tomado las medidas adecuadas para abordar la vulnerabilidad o el incidente.

El propósito del

Apéndice AA es brindar instrucciones para orientar en la creación del informe de análisis de vulnerabilidad, adaptado a las necesidades específicas descritas. Por esta razón proporciona explicaciones claras de las secciones que lo conforman, además de incluir los detalles de la vulnerabilidad, la categorización, la priorización y la aprobación.

Este documento tiene como objetivo garantizar que los informes de análisis sean completos, precisos y estándarizados, facilitando una gestión eficaz de la vulnerabilidad en el contexto de Symbiotic. De esta manera, el escrito realizado en el

Apéndice AA, se convierte en una herramienta esencial para documentar y comunicar de manera efectiva eventos de detección de Vulnerabilidades de Red.

Comunicación con el equipo del trabajo

Esta unidad describe cómo se comunican entre sí los responsables del proceso de detección de Vulnerabilidades de Red. Para ello se seguirá el protocolo definido en el Anexo V que forma parte del Plan de Comunicación de Vulnerabilidad.

Este proceso se basa en la Política de envío de información e incluye la distribución del Reporte de Análisis y Priorización de Vulnerabilidades de Red de Symbiotic descrito en el

Apéndice AA, El personal responsable de este proceso debe comunicarse a través del sistema de correo electrónico Symbiotic. Además, los administradores de seguridad y monitoreo

recibirán notificaciones mediante el envío de mensajes de la plataforma de Slack, el cuál es el medio oficial de comunicación interno de Symbiotic.

Alineación con los estándares de la industria

En esta sección, se define la alineación del proceso con los estándares de la industria por esta razón se utilizan como insumos los hallazgos encontrados en el apartado 5.1.1. Para el flujo del proceso que se ha presentado como parte de la solución se utiliza las recomendaciones dadas por (Scarfone K & Souppaya M, 2022). A continuación, se describen los aspectos que los autores establecen para estructurar de manera íntegra el proceso To Be de analizar Vulnerabilidades de Red.

> La evaluación de la vulnerabilidad incluiría lo siguiente: Determinar la importancia de la amenaza o vulnerabilidad. Determinar qué sistemas son vulnerables o expuestos, centrándose en operaciones críticas y otros sistemas de alta prioridad. Analizar los efectos en la organización, la red y el sistema en caso de que la vulnerabilidad no se solucione y explote. (Scarfone K & Souppaya M, 2022, p. 23)

Según con lo explicado por los autores y lo evidenciado en el análisis, se establece que la primera oportunidad de mejora está relacionada con la categorización de las Vulnerabilidades de Red. En este caso se desarrolló todo un sistema de clasificación que se detalle en la política de Gestión de Vulnerabilidades de Red de la sección 5.1.2. Dicho sistema permite que Symbiotic pueda categorizar la vulnerabilidad según el componente del sistema en que se encuentra.

Posteriormente, se definió un sistema de priorización de acuerdo con las necesidades definidas por la empresa. De acuerdo con el *Security and Monitoring Manager* y el *IT Ops and Compliance Agent* se busca priorizar según los criterios de impacto y probabilidad. Para ello se emplea como base el estándar *ASINZS 4360: 1999 Risk Management* definido por el Council of Standards Australia (2003).

Por último, también se establece una plantilla para el reporte de análisis, la cual permite mejorar la comunicación entre las diferentes partes interesadas del proceso, destacando la importancia de la alta dirección en las decisiones críticas de gestión de Vulnerabilidades de Red.

5.1.2.2.3 Proceso de Mitigación

Esta sección describe los elementos identificados en el análisis del proceso evidenciados en el apartado 4.2.3 que incluye la evaluación del proceso en cuestión. Adicionalmente, el Apéndice U sirve como punto de partida para iniciar el rediseño del proceso de mitigación y su correspondiente representación visual.

Rediseño del proceso

El Anexo IX define el nuevo flujo desarrollado para el proceso en cuestión. El procedimiento de mitigación que se describe tiene como objetivo abordar eficazmente las Vulnerabilidades de Red identificadas a través del sistema IDS de Google, al mismo tiempo que se adhiere a las mejores prácticas del sector.

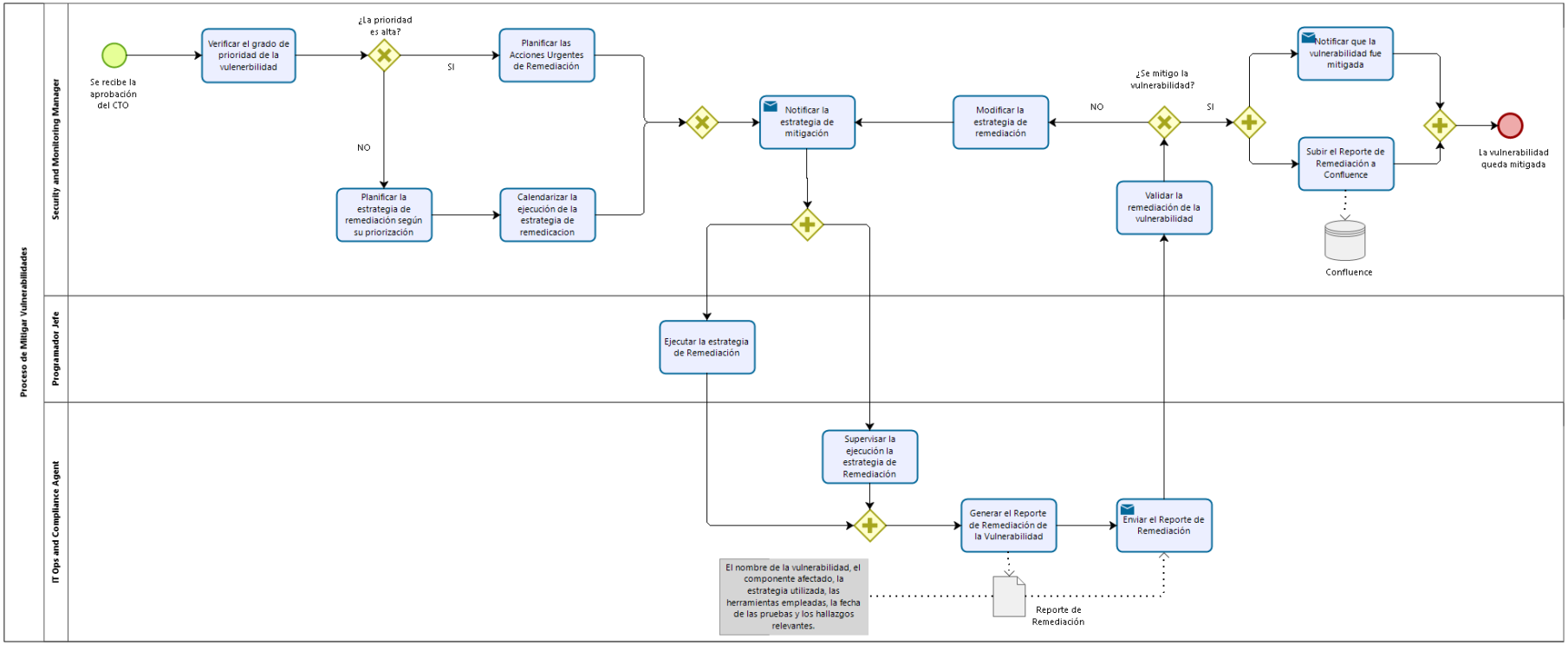
A partir de las oportunidades de mejora evidenciadas en la sección 5.1.1. Se establece la propiedad del procedimiento asignándolo al *Security and Monitoring Manager* y definiendo como cliente al Departamento de *IT Operations and Compliance*. Uno de los aspectos de mejora, está relacionado con la planificación de las estrategias de abordaje de Vulnerabilidades de Red. Dichos planes de mitigación se definen alrededor de la priorización asignada según la gravedad de acuerdo con las recomendaciones del NIST (Scarfone K & Souppaya M, 2022, pp. 25–26)

Dentro de las actividades descritas en el apartado del procedimiento desarrollado en el Anexo IX, se instaura la ejecución inmediata de las estrategias para abordar las Vulnerabilidades de Red criticas encontradas. Así mismo, este rediseño busca aplicar las buenas prácticas de la industria, (Scarfone K & Souppaya M, 2022, p. 28) afirman que la implementación de la estrategia de abordaje debe controlarse y planificarse para minimizar el impacto en el funcionamiento normal del sistema. Además, es importante documentar adecuadamente el proceso de implementación para futuras referencias y auditorías de seguridad.

De este modo, el rediseño del proceso busca integrarse con los procesos de análisis y priorización junto con la identificación de Vulnerabilidades de Red para proporcionar una gestión integral de las amenazas a la seguridad. Aunque los KPI de seguimiento no están definidos actualmente, su eficacia es esencial para mantener la seguridad organizacional en un entorno digital cambiante.

La Figura 33, es una representación simplificada de las actividades del proceso de Mitigar Vulnerabilidades de Red a partir del uso de en BPMN 2.0.

Figura 33 Proceso "To Be" Mitigar



Fuente: Elaboración propia, 2023

Simulación del proceso

En este apartado se ejecuta la simulación del proceso To Be de Mitigar Vulnerabilidades de Red bajo las mismas condiciones del proceso As Is, esto permite realizar un análisis del uso de los recursos asignados al proceso en cuestión.

Figura 34 Resultados Simulación To Be Mitigar

Name	Type	Instances completed	Instances started	Min. time	Max. time	Avg. time	Total time
Proceso de Mitigar Vulnerabilidades	Process	100	100	4h 30m	1d 10h 40m	8h 35m 6s	51d 4h 5m
Se recibe la aprobación del CTO	Start event	100					
Verificar el grado de prioridad de la vulenerbilidad	Task	100	100	20m	40m	20m 12s	1d 9h 40m
¿La prioridad es alta?	Gateway	100	100				
Planificar la estrategia de remediación según su priorización	Task	49	49	1h	1h 20m	1h 1m 25s	2d 2h 10m
Calendarizar la ejecución de la estrategia de remedicacion	Task	49	49	10m	20m	10m 36s	8h 40m
Planificar las Acciones Urgentes de Remediación	Task	51	51	1h	1h	1h	2d 3h
Ejecutar la estrategia de Remediación	Task	177	177	2h	3h 55m	2h 38s	14d 19h 55m
ExclusiveGateway	Gateway	100	100				
Supervisar la ejecución la estrategia de Remediación	Task	177	177	2h	3h 55m	2h 38s	14d 19h 55m
ParallelGateway	Gateway	177	177				
ParallelGateway	Gateway	177	177				
Generar el Reporte de Remediación de la Vulnerabilidad	Task	177	177	30m	2h 30m	30m 50s	3d 19h
Validar la remediación de la vulnerabilidad	Task	177	177	20m	40m	20m 22s	2d 12h 5m
¿Se mitigo la vulnerabilidad?	Gateway	177	177				
La vulnerabilidad queda mitigada	End event	100					
Enviar el Reporte de Remediación	Task	177	177	5m	35m	5m 11s	15h 20m
Notificar la estrategia de mitigación	Task	177	177	5m	1h 25m	5m 32s	16h 20m
Notificar que la vulnerabilidad fue mitigada	Task	100	100	5m	2h 5m	8m 12s	13h 40m
Modificar la estrategia de remediación	Task	77	77	2h	2h 20m	2h 15s	6d 10h 20m
Subir el Reporte de Remediación a Confluence	Task	100	100	10m	2h 10m	13m 12s	22h
ParallelGateway	Gateway	100	100				
ParallelGateway	Gateway	100	100				

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

A partir de los datos obtenidos de la Figura 34, evidencian la ejecución de la simulación, se posibilita la comparación de datos con los resultados obtenidos del proceso As Is. Los hallazgos sobre el proceso To Be son los siguientes el tiempo mínimo requerido para completar una instancia es de 4 horas y 30 minutos.

Mientras que el tiempo máximo es de 1 día, 10 horas y 40 minutos. El tiempo promedio es de aproximadamente 8 horas y 35 minutos por instancia. Estos datos permiten realizar la comparación que se muestra en la Tabla 31 la cual establece las diferencias entre el tiempo mínimo, máximo, promedio y total del proceso de Mitigar Vulnerabilidades de Red.

Tabla 31 Comparación de Tiempos Mitigar Vulnerabilidades de Red

Tiempo	As Is	To Be	Diferencia	Porcentaje
Mínimo	1h 35m	4h 30m	2h 55m de aumento	Aumento del 191.67%
Máximo	0d 19h 30m	1d 10h 40m	0d 14h 10m de aumento	Aumento del 116.84%
Promedio	9h 53m	8h 35m	1h 18m de reducción de tiempo	Reducción del 22.41%
Total	191d 14h 40m	51d 4h 5m	140d 10h 35m de ahorro de tiempo	Reducción del 73.26%

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

A continuación, se muestran los costos fijos totales aproximados del proceso a través de la Tabla 32.

Tabla 32 Costos del Proceso To Be de Mitigar Vulnerabilidades de Red

Nombre	Tiempo Mínimo	Tiempo Máximo	Tiempo Promedio	Tiempo Total	Costos fijo total
Proceso de Mitogación de Vulnerabilidades de Red	4h 30m	1d 10h 40m	8h 35m 6s	51d 4h 5m	$7,587.55.

Fuente: Elaboración propia (2023) con información suministrada por Bizagi (2023).

Creación del Reporte de Remediación

En la siguiente sección se define el Reporte de Remediación de Vulnerabilidades de Red. Este informe ha sido generado con el objetivo de documentar, abordar y corregir las Vulnerabilidades de Red identificadas, en los componentes de los sistemas. Así mismo, se establecen las instrucciones para completar el reporte presentado en el Apéndice BB. A continuación, se detallan las partes que forman parte del documento:

Información del informe: esta sección presenta información básica para la identificación del reporte.

- Reportado por: se debe ingresar el nombre del responsable del reporte.
- Fecha del informe: se debe ingresar la fecha en que se generará el informe.
- Cargo: se debe indicar el puesto o cargo dentro de la organización.
- Número de informe: se debe asignar un número de identificación único al informe.

Información de corrección de Vulnerabilidades de Red: en este apartado del reporte se detalla la información relacionada con el proceso de mitigación y la aplicación de la estrategia de mitigación aplicada de la vulnerabilidad y consta de las siguientes partes:

- Nombre de la vulnerabilidad: se ingresa el nombre o título que identifica de forma única la vulnerabilidad.
- Componente afectado: se ingresa el nombre o descripción del componente afectado por la vulnerabilidad.
- Prioridad: se selecciona la prioridad de la vulnerabilidad según su gravedad. Las categorías de priorización elegibles son “alto”, “medio” o “bajo”.
- Estado: se comprueba si la vulnerabilidad se ha solucionado o no. Se debe seleccionar Mitigado si el problema se resolvió o No mitigado si el problema persiste.
- Herramientas utilizadas: se proporciona una descripción detallada de las herramientas utilizadas durante las pruebas para identificar y remediar la vulnerabilidad.
- Estrategia utilizada: en el apartado se describe la estrategia o metodología específica utilizada para identificar y remediar la vulnerabilidad.
- Recomendaciones: en esta sección se definen las recomendaciones específicas para mitigar o remediar la vulnerabilidad identificada. Además, se debe describir las acciones necesarias para abordar el problema de seguridad.

Información adicional: esta sección contiene comentarios o información adicional relacionada con la amenaza que tenga la posibilidad de utilizar específicamente en fases posteriores del proceso de mitigación de vulnerabilidad.

Aprobación: por último, se debe aprobar y firmar por el gerente o supervisor correspondiente.

Comunicación con el equipo de trabajo

Este apartado define las recomendaciones de comunicación con el equipo de trabajo. Dichas sugerencias buscan establecer una estructura de comunicación eficaz durante el proceso de mitigación de Vulnerabilidades de Red que garantice que todas las partes interesadas estén informadas y actúen de manera oportuna.

El proceso toma como referencia el flujo de actividades propuestas en el rediseño del proceso de mitigación. El flujo comienza con la aprobación del CTO y aborda las Vulnerabilidades de Red como prioridad o en función de su nivel de riesgo.

La comunicación temprana de las estrategias de mitigación garantiza que todos los involucrados estén conscientes de la situación y estén listos para actuar, mientras que el monitoreo proactivo durante la implementación garantiza que se sigan los pasos. La validación del abordaje permite revisar y ajustar las políticas si las Vulnerabilidades de Red persisten. Una vez que se logra la mitigación, el proceso se completa con la notificación y documentación adecuadas.

Alineación con los estándares de la industria

En esta sección se establecen los aspectos que se consideraron para el alineamiento del proceso To Be presentado como solución con las buenas prácticas de la industria. Primero cabe recalcar que Hallet & Chen (2021, p. 42) explican que:

> La mitigación de Vulnerabilidades de Red y amenazas puede ser tan simple como modificar un ajuste de configuración o tan compleja como la instalación de una versión completamente nueva del software. No existe un enfoque de aplicación único que sea aplicable a todos los software, sistemas operativos o componentes de aplicaciones. Hallet & Chen (2021, p. 42)

A partir de la cita anterior y como decisión empresarial tomada en conjunto con el CTO, el *Security and Monitoring Manager* y el *IT Ops and Compliance Manager*, el rediseño del proceso se centra en, las validaciones de las actividades del proceso. Esto debido a que la propuesta busca que la asignación de recursos como costo y la accesibilidad de los recursos humanos calificados sean definidos según el nivel de priorización de la vulnerabilidad.

La comunicación temprana de la estrategia de abordaje junto con la actividad de supervisión de la implementación del plan de mitigación permite que el proceso se alinee a las recomendaciones del NIST, para mantener una comunicación efectiva y una gestión continua durante todo el proceso de mitigación. De la misma manera, el rediseño del proceso hace énfasis en validar la estrategia de abordaje, debido a que si la vulnerabilidad no queda mitigada se debe hacer una corrección en la estrategia, Este es un aspecto al que las buenas prácticas de la industria prestan atención para solucionar de efectiva de la amenaza.

Otro de los aspectos, que se tomó en cuenta para ajustar el proceso con las buenas prácticas fue crear una base de datos de mitigaciones específicas para Symbiotic, este punto se abarca con el Reporte de Remediación de Vulnerabilidades de Red presentado en el Apéndice BB. El reporte, además de permitir la comunicación y documentación, sirve como un registro de referencia y consulta para futuras estrategias. Esta base de datos de soluciones se establece en el gestor de conocimiento de la empresa Confluence, haciendo una carpeta dentro del repositorio que sea específica para consultas lo que ayuda la creación de futuras estrategias de evacuación.

5.2. Estrategia de Implementación

El siguiente apartado equivale a la fase seis del procedimiento metodológico descrito en la sección 0, la cual define la estrategia de implementación de la propuesta de solución de la problemática que se aborda en el presente documento.

Para realizar la implementación se toman en cuenta diferentes aspectos como las partes de la propuesta que se han completado a lo largo del periodo del TFG. Así mismo, se describen las responsabilidades organizativas y el cronograma para implementar la propuesta. No obstante, para la estrategia de implementación también se define un pequeño plan de comunicación y se delimitan las métricas de control para que el plan sea capaz de llevarse a cabo.

5.2.1. Partes de la Propuesta Implementadas en el TFG

Debido al diseño de la investigación, la solución del problema se aborda desde una perspectiva práctica que apoya la participación de las partes interesadas y la implementación de soluciones viables (ver sección 3.2). Por ende, mientras se realizó el TFG fue posible la ejecución de actividades y acciones que forman parte del Plan de Gestión y que permiten evidenciar su implementación en la organización.

5.2.1.1. Creación de Documentación

Para la propuesta de la solución como bien se explicó en el apartado anterior, se tuvo que desarrollar diversa documentación para la organización. A continuación, se mencionan los documentos presentados al departamento de *IT Operations and Compliance*.

El Anexo V muestra el Plan de Comunicación de Vulnerabilidades de Red. Dicho documento se diseñó con el objetivo de facilitar una comunicación efectiva entre las responsables de la gestión y las partes interesadas del proceso. La creación de las plantillas permite estandarizar el proceso de documentación y reporte de Vulnerabilidades de Red dentro de Symbiotic. El Apéndice Z permite ver la publicación del reporte de Identificación de Vulnerabilidades de Red.

Del mismo modo, el

Apéndice AA contiene el reporte de Análisis de Vulnerabilidades de Red. Por último, se presenta el Apéndice BB, el cual permite ver la publicación del reporte de Mitigación de Vulnerabilidades de Red. De esta forma, también se presenta el Anexo V, el cual incluye el Catálogo de KPIS. Este documento establece indicadores de desempeño para medir y mejorar la eficacia de la gestión de la vulnerabilidad.

5.2.1.2. Actualización de Documentación

Pese a que Symbiotic ya contaba con una política que abordaba cómo gestionar las Vulnerabilidades de Red, era una política que se compartía con los riesgos, esto era una de las causas principales de la problemática que se estableció en la sección 1.3.1. No obstante, el plan de gestión contempla la actualización de las políticas y procedimientos aquí establecidos, tomando en cuenta el análisis documental realizado en el apartado 4.1.4, las oportunidades de mejora descritas en la sección 4.4, las acciones recomendadas en cuanto al uso de herramientas y las recomendaciones para la estandarización de procesos.

5.2.1.3. Definición de los Procedimientos

De igual forma el plan de gestión contempla la definición de los procedimientos para cada etapa del ciclo de vida de Vulnerabilidades de Red. Los cuales desempeñan el papel de instructivos de ejecución y de consulta para el personal de Symbiotic. Así mismo, los procedimientos sirven para respaldar la ejecución de la política de Gestión de Vulnerabilidades de Red.

La documentación de los procedimientos definidos en los Anexo VII, Anexo VIII y Anexo IX también permiten la asignación de los roles, responsabilidades y actividades específicas relacionadas con los procedimientos descritos en la política. Esto garantiza que todo el personal involucrado tenga una comprensión clara de lo esperado de ellos y cómo deben completar sus tareas. Además, permite la estandarización en la ejecución de los procesos lo cual es esencial para evitar malentendidos y errores. La estandarización permite garantizar que todos responsables completen estas tareas de la misma manera, de modo que se reduzcan la variabilidad y la posibilidad de error.

La documentación de los procedimientos son una herramienta que facilita al departamento de *IT Ops and Compliance* la formación y capacitación de los empleados nuevos. De la misma manera, dichos procedimientos sirven como guía para aprender a cómo llevar a cabo sus responsabilidades esto ayuda a solventar una de las causas de la problemática descrita en la sección 1.3.1. A su vez, los procesos promueven una comunicación clara y efectiva dentro de la organización, ya que cualquier persona involucrada tiene la posibilidad de consultar o referirse a los instructivos definidos.

Otro de los aspectos que busca erradicar este componente de la solución, se encuentra relacionado con la gestión del conocimiento. Los procedimientos reducen la dependencia de las personas para realizar tareas críticas. En lugar de depender de la memoria o la experiencia de una sola persona, las organizaciones pueden confiar en la documentación. Esto debido a que los empleados ayudan en el desarrollo continuo de la documentación del programa a medida que adquieren conocimientos y experiencia sobre la ejecución de los procesos.

Por último, la documentación creada también ayuda a demostrar el cumplimiento con temas de auditoría. Symbiotic tiene la posibilidad de utilizar esta documentación para demostrar que se están siguiendo las regulaciones, prácticas legales que recaen sobre la gestión de Vulnerabilidades de Red.

5.2.2. Cronograma de Implementación

En el siguiente apartado se muestra la

Tabla 44, la cual plantea el cronograma presentado en el Apéndice C ejecución para el proceso de Gestión Vulnerabilidades de Red que Symbiotic busca desarrollar.

Tabla 33 Cronograma de Implementación

	Actividades	Periodo	Estado
1	Documentación	--	--
1.1	Creación del Plan de Comunicación de Vulnerabilidades de Red.	Septiembre 2023	Completado
1.2	Creación de las Plantillas de Reportes.	Octubre 2023	Completado
1.3	Creación del Catálogo de KPIS.	Septiembre 2023	Completado
1.4	Actualización de la Política de Gestión de Vulnerabilidades de Red.	Septiembre 2023	Completado
2	Material de Entrenamiento	--	--
2.1	Material de Entrenamiento de la Política	Septiembre 2023	
2.2	Material de Entrenamiento Plan de Comunicación.	Septiembre 2023	Completado
2.3	Material de Entrenamiento Catálogo de KPI's.	Septiembre 2023	Completado
2.4	Material de Entrenamiento de la herramienta IDS.	Noviembre 2023	No iniciado
3	Herramientas	--	--
3.1	Creación del manual de usuario de la herramienta IDS.	Noviembre 2023	No iniciado
3.2	Taller de la herramienta IDS.	Noviembre – Diciembre 2023	No iniciado
4	Procesos	--	--
4.1	Perfil de los procesos del ciclo de vida de las Vulnerabilidades de Red.	Octubre 2023	Completado
4.2	Taller de uso de las plantillas de los reportes.	Noviembre 2023	No iniciado
4.3	Implementación del Plan de Gestión.	Noviembre - Diciembre 2023	No iniciado
5	Control y seguimiento	--	--
5.1	Revisión de la nueva documentación generada por los procesos.	Noviembre – Diciembre 2023	No iniciado
5.2	Reunión mensual de control y seguimiento.	Noviembre – Diciembre 2023	No iniciado
5.3	Reunión trimestral de seguimiento de alineación con los estándares.	Noviembre – Diciembre 2023	No iniciado

Fuente: Elaboración propia, 2023.

5.2.3. Responsables de la Implementación

Después de haber definido el cronograma de ejecución de la propuesta de solución, es crucial identificar los roles que desempeñará cada miembro de la organización en la ejecución de la estrategia. Esta identificación permite especificar las funciones y responsabilidades encomendadas a cada miembro, la cual incluye a personas que tienen la posibilidad de verse directamente afectadas por el proyecto, así como aquellas que no tengan un impacto directo.

Para esto se desarrolla Tabla 34, que incluye matriz RACI, la cual sirve como herramienta de gobernanza destinada a especificar y aclarar las funciones y responsabilidades de quienes participan en la propuesta de solución de Symbiotic. A continuación, se define el significado de cada una de las letras correspondientes a RACI.

4. **Responsable *(Responsible):*** este rol corresponde a la persona responsable de realizar una tarea o actividad específica. Son directamente responsables de la ejecución de la obra y de su finalización exitosa.
5. **Responsable de Aprobación (*Accountable*):** se refiere a la persona encargada de la toma de decisión final y aprobación del trabajo realizado. Su tarea principal es garantizar que el trabajo cumpla con los estándares establecidos y logre los resultados esperados.
6. **Consultor (*Consulted*)**: este cargo se otorga a una persona que contribuye al desarrollo del encargo a través de conocimientos, experiencia o acceso a datos pertinentes.
7. **Informado (*Informed*):** las personas en este rol intentan estar informadas sobre el progreso y los resultados del trabajo realizado, incluso si no están directamente involucrados en la ejecución del trabajo.

Tabla 34 Matriz RACI de Implementación

Responsables	Security and Monitoring Manager	Security and Monitoring Agent	IT Ops and Compliance Manager	IT Ops and Compliance Agent
Actividades	--	--	--	--
Documentación	--	--	--	--
Creación del Plan de Comunicación de Vulnerabilidades de Red.	C	I	A	R
Creación de las Plantillas de Reportes.	I	I	A	R
Creación del Catálogo de KPIS.	A	I	A	R
Actualización de la Política de Gestión de Vulnerabilidades de Red.	C	I	A	R
Material de Entrenamiento	--	--	--	--
Material de Entrenamiento de la Política	I	I	A	R

Responsables	Security and Monitoring Manager	Security and Monitoring Agent	IT Ops and Compliance Manager	IT Ops and Compliance Agent
Actividades	--	--	--	--
Material de Entrenamiento Plan de Comunicación.	I	I	A	R
Material de Entrenamiento Catálogo de KPI's.	A	I	A	R
Material de Entrenamiento de la herramienta IDS.	C	R	A	I
Herramientas	--	--	--	--
Creación del manual de usuario de la herramienta IDS.	A	R	I	I
Taller de la herramienta IDS.	R	I	I	I
Procesos	--	--	--	--
Perfil de los procesos del ciclo de vida de las Vulnerabilidades de Red.	A	C	C	R
Taller de uso de las plantillas de los reportes.	I	I	A	R
Implementación del Plan de Gestión.	R	R	R	R
Ejecución del Plan Piloto.	R	R	R	R
Control y seguimiento	--	--	--	--
Revisión de la nueva documentación generada por los procesos.	R	I	R	I
Reunión mensual de control y seguimiento.	R	I	R	I
Reunión trimestral de seguimiento de Alineación con Estándares de Seguridad Reconocidos.	R	I	R	I

Fuente: Elaboración propia, 2023.

5.2.4. Plan de Comunicación de la Implementación

En la presente sección se define la estrategia de comunicación que se utilizará para la implementación de la propuesta de solución. El objetivo de dicha estrategia es garantizar que todas las actividades sean comunicadas claramente sobre los cambios, las expectativas asociadas, y aborde cómo la implementación será exitosa y se integrará efectivamente en la cultura de la empresa.

Objetivo

Garantizar que todas las partes interesadas de Symbiotic comprendan las actividades relacionadas a la implementación de la solución al proceso de gestión de Vulnerabilidades de Red.

Canales de comunicación

Esta sección establece los diferentes canales de comunicación para llegar a todos las partes involucradas, en la implementación:

8. Correo electrónico: se utiliza el correo interno de la organización para comunicaciones oficiales y actualizaciones periódicas, del estado de la implementación de la propuesta.
9. Reuniones informativas: se realizarán tanto presenciales como en línea, para que la organización reciba los entregables de los componentes de la solución.

Partes Interesadas y Actividades de Comunicación

En el siguiente apartado se establecen las actividades de comunicación y partes interesadas de ejecutarlas, además del canal por el cual se comunica dicha actividad. Para ello, se hará uso de la Tabla 35 con la intención de definir el responsable de cada una de las actividades que se deben comunicar.

Tabla 35 Matriz RACI Actividades de Comunicación

Responsables		Security and Monitoring Manager	Security and Monitoring Agent	IT Ops and Compliance Manager	IT Ops and Compliance Agent
Actividades	Canal	--	--	--	--
Lanzamiento de la iniciativa del Plan de Gestión.	Correo electrónico - Reunión informativa	A	I	A	R
Comunicación Inicial de la solución	Reunión informativa	I	I	A	R
Identificación del personal para la	Correo electrónico	I	R	A	R

Responsables		Security and Monitoring Manager	Security and Monitoring Agent	IT Ops and Compliance Manager	IT Ops and Compliance Agent
Actividades	Canal	--	--	--	--
capacitación y concientización					
Lanzamiento Oficial del Plan de Gestión.	Correo electrónico - Reunión informativa	A	I	A	R
Implementación del Plan de Gestión.	Correo electrónico - Reunión informativa	R	R	R	R
Entregables de los componentes de la solución.	Reunión informativa	A	I	A	R
Comunicación del estado del proyecto.	Correo electrónico	I	I	A	R
Retroalimentación.	Reunión informativa	R	R	R	I

Fuente: Elaboración propia, 2023.

5.2.5. Métricas de Control y Seguimiento de la Implementación

En este apartado se desarrolla la fase siete del procedimiento metodológico definido en la sección 0. Además, el presente apartado ayuda a definir las acciones para que se asegure la adecuada implementación de la gestión de Vulnerabilidades de Red en la organización. Para que el proceso se realice de forma adecuada se sigue lo definido en la sección 5.1.2 Política de Gestión de Vulnerabilidades de Red que establece los estatutos para el seguimiento y control. Estas consideraciones permiten que el monitoreo de la implementación del plan, sigan un proceso estandarizado, que tenga responsables y KPI's asignados.

El seguimiento y control del proyecto incluirá reuniones mensuales de seguimiento y reuniones trimestrales (destinadas a evaluar periódicamente documentos relacionados con la seguridad de la información), las cuales son parte de la estrategia de comunicación definida en la sección 5.1.2.2, hace referencia al Plan de Comunicación de Gestión de Vulnerabilidades de Red (ver Anexo V). A continuación, se detallan las métricas definidas para controlar y evaluar el progreso de la puesta en práctica de la solución propuesta.

La Tabla 36 registra el porcentaje de cumplimiento en la implementación y seguimiento del Plan de Gestión de Vulnerabilidades de Red. Esta métrica define la cantidad de tareas completadas con las tareas programadas en la Tabla 34.

Tabla 36 Porcentaje de Cumplimiento

Campo	Data
Nombre del Indicador	Porcentaje de Cumplimiento
Código del Indicador	CS-01
Objetivo Estratégico	Evaluar el progreso en la implementación y seguimiento del plan de gestión de Vulnerabilidades de Red.
Objetivo de Seguridad	Verificar el cumplimiento de las políticas de seguridad de la información.
Medida	Porcentaje.
Tipo de Medida	Cuantitativa.
Fórmula	(Tareas completadas / Tareas programadas) x 100
Aplicación Pruebas	Al evaluar el progreso en la implementación.
Frecuencia	Quincenal.
Responsables	*IT Ops and Compliance Manager.*
Fuente de Datos	Registros de seguimiento y control.

Fuente: Adaptado de (Chew et al., 2008, p. 51)

Así mismo, la Tabla 37 ayuda a fijar la cantidad de reuniones programadas y realizadas para el seguimiento del proceso del desarrollo de la implementación. Su propósito es asegurar una comunicación regular y efectiva dentro de Symbiotic. Al evaluar las reuniones trimestrales, presentar un informe; al evaluar las reuniones mensuales y presentar un informe mensualmente.

Tabla 37 Porcentaje de Frecuencia de Reuniones

Campo	Data
Nombre del Indicador	Porcentaje de Frecuencia de Reuniones.
Código del Indicador	CS-02
Objetivo Estratégico	Asegurar que se lleven a cabo reuniones programadas de seguimiento y control.
Objetivo de Seguridad	Mantener un canal de comunicación regular sobre la gestión de Vulnerabilidades de Red.
Medida	Porcentaje.
Tipo de Medida	Cuantitativa.
Fórmula	(Reuniones completadas / Reuniones programadas) x 100
Aplicación Pruebas	Al evaluar el progreso en la implementación.
Frecuencia	Quincenal o mensual.
Responsables	*IT Ops and Compliance Manager.*
Fuente de Datos	Registros de seguimiento y control.

Fuente: Adaptado de (Chew et al., 2008, p. 51)

5.3. Control y Monitoreo

En esta sección se establece la fase siete del procedimiento metodológico desarrollado en el apartado 0 y está basado en el catálogo de KPIs desarrollado en el marco del proyecto. El catálogo define indicadores clave de desempeño específicos para medir la efectividad y eficiencia de las prácticas de gestión de vulnerabilidades de red de Symbiotic.

Los indicadores proporcionan indicadores cuantitativos que miden el desempeño de los procesos y determinan el grado de cumplimiento de los objetivos establecidos. Al monitorear constantemente estos KPI, Symbiotic busca mantener una visión detallada de la postura de seguridad de la organización contra las vulnerabilidades de red. Al adoptar este enfoque, se busca que el departamento de *IT Operations and Compliance* detecta vulnerabilidades potenciales de manera temprana, sino que también respalda la toma de decisiones informadas para mejorar continuamente las medidas de seguridad.

5.3.1. Catálogo de KPI's

El presente apartado define el catálogo de métricas de desempeño para la gestión de Vulnerabilidades de Red (ver Anexo VI) este hace referencia a la fase siete del procedimiento metodológico. Para la definición de los KPI's se hizo uso de los hallazgos mostrados en los apéndices Apéndice Q y el Apéndice R, con el fin de establecer métricas que se adecuen a las necesidades de la organización.

Chew et al. (2008, p. 8) definen varios factores al desarrollar e implementar un programa de medición, en la NIST SP 800-55 Guía de medición para seguridad de información, a continuación, se mencionan dichos aspectos.

> Las medidas deben proporcionar datos cuantificables, ya sea en forma de porcentajes, promedios o valores numéricos. La accesibilidad de los datos es un requisito para respaldar la toma de acciones. Los procesos de seguridad de la información que puedan repetirse y sean consistentes deben ser los únicos a medir. Las métricas elegidas deberían ser útiles para monitorear el desempeño general y elegir sabiamente cómo asignar los recursos. (Chew et al., 2008, p. 8)

El Anexo VI busca definir un catálogo de KPI alineado con las buenas prácticas establecidas por la NIST SP 800-55 Guía de medición para seguridad de información. Con el fin de que las métricas sean compatibles con los objetivos estratégicos y objetivos de seguridad de la información de Symbiotic.

Métricas del Proceso de Identificación

A parir del uso de la Tabla 38 se define la métrica establecida para el proceso de identificación de Vulnerabilidades de Red, la cual se encuentra relacionada con la cantidad de Vulnerabilidades de Red detectadas (GV-001) es útil para evaluar la postura de seguridad de la organización.

Tabla 38 KPI Cantidad de Vulnerabilidades de Red Detectadas

Nombre del Indicador	Cantidad de Vulnerabilidades de Red Detectadas
Código del Indicador	GV-001
Objetivo Estratégico	Fortalecer la postura de seguridad de la organización.
Objetivo de TI	Garantizar la seguridad de los componentes del sistema Tap on Phone de Symbiotic frente a amenazas.
Medida	Número total de Vulnerabilidades de Red detectadas.
Tipo de Medida	Cuantitativa.
Fórmula	Ninguna.
Aplicación de Pruebas	La métrica se utilizará durante las revisiones regulares de seguridad de los componentes del sistema.
Frecuencia	Quincenal.
Responsables	*Security and Monitoring Agent.*
Fuente de Datos	Reportes de alarmas de seguridad sobre las señales de actividad sospechosa.

Fuente: Adaptado de Chew et al. (2008, p. 51)

La Tabla 38 permite mostrar la justificación de la creación del "KPI Cantidad de Vulnerabilidades de Red Detectadas". Este indicador refleja el número total de Vulnerabilidades de Red detectadas en los componentes del sistema y permite una evaluación objetiva y cuantitativa del estado de seguridad. La implementación de este indicador es consistente con el objetivo estratégico de fortalecer la postura de seguridad de la organización y el objetivo de TI de garantizar la seguridad de los sistemas.

Métricas del Proceso de Análisis

A continuación, se muestra la métrica definida para el porcentaje de Vulnerabilidades de Red clasificadas (GV-002), que enfatiza la categorización de las Vulnerabilidades de Red. Para detallar el indicador se usa la Tabla 39.

Tabla 39 KPI Porcentaje de Vulnerabilidades de Red clasificadas

Nombre del Indicador	Porcentaje de Vulnerabilidades de Red clasificadas
Código del Indicador	GV-002
Objetivo Estratégico	Fortalecer la postura de seguridad de la organización.
Objetivo de TI	Categorizar de manera eficiente las Vulnerabilidades de Red detectadas de acuerdo con el componente del sistema al que pertenece.
Medida	Porcentaje
Tipo de Medida	Cuantitativa
Fórmula	(Cantidad de Vulnerabilidades de Red clasificadas por componente / Cantidad total de Vulnerabilidades de Red) x 100
Aplicación de Pruebas	La métrica se utilizará durante las revisiones regulares de seguridad de los componentes del sistema.
Frecuencia	Mensual
Responsables	*Security and Monitoring Manager.* *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Fuente de Datos	El informe de análisis de Vulnerabilidades de Red.

Fuente: Adaptado de Chew et al. (2008, p. 51)

La Tabla 39, permite establecer la postura de seguridad de la organización para la correcta clasificación de las Vulnerabilidades de Red detectadas. La categorización de dichas amenazas es importante debido a que permite a los responsables identificar cuáles son los componentes del sistema afectados para una adecuada priorización y prevención de amenazas.

La fórmula utilizada para este indicador permite comparar el porcentaje de Vulnerabilidades de Red clasificadas con respecto al total de Vulnerabilidades de Red, realizando una evaluación cuantitativa y objetiva del proceso de clasificación. Al calcular el porcentaje de Vulnerabilidades de Red clasificadas, Symbiotic evalúa la capacidad de la organización para comprender las amenazas en su entorno digital.

Métricas del Proceso de Priorización

El indicador relacionado al proceso de priorización se encuentra vinculada a la tasa de Vulnerabilidades de Red criticas priorizadas. La Tabla 40 permite conocer a mayor detalle la definición de dicha métrica.

Tabla 40 KPI Tasa de Vulnerabilidades de Red Críticas Priorizadas

Nombre del Indicador	Tasa de Vulnerabilidades de Red Críticas Priorizadas
Código del Indicador	GV-003
Objetivo Estratégico	Incrementar la seguridad de Symbiotic a través de la mitigación de Vulnerabilidades de Red críticas.
Objetivo de TI	Garantizar la seguridad de los activos de información críticos que poseen los componentes del sistema.
Medida	Porcentaje de Vulnerabilidades de Red criticas priorizadas en relación con el total de Vulnerabilidades de Red criticas detectadas.
Tipo de Medida	Cuantitativa
Fórmula	(Número de Vulnerabilidades de Red Críticas Priorizadas / Cantidad de Vulnerabilidades de Red Detectadas) x 100.
Aplicación de Pruebas	La métrica se utilizará durante las revisiones regulares de seguridad de los componentes del sistema.
Frecuencia	Mensual.
Responsables	*Security and Monitoring Manager*. *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Fuente de Datos	El informe de análisis de Vulnerabilidades de Red.

Fuente: Adaptado de Chew et al. (2008, p. 51)

El indicador descrito en la Tabla 40 se basa en el objetivo estratégico de mejorar la seguridad de Symbiotic reduciendo las Vulnerabilidades de Red críticas. Esta métrica proporciona una visión clara de qué tan efectiva es la organización en identificar y abordar las Vulnerabilidades de Red más graves.

Así mismo, el indicador permite al departamento de *IT Ops and Compliance* de Symbiotic evaluar, priorizar y abordar las Vulnerabilidades de Red críticas para reducir los riesgos asociados a ellas y que tienen la posibilidad de afectar a la organización.

De la misma forma, el indicador ayuda a determinar si se están tomando medidas efectivas para reducir amenazas graves que pueden afectar seriamente la seguridad y las operaciones de Symbiotic. Por ende, también ayuda a aumentar la transparencia en la rendición de cuentas.

Métricas del Proceso de Mitigación

En la siguiente sección se definen los indicadores de rendimiento relacionado con el proceso de mitigación de Vulnerabilidades de Red. La Tabla 41 definir el porcentaje de Vulnerabilidades de Red mitigadas con éxito y la Tabla 42 establece las características relacionadas con el tiempo promedio empleado para aplicar medidas de mitigación.

Tabla 41 KPI Porcentaje de Vulnerabilidades de Red mitigadas con éxito

Nombre del Indicador	Porcentaje de Vulnerabilidades de Red mitigadas con éxito
Código del Indicador	GV-004
Objetivo Estratégico	Mejorar la capacidad de resistencia de las Vulnerabilidades de Red a través de una mitigación eficaz.
Objetivo de TI	Incrementar el porcentaje de Vulnerabilidades de Red mitigadas que garanticen la reducción de riesgos de exposición a amenazas de seguridad.
Medida	Porcentaje de Vulnerabilidades de Red mitigadas con éxito sobre la cantidad total de Vulnerabilidades de Red detectadas.
Tipo de Medida	Cuantitativa
Fórmula	(Número de Vulnerabilidades de Red Mitigadas con Éxito / Número Total de Vulnerabilidades de Red Identificadas) x 100.
Aplicación de Pruebas	La métrica se utilizará durante las revisiones regulares de seguridad de los componentes del sistema, así mismo cada vez que se realice el proceso de mitigación y el proceso posterior de seguimiento.
Frecuencia	Mensual
Responsables	*Security and Monitoring Manager*. *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Fuente de Datos	El informe de análisis de Vulnerabilidades de Red, reporte de mitigación de Vulnerabilidades de Red y reporte de seguimiento.

Fuente: Adaptado de Chew et al. (2008, p. 51)

La métrica descrita en la Tabla 41, permite identificar la eficacia de las medidas de mitigación que se desarrollan en Symbiotic. Según los autores Hallet & Chen (2021) explican que "La mitigación exitosa de Vulnerabilidades de Red contribuye a la resiliencia de la organización frente a amenazas de seguridad."

A partir, de la explicación anterior la métrica establecida, proporciona datos objetivos sobre el éxito en la mitigación, lo que respalda la toma de decisiones. La fórmula definida para el indicador ayuda a transparencia y la comprensión para todas las partes interesadas sobre cómo se calcula la métrica permitiendo entender la importancia de la alineación con los objetivos de la empresa. Así mismo, el indicador apoya a crear una cultura de mejora continua de la seguridad de la información en la organización basada las mejores prácticas de la industria.

A continuación, se presenta la Tabla 42, que establece las características relacionadas con el tiempo promedio empleado para aplicar medidas de mitigación.

Tabla 42 KPI Tiempo promedio para aplicar medidas de mitigación

Nombre del Indicador	Tiempo promedio para aplicar medidas de mitigación
Código del Indicador	GV-005
Objetivo Estratégico	Mejorar la capacidad de resistencia de las Vulnerabilidades de Red a través de una mitigación eficaz.
Objetivo de TI	Reducir el tiempo desee la detección hasta la mitigación exitosa de las Vulnerabilidades de Red.
Medida	El tiempo promedio en días, desde la detección hasta la aplicación exitosa de pruebas de mitigación.
Tipo de Medida	Cuantitativa
Fórmula	Este indicador se mide directamente en días.
Aplicación de Pruebas	Esta métrica se aplica al monitoreo de Vulnerabilidades de Red y a cualquier ciclo de mitigación.
Frecuencia	Cada vez que se detecte una vulnerabilidad nueva.
Responsables	*Security and Monitoring Manager.* *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Fuente de Datos	Reportes de alarmas de seguridad sobre las señales de actividad sospechosa. Reporte de mitigación de Vulnerabilidades de Red.

Fuente: Adaptado de Chew et al. (2008, p. 51)

Además de respaldar la toma de decisiones informadas, la métrica descrita en la Tabla 42 también ayuda a evaluar la eficacia de las actividades relacionadas con el tiempo de aplicación de estrategias de remediación efectivas. Lo anterior, con el objetivo a reducir el tiempo desde el descubrimiento de la vulnerabilidad hasta la mitigación exitosa (GV-005).

El indicador permite evidenciar que tan amplia es la ventana de tiempo de exposición a amenazas potenciales. Así mismo, la métrica permite priorizar las estrategias de comunicación definidas dentro de Symbiotic para rastrear los riesgos potenciales.

Métricas del Proceso de Comunicación

La presente sección establece las métricas para el proceso de comunicación relacionado con la gestión de Vulnerabilidades de Red. Dichas métricas permiten garantizar la seguridad de la información en la organización. Las métricas definidas se relacionan con la evaluación de la eficiencia y rapidez de informar las Vulnerabilidades de Red encontradas en los componentes del sistema y aplicaciones cruciales.

Tabla 43 KPI Porcentaje de Vulnerabilidades de Red comunicadas a tiempo

Nombre del Indicador	Porcentaje de Vulnerabilidades de Red comunicadas a tiempo
Código del Indicador	GV-006
Objetivo Estratégico	Mejorar el proceso de comunicación relacionado a las Vulnerabilidades de Red.
Objetivo de TI	Consolidar que todas las partes interesadas en la gestión de Vulnerabilidades de Red sean comunicadas de forma asertiva.
Medida	Porcentaje.
Tipo de Medida	Cuantitativa.
Fórmula	(Número de Vulnerabilidades de Red comunicadas a tiempo / Total de Vulnerabilidades de Red detectadas) x 100
Aplicación de Pruebas	La métrica se utilizará durante las revisiones regulares de seguridad.
Frecuencia	Mensual.
Responsables	*Security and Monitoring Manager.* *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Fuente de Datos	Reporte de mitigación de Vulnerabilidades de Red y reporte de seguimiento.

Fuente: Adaptado de Chew et al. (2008, p. 51)

La métrica GV-006 descrita en la Tabla 43Tabla 43 permite que el departamento de *IT Ops and Compliance* sea capaz de garantizar que las Vulnerabilidades de Red se comuniquen a tiempo y se alineen con las buenas prácticas y regulaciones que son esenciales en la gestión de Vulnerabilidades de Red y la seguridad de la información. Esta métrica ayuda a comprender que tan eficaces son las estrategias de comunicación internas planteadas en el Anexo V para la notificación a las partes interesadas.

A continuación, se muestra la Tabla 44, que establecen las características relacionadas al tiempo promedio empleado para comunicar Vulnerabilidades de Red críticas. Esta métrica ayuda a la toma de medidas rápidas y efectivas en la gestión de la seguridad de la información.

Tabla 44 Tiempo promedio para comunicar Vulnerabilidades de Red críticas

Nombre del Indicador	Tiempo promedio para comunicar Vulnerabilidades de Red críticas
Código del Indicador	GV-007
Objetivo Estratégico	Impulsar la eficiencia de la comunicación de Vulnerabilidades de Red críticas.
Objetivo de TI	Garantizar que las Vulnerabilidades de Red críticas se comuniquen de manera oportuna para la mitigación.
Medida	Tiempo promedio en horas (h)
Tipo de Medida	Cuantitativa.
Fórmula	(Suma de tiempos para comunicar Vulnerabilidades de Red críticas) / (Número de Vulnerabilidades de Red críticas comunicadas)
Aplicación de Pruebas	La métrica se utilizará durante las revisiones regulares de seguridad.
Frecuencia	Mensual.
Responsables	*Security and Monitoring Manager*. *Security and Monitoring Agent.*
Fuente de Datos	Reporte de mitigación de Vulnerabilidades de Red y reporte de seguimiento.

Fuente: Adaptado de Chew et al. (2008, p. 51)

La Tabla 44 garantiza que las Vulnerabilidades de Red críticas se comuniquen para ser mitigadas de manera oportuna, así mismo, el indicador permite que la comunicación ayude a la identificación de riesgos asociados de manera más rápida con el fin de reducir la continuidad del servicio que ofrece Symbiotic

5.4. Análisis de Costo - Beneficio de la Propuesta.

El siguiente apartado equivale a la fase seis del procedimiento metodológico descrito en la sección 0. El propósito de este apartado es realizar un análisis financiero del proyecto con el fin de proyectar los diversos aspectos que se deben considerar antes, durante y después de la implementación de la solución en términos monetarios. El Ministerio de Trabajo y Seguridad Social (2023) señala que el salario mínimo de un licenciado es de ¢752,220.04. Además, el precio por hora de la herramienta IDS de Google que cuenta la empresa es de $1.50.

Del mismo modo, el Apéndice G muestra las aproximaciones de los salarios del personal de Symbiotic, en donde de detalla que el *IT Ops and Compliance Manager* es de ¢1,640,820, el *IT Ops and Compliance Agent* es de ¢626,828.55, el salario del *Security and Monitoring Manager* de ¢l,750,420 y por último el del Desarrollador jefe es de ¢2,075,640.

La distribución de los costos aproximados de los procesos As Is son tomados del apartado 4.3 del capítulo de Análisis y los costos relacionados a los modelos de los rediseños se obtienen del apartado 5.1.2.4. Así mismo, la Tabla 45 muestra los beneficios financieros vinculados al ahorro de cada uno de estos procesos.

Tabla 45 Beneficios Financieros

Costos de ejecución	As is	To be	Diferencia de ahorro en un año	Diferencia de ahorro en dos años	Porcentaje de ahorro
Proceso Identificar	$17,432.46	$8,046.08	$9,386.38	$18,772.76	53%
Proceso Analizar y Priorizar	$ 9,767.66	$8,514.03	$1,253.63	$2,507.26	12.84%
Proceso Mitigar	$ 23,850.72	$7,587.55	$16,263.17	$32,526.34	68.09%
TOTAL	*$ 51,050.84*	*$24,147.66*	*$26,903.18*	*$53,806.36*	52.72%

Fuente: Elaboración propia (2023)

A partir de los datos mostrados en laTabla 45, se evidencia que el Proceso de Identificar tiene un ahorro aproximado del 53%; el Proceso de Analizar y Priorizar del 12.84%, y el Proceso de Mitigar del 68.09%.

De acuerdo de los porcentajes obtenidos combinando los tres procesos es de alrededor del 52.72% en comparación con la situación actual de la Gestión de Vulnerabilidades de Red en la organización. Para la implementación también se debe tomar en cuenta que la implementación no tiene un costo monetario directo en adquisiciones de software o herramientas nuevas.

La solución si contempla un costo de tiempo del personal y de los recursos invertidos. A continuación, se utiliza la Tabla 46 para desglosar los costos directos asociados con la implementación de la solución, en el departamento de IT Operations and Compliance de Symbiotic.

Tabla 46 Costos Directos de Implementación

Costos Directos de Implementación	
Descripción	Costo en horas colaborador en dólares
Actualización de la documentación existente (8 horas)	$39.13
Creación de documentación nueva (40 horas).	$195.64
Documentación de los procesos de gestión (20 horas).	$97.82
Capacitación interna del rediseño del proceso para los miembros del departamento, uso de las plantillas de los reportes (20 horas).	$744.43
Taller de la herramienta IDS (8 horas).	$273.16
Seguimiento del proyecto (20 horas)	$529.22
TOTAL	*$1,350.18*

Fuente: Elaboración propia (2023)

A continuación, se presenta Tabla 47 relacionada con los costos indirectos asociados con la infraestructura tecnológica, las comunicaciones, licencias y las operaciones generales de que se necesitan para el desarrollo de la propuesta de solución que se le brinda a Symbiotic en Costa Rica.

Tabla 47 Costos Indirectos de la Implementación

Costos Indirectos de Implementación	
Descripción	Costo mensual en dólares
Servicios en la nube (Google Cloud Platform)	$1500
Herramientas de desarrollo (IDS Google)	$1,080
Depreciación en línea recta Equipamiento de oficina (Dell Latitude 3420 14" HD, Core i5-1135G7 2.4 GHz, 16GB RAM, 256GB SSD)	$8.67
Costos de servicios de internet (Fibra Óptica ICE, 100 Megas)	$49.58
Herramientas de comunicación (Slack, 6 personas)	$43.50
Licencias de Confluence (6 personas, Dept It Ops and Compliance)	$36.3
TOTAL	*$2758.05*

Fuente: Elaboración propia (2023)

Del mismo modo, Tabla 48, se describen los costos de operación de los procesos con el tiempo semanal asignado por el *IT Ops and Compliance Manager* y el CTO establecidos en el Apéndice G.

Tabla 48 Costos de Operación

Costos de operación	Operación primer año	Operación segundo año	Operación total
IT Ops and Compliance Manager	$7,374.47	$7,374.47	$14,748.94
IT Ops and Compliance Agent	$2,817.21	$2,817.21	$5,634.41
Security and Monitoring Agent	$3,380.76	$3,380.76	$6,761.53
Security and Monitoring Manager	$7,867.06	$7,867.06	$15,734.11
TOTAL	*$21,439.50*	*$21,439.50*	*$42,879.00*

Fuente: Elaboración propia, 2023.

En forma de resumen se comprende que los Costos Totales contemplan los Costos Directos de Implementación $1,350.18 y los Costos Indirectos de Implementación $2,758.05, así mismo los Costos de Operación $42,879.00 haciendo que el costo total de la inversión de la propuesta sea de $46,987.23. Es crucial considerar este monto en el contexto de los beneficios esperados y la mejora en la postura de seguridad de Symbiotic. La inversión realizada está destinada a fortalecer la gestión de vulnerabilidades, lo que, a su vez, contribuirá a la seguridad integral de la organización y a la reducción de riesgos.

Una vez que se han examinado los beneficios descritos en la Tabla 45 y el estudio de los costos en las Tabla 46, Tabla 47 y la Tabla 48 de implementar la solución sugerida, se determina el retorno de la inversión (ROI) del proyecto, utilizando la siguiente fórmula:

$$ROI = \frac{(Beneficios - Costo\ de\ Inversión)}{Costo\ de\ Inversión}\ x\ 100$$

Figura 35 Cálculo del ROI

$$ROI = \frac{(\$53{,}806.36 - \$46{,}987.23)}{(\$46{,}987.23)}\ x\ 100 = 14.52\%$$

Fuente: Elaboración propia, 2023.

Según el resultado de la aplicación de la fórmula del ROI, como se muestra en la Figura 35, la propuesta de solución desarrollada en este documento indica que la inversión inicial se recupera un 14.52% de las veces, lo cual genera un valor de retorno positivo. El resultado obtenido demuestra que los beneficios superan los costos de la implementación de la solución. Así mismo, un ROI de 14.52% demuestra la viabilidad financiera del proyecto. En la práctica, esto significa que la solución propuesta aporta beneficios económicos a la Symbiotic.

El ROI obtenido también valida la inversión y el esfuerzo realizado en el proyecto. Igualmente, este resultado refuerza las decisiones que se tomarán en el futuro y enfatiza la importancia de mantener el proyecto bien administrado para lograr un crecimiento rentable a largo plazo. Esto crea una base financiera sólida para el departamento de *IT Operations and Compliance de Symbiotic*.

6. Conclusiones

El siguiente capítulo brinda la oportunidad de identificar las enseñanzas adquiridas durante el desarrollo del proyecto final de graduación. A continuación, se detallan aquellos hallazgos y conclusiones que se evidenciaron a lo largo de la ejecución de este proyecto y que están asociados con cada uno de los objetivos específicos definidos en la sección 1.4 del Capítulo 1.

6.1. Objetivo específico 1

En relación con el objetivo específico 1: Analizar la situación actual de la gestión de Vulnerabilidades de Red para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria, se concluye lo siguiente:

6.1.1 Por medio del instrumento de observación documental aplicado en la sección 4.1.4 se encuentra que no existe documentación para cada proceso analizado, ni contempla la asignación de roles o responsabilidades, así mismo se muestra una ausencia de objetivos claros definidos para cada uno de los procesos. Este vacío de información contribuye a una comprensión limitada por parte del personal en lo que respecta a los pasos a seguir en dichos procesos.

6.1.2 Por medio de los instrumentos de investigación aplicados, la entrevista definida en el Apéndice L se encuentra que el 66.7% del personal afirma que no existe un protocolo formal de comunicación, esto genera los problemas de comunicación y coordinación entre los diferentes involucrados.

6.1.3 Los análisis detallados en la sección 4.3.1 del proceso de Identificación de Vulnerabilidades de Red indican que no se identifican actividades sin valor añadido. Sin embargo, se observan desperdicios principalmente asociados con aspectos relacionados con el inventario y movimiento en dicho proceso

6.1.4 Al realizar la simulación con Bizagi, se ha calculado un tiempo promedio de 15 horas y 58 minutos para el proceso de Identificación de Vulnerabilidades de Red, reforzando la conclusión anterior sobre la eficiencia del proceso señalando áreas específicas para mejorar en términos de inventario y movimiento.

6.1.5 El análisis detallado del proceso de Análisis de Vulnerabilidades de Red en el Capítulo IV resalta la carencia de valor añadido en la actividad de notificación durante las reuniones de análisis. Este hallazgo subraya la necesidad de mejorar el proceso, enfocándose en la eliminación actividades que no contribuyen al valor general del procedimiento.

6.1.6 La identificación principal de desperdicios del proceso de Análisis de Vulnerabilidades de Red se relaciona con el tiempo de espera, esto se evidencia en la simulación donde se halla un tiempo promedio de 11 horas y 37 minutos.

6.1.7 Respecto al proceso de Mitigación de Vulnerabilidades de Red, los análisis realizados en la sección 4.3.3 revelan que cada una de las actividades contribuye con valor añadido al proceso.

6.1.8 Se destaca que la principal fuente de desperdicio con el proceso Mitigación de Vulnerabilidades de Red se relaciona con el tiempo de espera, como se demuestra en la simulación, evidenciando un tiempo promedio de 9 horas y 53 minutos.

6.2. Objetivo específico 2

En relación con el objetivo específico 2: Diseñar un marco de trabajo de la Gestión de Vulnerabilidades de Red para la Estandarización de las actividades de su ciclo de vida basado en las buenas prácticas internacionales, se concluye lo siguiente:

6.2.1 El análisis de brecha realizado en el Capítulo V identifica las oportunidades de mejora entre la situación actual y el estado ideal de la gestión de Vulnerabilidades de Red, las cuales permitieron realizar el rediseño de los procesos pertenecientes a la gestión de Vulnerabilidades de Red que se analizaron en el Capítulo IV.

6.2.2 Se encuentra que la capacitación del personal es un factor que ayuda a contribuir a la cultura organizacional de Symbiotic en temas de seguridad, esto se evidencia en la sección 5.1.2.3.

6.2.3 La creación de una Política de Gestión de Vulnerabilidades de Red (VM-01, ver Anexo IV

6.2.4) permite que Symbiotic establezca las bases para un marco de trabajo sólido y alineado con los estándares de la industria.

6.2.5 El plan de comunicación de gestión de Vulnerabilidades de Red desarrollado para la solución (VM-02, ver Anexo V) establece un enfoque que garantiza el uso de estrategias y canales de comunicación esto permite abordar los desafíos de comunicación y coordinación existentes descritos en el Capítulo I.

6.2.6 El proceso de rediseño y modelado de los subprocesos se basa en las buenas prácticas de la industria, la revisión documental hecha en el Capítulo IV y la revisión literaria realizada en el Capítulo II, así como en la retroalimentación de los sujetos de investigación.

6.2.7 Según lo datos obtenidos de análisis documental del Capítulo IV, se desarrolló un sistema de categorización que permite que las Vulnerabilidades de Red sean clasificadas y priorizadas en función de su gravedad y propensión a la explotación, esto se evidencia en el Anexo IV

6.2.8 Se desarrollaron diferentes tipos de reportes para estandarizar la documentación y comunicación de eventos relacionados a los procesos gestión de la temática estudiada, dando como solución a los problemas de notificación de las Vulnerabilidades de Red.

6.2.9 El rediseño del proceso de Identificación de Vulnerabilidades de Red muestra que existe un promedio de 5h 11m de ahorro de tiempo en comparación con el estado As Is, equivalente a un 32.38% como se evidencia en la Tabla 28.

6.2.10 Según lo evidenciado en la Tabla 30, se halla que el rediseño del proceso de Análisis y Priorización tiene un promedio de 2h 55m de ahorro de tiempo equivalente al 25.06%, en comparación con el proceso As Is.

6.2.11 La Tabla 31 muestra que rediseño del proceso de mitigación de Vulnerabilidades de Red tiene una reducción de tiempo 1h 18m referente 22.41%, según lo comparado con el proceso As Is.

6.3. Objetivo específico 3

En relación con el objetivo específico 3: Definir indicadores de desempeño (KPI) para la medición del rendimiento del proceso de gestión de Vulnerabilidades de Red en términos de las fases de su ciclo de vida, se concluye lo siguiente:

6.3.1 El desarrollo de un catálogo de KPI's (VM-06, Anexo VI) es un elemento esencial para Symbiotic. Esto se constató en el análisis de brecha ejecutado en el Capítulo V. El documento busca evaluar y mejorar los procesos definidos en la solución.

6.3.2 La selección adecuada de métricas se realizó mediante la aplicación de los instrumentos de investigación Apéndice Q y el Apéndice R.

6.3.3 Los KPIs del catálogo propuesto siguen el formato de la NIST SP 800-55 la cual es una guía para la medición de los protocolos de seguridad de la información.

6.3.4 Los KPI's definidos proporcionan datos cuantificables, lo que permite que la toma de decisiones se base en evidencias.

6.3.5 Alinear los KPI con los objetivos estratégicos de Symbiotic se considera fundamental para medir el progreso de la implementación de la gestión.

6.4. Objetivo general

En relación con el objetivo general: Proponer un Plan de Gestión de Vulnerabilidades de Red para la definición de un marco de trabajo que aborde las actividades de su ciclo de vida que se administran en el departamento de *IT Operations and Compliance* de Symbiotic, a partir del uso de las buenas prácticas de la industria, se concluye lo siguiente:

6.4.1 La propuesta de un Plan de Gestión de Vulnerabilidades de Red aborda de manera integral las actividades a lo largo del ciclo de vida de las vulnerabilidades. La implementación de este marco de trabajo proporciona una estructura sólida que guía la ejecución eficiente de procesos, desde la identificación hasta la mitigación, incorporando estándares reconocidos como el NIST SP 800-40 y CyBOK fortaleciendo así la postura de seguridad de Symbiotic.

6.4.2 La implementación del plan no solo fortalece la seguridad informática de Symbiotic, sino que también proporciona información cuantitativa y cualitativa valiosa a través de los KPIs. Esto facilita la toma de decisiones informadas al permitir una evaluación clara del estado de seguridad y la efectividad de las medidas implementadas.

6.4.3 Según los resultados obtenidos del cálculo del ROI realizado en la sección 5.4, se concluye que el proyecto es factible dado que la inversión inicial se recupera un 14.52%.

6.4.4 El análisis costo beneficio realizado en la sección 5.3 evidencia que el proyecto tiene un impacto positivo, debido a que la suma total de los ahorros anuales en los tres procesos asciende a $26,903.18, con un ahorro acumulado de $53,806.36 en dos años. Esto representa un porcentaje de ahorro del 52.72% en el costo total de ejecución.

7. Recomendaciones

En este capítulo se detallan las recomendaciones que el investigador considera importantes para que el desarrollo del proyecto sea adecuado. Así mismo, este documento presenta las sugerencias desarrolladas para el TFG y se encuentran organizadas según cada objetivo planteado en este documento.

7.1. Objetivo específico 1

En relación con el objetivo específico 1: Analizar la situación actual de la gestión de Vulnerabilidades de Red para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria, se recomienda lo siguiente:

7.1.1 Delegar al *IT Compliance Agent* para que sea el responsable de mantener actualizada la documentación y los repositorios creados para cada uno de los procesos definidos en la solución.

7.1.2 Utilizar toda la documentación realizada con el objetivo de apoyar los diferentes procesos de gestión de Vulnerabilidades de Red de Symbiotic para promover la estandarización.

7.1.3 Establecer sesiones de trabajo grupales para compartir el conocimiento adquirido durante el proceso de gestión de Vulnerabilidades de Red, con el objetivo de identificar patrones que tengan la posibilidad de repetirse y diseñar o documentar escenarios de acción para cada uno de ellos y así darle más madurez al proceso.

7.1.4 Proporcionar formación y concienciación sobre la gestión de Vulnerabilidades de Red a los empleados de Symbiotic, no solo al personal del departamento de *IT Operations and Compliance*, para incentivar que se cree una cultura de ciberseguridad.

7.2. Objetivo específico 2

En relación con el objetivo específico 2: Diseñar un marco de trabajo de la Gestión de Vulnerabilidades de Red para la estandarización de las actividades de su ciclo de vida basado en las buenas prácticas internacionales, se recomienda lo siguiente:

7.2.1 Velar que para las actualizaciones futuras que se realicen al marco de trabajo planteado en este proyecto, se contemplen las buenas prácticas de la industria, debido a la experiencia y conocimiento de profesionales que desarrollan dichos estándares de la industria.

7.2.2 Se recomienda el uso de material oficial de apoyo sobre las mejores prácticas o estándares publicados por las organizaciones que velan por la seguridad ya sean NIST, PCI o ITIL, que fueron utilizadas como parte esencial del desarrollo de este trabajo final de graduación.

7.2.3 Tener presente que el marco de trabajo definido va a estar a disposición de ser adaptado según los estándares y marcos de trabajo seleccionados para que se ajusten a las operaciones y procesos de Symbiotic.

7.2.4 Para asegurarse de que los procedimientos establecidos en el marco de trabajo de gestión de Vulnerabilidades de Red funcionen correctamente, se deben realizar pruebas periódicas.

7.3. Objetivo específico 3

En relación con el objetivo específico 3: Definir indicadores de desempeño (KPI) para la medición del rendimiento del proceso de gestión de Vulnerabilidades de Red en términos de las fases de su ciclo de vida, se recomienda lo siguiente:

7.3.1 Integrar el formato establecido para el catálogo de KPI's a las diferentes métricas de otros procesos de la organización con el objetivo de estandarizar el proceso de control.
7.3.2 Realizar las reuniones de seguimiento mensuales y trimestrales establecidas en el Plan de Comunicación para generar retroalimentación por parte de los involucrados de la gestión, sobre modificaciones de métricas o estrategias, con el fin de medir el rendimiento de los procesos definidos en la solución.
7.3.3 Considerar el desarrollo de herramientas para facilitar la recopilación de los datos para las métricas.
7.3.4 Realizar análisis periódicos a las métricas con el propósito de identificar tendencias y patrones de desempeño para ayudar en la toma de decisiones.

7.4. Objetivo general

En relación con el objetivo general: Proponer un Plan de Gestión de Vulnerabilidades de Red para la definición de un marco de trabajo que aborde las actividades de su ciclo de vida que se administran en el departamento de *IT Operations and Compliance* de Symbiotic, a partir del uso de las buenas prácticas de la industria, se recomienda lo siguiente:

7.4.1 Se recomienda establecer un proceso de revisión periódica del Plan de Gestión de Vulnerabilidades de Red para asegurar su vigencia y efectividad. La ciberseguridad es un campo dinámico, y la actualización constante del plan garantizará que esté alineado con las últimas amenazas y tecnologías.
7.4.2 Considerando la importancia de la conciencia y compromiso del personal, se sugiere implementar programas regulares de capacitación en seguridad informática.
7.4.3 Fomentar la colaboración estrecha entre el departamento de IT Operations and Compliance y otros departamentos relevantes, como Desarrollo de Software y Administración de Proyectos, para asegurar una perspectiva holística y una respuesta coordinada ante incidentes de seguridad.
7.4.4 A pesar de los resultados favorables, se recomienda un seguimiento constante de los procesos para evaluar si se logran los ahorros deseados. Esto garantiza que se obtengan los beneficios esperados y que las inversiones sigan siendo rentables a largo plazo.
7.4.5 Desarrollar métricas de rendimiento (KPI) para medir y evaluar periódicamente los ahorros y los beneficios de las mejoras de procesos propuestas en la solución.

8. Referencias

Alfaro, J. (2017). *Metodología para la gestión de riesgos de TI basada en COBIT 5* [Graduación Metodología para la gestión de riesgos de TI basada en COBIT 5]. https://repositoriotec.tec.ac.cr/bitstream/handle/2238/11060/metodologia_gestion_riesgos_ti_basada_cobit5.pdf?sequence=1

Arias, F. (2012). *El Proyecto de Investigación Introducción a la metodología científica* (6ta ed.). Editorial Episteme.

AXELOS. (2019). *ITIL® 4 Foundation: IT Infrastructure Library*.

Bizagi. (2023). *Bizagi, one platform; every process. Guía de uso estudio.* https://help.bizagi.com/bpm-suite/es/index.html?glossary.htm

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *NIST SP 800-55 Perfomance Measurement Guide for Information Security* (Revision 1). National Institute of Standards and Technology.

Corona, M. (2019). *ITIL4 qué significa para mi y para mi organización*. ITIL4 qué significa para mi y para mi organización - YouTube

Council of Standards Australia. (2003). *AS/NZS 4360: 1999 Risk management*.

Cybersecurity & Infrastructure Security Agency. (2016). *Vulnerability Management Version 1.1*. CRR Supplemental Resource Guide. https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf

Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2018). *Fundamentals of Business Process Management*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-56509-4

Gartner. (2023a). *Definition of Business Process – Gartner Information Technology Glossary*. https://www.gartner.com/en/information-technology/glossary/business-process

Gartner. (2023b). *¿Qué es la planificación estratégica? Plantillas, pasos y guía de procesos* . https://www.gartner.es/es/insights/planificacion-estrategica

Goldsby, T., & Martichenko, R. (2005). *Lean Six Sigma Logistics*. J. Ross Publishing, Inc.

Google. (2023). *Cloud IDS overview*. https://cloud.google.com/intrusion-detection-system/docs/overview

Hallet, J., & Chen, C. (2021). *The Cyber Security Body of Knowledge* (1st ed., Vol. 1). The National Cyber Security Centre. https://www.cybok.org/media/downloads/Risk-Management--Governance-issue-1.0.pdf

Hernández, R., Fernández, C., & Baptista, M. (2010). *METODOLOGÍA de la investigación* (Quinta edición). McGRAW-HILL . https://www.icmujeres.gob.mx/wp-content/uploads/2020/05/Sampieri.Met.Inv.pdf

Instituto Nacional de Ciberseguridad de España. (2020). *Glosario de términos de ciberseguridad Una guía de aproximación para el empresario*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Scarfone K, & Souppaya M. (2022). *NIST SP 800-40 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. https://doi.org/10.6028/NIST.SP.800-40ver4

Ministerio de Trabajo y Seguridad Social. (2023, December 22). *Salario Mínimo Mensual. 2023*.

Organización de los Estados Americanos (OEA). (2019). *Marco NIST: Un abordaje integral de la Ciberseguridad*. OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf (oas.org)

PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4* (4th ed.). PCI Security Standards Council. https://www.pcisecuritystandards.org/document_library/?document=pci_dss

Real Academia Española. (2023a). *Brecha*. Diccionario de La Lengua Española. https://dle.rae.es/brecha

Real Academia Española. (2023b). *Gestión*. Diccionario de La Lengua Española. gestión | Definición | Diccionario de la lengua española | RAE - ASALE

Real Academia Española. (2023c). *Plan*. Diccionario de La Lengua Española. https://dle.rae.es/plan

Real Academia Española. (2023d). *Vulnerabilidad*. Diccionario de La Lengua Española. vulnerabilidad | Definición | Diccionario de la lengua española | RAE - ASALE

Shobhit, M. (2020, February 10). *Vulnerability Management, Vulnerability Management v/s Penetration Testing, Vulnerability Management Lifecycle*. https://grcmusings.com/vulnerability-management-vulnerability-management-v-s-penetration-testing-vulnerability-management-lifecycle/

Symbiotic. (2023). *Symbiotic*. Linkedin. https://cr.linkedin.com/company/symbiotic-com

Tripwire. (2023). *Tripwire ExpertOps Case Study* . Fortra. https://www.tripwire.com/resources/case-studies/it-operations-upgraded-vulnerability-management

Ulate, I., & Vargas, E. (2016). *Metodología para elaborar una tesis*. Editorial Universidad Estatal a Distancia.

Weller, J. (2018, October 18). *Guía completa para el análisis de brechas*. Smartsheet. https://es.smartsheet.com/gap-analysis-method-examples

Whitman, M., & Mattord, H. (2018). *Principles of Information Security* (6ta ed.). Cengage Learning.

9. Apéndices

9.1. Apéndice A Plantilla de Minuta

MINUTA DE REUNIÓN

Proyecto: Nombre exacto del mismo

Reunión No.	Es un núm. consecutivo para este proyecto	**Fecha:**	Indicar la fecha exacta de la reunión
Lugar:	Indicar dónde fue la reunión	**Hora Inicio/Finalización:**	xx:00 am. / yy:00 am
Objetivo de la reunión:			
Participantes:	Presentes:		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito
2	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito
3	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito

Próxima reunión

Temas a tratar	Fecha	Convocados
En la próxima reunión	indicar	Nombre de quiénes asistirán a esta próxima reunión.

Fuente: Elaboración propia (2023).

9.2. Apéndice B Plantilla Gestión de Cambios

Reporte de estado del proyecto

COD. DEL PROYECTO	[Código del proyecto]	PATROCINADOR	[Nombre de la empresa]
DIRECTOR DE PROYECTO	[Nombre del director de proyecto]	FECHA DE REPORTE	[Fecha de corte del reporte]

ESTATUS DEL PROYECTO

Estado general del proyecto

AVANCE GENERAL	ROJO	Resumen: [Escribir el estado general del proyecto aquí]

Indicadores clave

Componente	Estado	Notas
ALCANCE	VERDE	
AVANCE	ROJO	
RIESGOS	AMARILLO	

Clave de estado

ROJO — [Describa qué significa ROJO]
AMARILLO — [Describa qué significa AMARILLO]
VERDE — [Describa qué significa VERDE]

TRABAJO FINALIZADO	TRABAJO PARA EL SIGUIENTE PERÍODO

RIESGOS / PROBLEMAS / RFCs

Asunto	Tipo	Acciones	Responsable
1.	[Riesgo, problema o RFC]		

Fuente: Elaboración propia (2023

9.3. Apéndice C Cronograma de minutas de reuniones

Número de Reunión	Lugar – Fecha Hora Inicio / Final	Presentes	Objetivos	Temas Tratados
1	Google Meets Fecha: 1-8-23 Hora Inicio: 16:00 pm Hora Final: 17:00 pm	Prof.: Pedro Leiva Ariel Rodríguez	Revisión del anteproyecto, cronograma y tips para el inicio de TFG	Revisión del reglamento y el cronograma Agenda Reunión con la empresa Utilizar un gestor de referencias Revisión del anteproyecto
2	Google Meets Fecha: 10-8-23 Hora Inicio: 16:00 pm Hora Final: 17:00 pm	Prof. Pedro Leiva Ariel Rodríguez Representante: Guillermo Ávila	Reunión con el encargado de la organización	Revisión del reglamento Agenda Reunión con el profesor tutor Lectura obligatoria del libro: Metodología para elaborar una tesis
3	Google Meets Fecha: 16-8-23 Hora Inicio: 11:00 am Hora Final: 12:00 pm	Prof.: Pedro Leiva Ariel Rodríguez	Revisión capítulo 1 y capítulo 2	Revisión capítulo 1 Definición capítulo 2
4	Google Meets Fecha: 23-8-23 Hora Inicio: 14:30 pm Hora Final: 15:30 pm	Prof.: Pedro Leiva Ariel Rodríguez	Revisión del avance del entregable del Capítulo 3	Revisión marco metodológico Definición de variables de investigación
5	Google Meets Fecha: 30-8-23 Hora Inicio: 14:00 pm Hora Final: 15:00 pm	Prof.: Pedro Leiva Ariel Rodríguez	Revisión adelanto capítulo 3	Revisión de la tabla de variables de investigación Revisión de la tabla de operacionalización
6	Google Meets Fecha: 6-9-23 Hora Inicio: 11:00 am Hora Final: 12:00 pm	Prof.: Pedro Leiva Ariel Rodríguez	Revisión avance capítulo 4	Revisión aplicación de instrumentos de investigación Revisión del Análisis de la situación actual
7	Google Meets Fecha: 14-9-23 Hora Inicio: 14:00 pm Hora Final: 15:00 pm	Prof.: Pedro Leiva Ariel Rodríguez	Revisión avance capítulo 4	Revisión del: Modelado de Procesos "As Is" Análisis de los Procesos
8	Google Meets Fecha: 20-9-23 Hora Inicio: 16:00 pm Hora Final: 17:00 pm	Prof. Pedro Leiva Ariel Rodríguez Representante: Guillermo Ávila	Segunda reunión con el encargado de la organización	Revisiones entregables del producto Pertenecientes al capítulo 4 Revisión Avance general del proyecto

Número de Reunión	Lugar – Fecha Hora Inicio / Final	Presentes	Objetivos	Temas Tratados
9	Google Meets Fecha: 26-9-23 Hora Inicio: 11:00 am Hora Final: 12:00 pm	Prof.: Pedro Leiva Ariel Rodríguez	Revisión avance capítulo 5	Revisión del: Análisis de Brecha Identificación de Oportunidades de Mejora de los procesos
10	Google Meets Fecha: 5-10-23 Hora Inicio: 11:00 am Hora Final: 12:00 pm	Prof.: Pedro Leiva Ariel Rodríguez	Revisión avance capítulo 5	Revisión de los componentes de la solución Revisión de la estrategia de implementación
11	Google Meets Fecha: 12-10-23 Hora Inicio: 9:00 am Hora Final: 10:00 am	Ariel Rodríguez Representante: Guillermo Ávila	Revisión avance capítulo 5 Segunda evaluación por parte de la organización	Se validan los entregables de la empresa realizada para el proceso de gestión abordado en el proyecto. Se realiza la clasificación según los entregables presentados la segunda evaluación. Se presenta y valida la estrategia de implementación de la solución.
12	Google Meets Fecha: 12-10-23 Hora Inicio: 11:00 am Hora Final: 12:00 pm	Prof.: Pedro Leiva Ariel Rodríguez	Revisión avance capítulo 5	Revisión del análisis financiero Se acuerda entregar el capítulo 5 completo el domingo 15 de octubre.
13	Google Meets Fecha: 19-10-23 Hora Inicio: 11:00 am Hora Final: 11:34 am	Prof.: Pedro Leiva Ariel Rodríguez	Revisión total entregable capitulo 6 y 7	Revisión de las conclusiones y recomendaciones del proyecto. Se coordina la entrega del documento para revisión del profesor el domingo 22 de oct. de 23 y envió a la filóloga.
14	Google Meets Fecha: 26-10-23 Hora Inicio: 11:00 am Hora Final: 12:00 am	Prof.: Pedro Leiva Ariel Rodríguez	Revisión documento de la presentación del proyecto realizado por el estudiante.	Se dan correcciones a la ppt realizada por el estudiante y se le aconseja distribuir el tiempo en 5 min caps 1 al 3, 5 min cap 4 y 10 min caps 5 a 7
15	Google Meets Fecha: 31-10-23 Hora Inicio: 9:00 am Hora Final: 9:30 am	Ariel Rodríguez Representante: Guillermo Ávila	Reunión 3 con la organización	Se realiza la presentación del proyecto de manera formal al encargado de la organización y con base a la exposición se realiza la tercera evaluación.
16	Google Meets Fecha: 2-11-23 Hora Inicio: 11:00 am Hora Final: 12:00 am	Prof.: Pedro Leiva Ariel Rodríguez	Revisión final del documento con correcciones de la filóloga	Se acuerda que el estudiante puede presentar el documento final

PEDRO IGNACIO LEIVA CHINCHILLA (FIRMA)
Firmado digitalmente por PEDRO IGNACIO LEIVA CHINCHILLA (FIRMA)
Fecha: 2023.10.31 18:50:37 -06'00'

Fuente: Elaboración propia (2023).

9.4. Apéndice D Minuta reunión 1 con la organización

MINUTA DE REUNIÓN

Propuesta de un Plan de Gestión de Vulnerabilidades para el departamento de IT Operations and Compliance de Symbiotic

Reunión No.	02	Fecha:	10 de agosto 2023
Lugar:	Google Meets	Hora Inicio/Finalización:	4:00 pm. / 5:00 pm
Objetivo de la reunión:	Reunión con el encargado de la organización		
Participantes:	Presentes: Prof. Pedro Leiva, Ariel Rodríguez Representante: Guillermo Ávila		
	Ausentes: Ninguno		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Revisión del reglamento	-	Se acuerda usar hacer la carta de confidencialidad por los temas a tratar en el documento.
2	Agenda Reunión con el profesor tutor		La reunión será el martes 15 de agosto de 2023 2pm - 3pm
3	Lectura obligatoria del libro Metodología para elaborar una tesis Ileana Ulate Soto ; Elizarda Vargas Morúa	Recomendando para la elaboración del marco metodológico	Se acuerda montar el marco teórico y metodológico en con base al libro recomendado por el profesor Pedro.

Próxima reunión

Temas a tratar	Fecha	Convocados
Revisión del entregable del Capítulo 1 y adelanto del capítulo 2	15 de agosto	Profesor. Pedro Leiva y Ariel Rodríguez

Fuente: Elaboración propia (2023).

9.5. Apéndice E Minuta reunión 2 con la organización

MINUTA DE REUNIÓN

Propuesta de un Plan de Gestión de Vulnerabilidades para el departamento de IT Operations and Compliance de Symbiotic

Reunión No.	09	**Fecha:**	20 de setiembre 2023
Lugar:	Google Meets	**Hora Inicio/Finalización:**	4:00 pm. / 5:00 pm
Objetivo de la reunión:	Segunda reunión entre el representante de la empresa y el profesor tutor. Revisión del capítulo 4 análisis de resultados		
Participantes:	Presentes: Profesor: Pedro Leiva Encargado de la empresa: Guillermo Ávila Ariel Rodríguez		
	Ausentes: Ninguno		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Revisión entregables del producto pertenecientes al capítulo 5	Guillermo Ávila confirma que se ha estado realizando la documentación perteneciente al plan de Gestión de Vulnerabilidades.	Se acuerda una reunión en semana 10, para presentar al profesor tutor la documentación realizada por el estudiante en el Gestor de Conocimiento de la empresa.
2	Revisión Avance general del proyecto	El profesor Pedro comenta los avances del estudiante y comenta con Guillermo sobre el desempeño del estudiante en la empresa y sobre el proyecto en general.	N/A

Próxima reunión

Temas para tratar	Fecha	Convocados
Revisión capítulo 5 y propuesta de modelado del rediseño de los procesos.	28-9-23	Pedro Leiva Ariel Rodríguez

Fuente: Elaboración propia (2023).

9.6. Apéndice F Minuta reunión 3 con la organización

MINUTA DE REUNIÓN

Propuesta de un Plan de Gestión de Vulnerabilidades para el departamento de IT Operations and Compliance de Symbiotic

Reunión No.	15	**Fecha:**	31 noviembre 2023
Lugar:	Google Meets	**Hora Inicio/Finalización:**	9:00 am / 9:30 am
Objetivo de la reunión:	Presentación TFG Ariel Rodríguez		
Participantes:	Presentes: Ariel Rodriguez, Representante organización: Guillermo Ávila Profesor: Pedro Leiva		
	Ausentes: Ninguno		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Presentación TFG Ariel Rodríguez**	Se presenta de manera formal el documento realizado por el estudiante a la organización y los entregables realizados	Se aprueba el desarrollo del TFG del estudiante. Se dan recomendaciones para la presentación del estudiante en la presentación.
2	**Retroalimentación**	Se da retroalimentación por parte del profesor y de la empresa del desempeño del estudiante	Ninguno

Próxima reunión

Temas para tratar	Fecha	Convocados

Fuente: Elaboración propia (2023).

9.7. Apéndice G Minuta Análisis Financiero

MINUTA DE REUNIÓN

Propuesta de un Plan de Gestión de Vulnerabilidades para el departamento de IT Operations and Compliance de Symbiotic

Reunión No.	10	**Fecha:**	3 de octubre 2023
Lugar:	Google Meets	**Hora Inicio/Finalización:**	2:40pm. / 3:10 pm
Objetivo de la reunión:	Recopilación de Información necesaria para el análisis financiero		
Participantes:	Presentes: Ariel Rodriguez, Javier Chacón y Guillermo Ávila		
	Ausentes: Ninguno		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Definición de horas semanales para cumplir tareas de gestión	20% de las horas destinadas, un día laboral a la semana	Se considera el dato para el análisis financiero.
2	Tiempo de entrenamiento	2 meses de entrenamiento, (1 mes de entrenamiento técnico y 1 mes de entrenamiento del puesto)	Se consideran los datos para el análisis financiero.
3	Cantidad de personas que se consideran contratar para apoyar	1 persona	Se considera el dato para el análisis financiero.
4	Consulta salario aproximado de los Manager de TI y de Seguridad	Salario aproximado IT Ops and Compliance Manager: ¢1,640,820 Salario aproximado Security and Monitoring Manager: ¢1,750,420 Salario aproximado Desarrollador Jefe: ¢2,075,640	Se consideran los datos para el análisis financiero.

Próxima reunión

Temas para tratar	Fecha	Convocados

Fuente: Elaboración propia (2023).

9.8. Apéndice H Bitácora Revisión Documental

Bitácora de Revisión Documental sobre la situación actual			
Id	Fecha	Nombre Documento	Hallazgo
RevD-01			
…			

Fuente: Elaboración propia (2023).

9.9. Apéndice I Bitácora de Observación

Bitácora de Observación del Proceso		
Id	Actividad Observada	Hallazgo
RevO-01		
RevO-n		

Fuente: Elaboración propia (2023).

9.10. Apéndice J Plantilla Análisis de Brecha

Análisis de Brecha				
Variable	Estado Actual	Estado Ideal	Brecha	Hallazgo
Variable 1				
Variable 2				
Variable n				

Fuente: Elaboración propia (2023).

9.11. Apéndice K Plantilla Perfil de Procesos

Plantilla Perfil de Procesos	
Objetivo	Explicar detalladamente el objetivo que cumple el proceso.
Dueño del proceso	Es la persona o entidad responsable de garantizar que el proceso cumpla.
Cliente	Persona que solicita el proceso.
Expectativas del cliente	
Disparador	Evento que inicia el proceso.
Actividades del proceso	Lista de actividades del proceso.
Interfases de entrada	Procesos que anteceden al proceso en cuestión.
Interfases de salida	Procesos que preceden al proceso en cuestión.
Recursos requeridos	Recursos humanos: Ejemplo: Ingeniero de Sitio Información, Documentos, Conocimientos: Ejemplo: Directrices de adquisición Entorno de Trabajo, Materiales, Infraestructura: Ejemplo: Sistema de información de adquisiciones
KPIs	Aquí se deben listar las medidas de rendimiento del proceso.
Observaciones	Datos adicionales

Fuente: Elaboración propia (2023).

9.12. Apéndice L Encuesta Situación Actual del Proceso

Encuesta TFG - Propuesta de un Plan de Gestión de Vulnerabilidades

La presente encuesta tiene como objetivo evaluar la situación actual de la gestión de vulnerabilidades en la organización de estudio. Entender el estado actual la capacidad para identificar, evaluar y abordar las vulnerabilidades de seguridad es esencial para tomar medidas proactivas y asegurar la confidencialidad, integridad y disponibilidad de los activos de información.

Las respuestas que se proporcionen en esta encuesta serán anónimas y confidenciales. Los resultados obtenidos permitirán tener una visión más clara de las fortalezas y áreas de mejora en relación con la gestión de vulnerabilidades. Esto ayudará a diseñar estrategias efectivas y alineadas con estándares reconocidos de seguridad, así como asignar los recursos necesarios para garantizar una gestión de vulnerabilidades más sólida y efectiva.

La encuesta consta de preguntas diseñadas para abordar diferentes aspectos de la gestión de vulnerabilidades en la organización. Las respuestas serán fundamentales para identificar desafíos, oportunidades y áreas críticas de atención.

Se agradece su participación y sus aportes en esta iniciativa para mejorar la postura de seguridad y proteger los activos de información de manera efectiva.

* Indica que la pregunta es obligatoria

1. Correo *

Encuesta sobre la situación actual del proceso de gestión de vulnerabilidades

2. ¿Está su organización actualmente implementando un proceso de gestión de vulnerabilidades? *

Marca solo un óvalo.

- Si
- No

3. ¿Cómo evaluaría la efectividad de su organización para identificar vulnerabilidades de seguridad en su infraestructura y sistemas? *

Marca solo un óvalo.

- Muy efectiva
- Efectiva
- Moderadamente efectiva
- Poco efectiva
- Inefectiva

4. ¿Se realizan evaluaciones regulares de seguridad para identificar posibles vulnerabilidades? Si es así, ¿con qué frecuencia? *

Marca solo un óvalo.

- Mensualmente
- Trimestralmente
- Semestralmente
- Anualmente
- No realizamos evaluaciones de seguridad

5. ¿Existe un procedimiento claro para la mitigación y resolución de vulnerabilidades una vez que son identificadas? *

Marca solo un óvalo.

- Sí, con pasos específicos y plazos definidos
- Sí, pero sin plazos definidos
- No, no hay un procedimiento establecido

6. ¿Se lleva a cabo una evaluación posterior a la mitigación para confirmar la resolución efectiva de las vulnerabilidades? *

Marca solo un óvalo.

- Siempre
- A veces
- Raramente
- Nunca

7. ¿Cómo se comunica la existencia de vulnerabilidades y las medidas tomadas a las partes interesadas? *

Marca solo un óvalo.

- Mediante informes detallados y actualizados
- A través de correos electrónicos
- En reuniones periódicas
- No se comunica de manera formal

8. ¿Existe un proceso para el análisis post-mortem de incidentes y vulnerabilidades con el objetivo de mejorar el proceso? *

Marca solo un óvalo.

- Sí, se realiza regularmente
- Sí, pero de manera ocasional
- No se realiza

9. ¿Su organización se adhiere a estándares reconocidos de seguridad de la industria en su proceso de gestión de vulnerabilidades?

Marca solo un óvalo.

- Sí, estamos completamente alineados con los estándares
- Sí, seguimos los estándares en la medida de lo posible
- No, estamos en proceso de adaptación a los estándares
- No, no seguimos ningún estándar específico
- No estoy seguro

10. ¿Qué tan familiarizado está con los requisitos de seguridad establecidos por estándares como PCI DSS, CyBOK o NIST? *

Marca solo un óvalo.

- Muy familiarizado
- Moderadamente familiarizado
- Algo familiarizado
- Poco familiarizado
- No estoy familiarizado

11. ¿Cuál es el nivel de prioridad que su organización otorga al cumplimiento de estándares de seguridad reconocidos? *

Marca solo un óvalo.

- Muy alta prioridad
- Alta prioridad
- Prioridad moderada
- Baja prioridad
- No es una prioridad

12. ¿Cuáles diría que son las brechas más críticas en el proceso de gestión de vulnerabilidades de la organización actualmente? *

Marca solo un óvalo.

- ◯ Falta de personal especializado
- ◯ Falta de herramientas adecuadas
- ◯ Falta de documentación clara
- ◯ Falta de procesos eficientes
- ◯ Otro: _____

13. ¿Qué medidas ha tomado su organización para abordar las brechas identificadas en el proceso de gestión de vulnerabilidades? *

Marca solo un óvalo.

- ◯ Contratar personal adicional
- ◯ Adquirir nuevas herramientas y tecnologías
- ◯ Revisar y actualizar la documentación
- ◯ Rediseñar procesos y flujos de trabajo
- ◯ No hemos tomado medidas concretas aún

14. ¿En qué medida considera que abordar estas brechas tendrá un impacto positivo en la seguridad general de la organización? *

Marca solo un óvalo.

- ◯ Muy efectiva
- ◯ Efectiva
- ◯ Moderadamente efectiva
- ◯ Poco efectiva
- ◯ Inefectiva

Fuente: Elaboración propia (2023).

9.13. Apéndice M Minuta recolección de información Encuesta Situación Actual

MINUTA DE REUNIÓN

Propuesta de un Plan de Gestión de Vulnerabilidades para el departamento de IT Operations and Compliance de Symbiotic

Reunión No.	06	**Fecha:**	30 de agosto 2023
Lugar:	Google Meets	**Hora Inicio/Finalización:**	2:30 pm. / 3:00 pm
Objetivo de la reunión:	Aplicación de la encuesta Apéndice M Encuesta Situación Actual del Proceso		
Participantes:	Presentes: IT Ops and Compliance Manager (Guillermo Ávila) IT Compliance Agents x 2 Cloud Engineer Security and Monitoring Agent Facilitador de la encuesta: Ariel Rodríguez		
	Ausentes: Ninguno		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Aplicación de la encuesta Apéndice M Encuesta Situación Actual del Proceso**	El facilitador explica el procedimiento para la toma de datos de la encuesta de la situación actual a los participantes y se asegura que las respuestas de sean enviadas correctamente.	El IT Ops and Compliance Manager aprueba la realización de la encuesta para el TFG del estudiante Ariel, y se organiza una reunión interna para exponer los resultados hallados.

Próxima reunión

Temas a tratar	Fecha	Convocados

Fuente: Elaboración propia (2023).

9.14. Apéndice N Entrevista: Diseño del Proceso de Gestión de Vulnerabilidades de Red y Componentes del Plan

Entrevistador: Ariel Enrique Rodriguez Cruz

Entrevistado: _____

Rol del entrevistado: _____

Fecha: _____ Hora Inicio: _____ Hora Final: _____

Lugar de la entrevista: _____

Preguntas:

Pregunta 1 ¿Podría ofrecer una descripción detallada de cómo la organización actualmente aborda la gestión de Vulnerabilidades de Red en sus sistemas y procesos?

Pregunta 2 ¿Cuáles son los objetivos principales que se persiguen al diseñar un proceso de Gestión de Vulnerabilidades de Red basado en las mejores prácticas internacionales?

Pregunta 3 En relación con el diseño del proceso, ¿cómo se están tomando en cuenta las mejores prácticas internacionales para la Estandarización de las actividades del ciclo de vida de las Vulnerabilidades de Red?

Pregunta 4 ¿Cuáles componentes considera esenciales y tiene previsto que se incorporen en el plan de gestión de Vulnerabilidades de Red para garantizar una administración completa y eficaz?

Pregunta 5 ¿Qué estrategias se están evaluando para llevar a cabo la identificación, clasificación y priorización de Vulnerabilidades de Red, tomando en consideración su impacto en las operaciones del negocio?

Pregunta 6 ¿De qué manera se tiene previsto que se gestionen las fases de mitigación y resolución de Vulnerabilidades de Red dentro del marco del proceso de gestión que se vaya a establecer?

Pregunta 7 Con respecto a la fase de evaluación posterior a la mitigación, ¿cuál es la perspectiva que la empresa busca garantizar para que las Vulnerabilidades de Red se aborden de manera eficaz?

Pregunta 8 ¿Cómo se pretende que se aborde la comunicación tanto de las Vulnerabilidades de Red identificadas como de las medidas adoptadas con las partes interesadas, incluyendo la protección de información sensible?

Pregunta 9 ¿Qué estrategias se contemplan para instaurar un proceso de mejora continua que permita mantener la vigencia y eficacia del proceso a lo largo del tiempo?

Pregunta 10 En términos de alineación con buenas prácticas internacionales, ¿cómo se planea garantizar que el proceso diseñado esté en consonancia con los estándares de seguridad reconocidos y las regulaciones aplicables?

Fuente: Elaboración propia (2023).

9.15. Apéndice O Aplicación del Apéndice N Entrevista: Diseño del Proceso de Gestión de Vulnerabilidades de Red y Componentes del Plan

MINUTA DE REUNIÓN

Propuesta de un Plan de Gestión de Vulnerabilidades para el departamento de IT Operations and Compliance de Symbiotic

Reunión No.	07	**Fecha:**	4 de setiembre 2023
Lugar:	Oficinas administrativas de Symbiotic Los Yoses, San Pedro. Montes de Oca. Condominio Emalfin. A#7	**Hora Inicio/Finalización:**	9:30 am. / 10:30 am
Objetivo de la reunión:	Aplicación del Apéndice N Entrevista: Diseño del Proceso de Gestión de Vulnerabilidades y Componentes del Plan		
Participantes:	Presentes: IT Ops and Compliance Manager (Guillermo Ávila) CTO (Javier Chacón) Facilitador de la entrevista: Ariel Rodríguez		
	Ausentes: Ninguno		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Aplicación del Apéndice N Entrevista: Diseño del Proceso de Gestión de Vulnerabilidades y Componentes del Plan	El IT Ops and Compliance Manager solicita que la entrevista se haga bajo supervisión del CTO.	El CTO aprueba la realización de la Entrevista: Diseño del Proceso de Gestión de Vulnerabilidades para el TFG del estudiante Ariel, y se organiza una reunión interna para exponer los resultados hallados.

Próxima reunión

Temas para tratar	Fecha	Convocados

Fuente: Elaboración propia (2023).

9.16. Apéndice P Resultados Entrevista: Diseño del Proceso de Gestión

Entrevistador: Ariel Enrique Rodriguez Cruz

Entrevistado: _Guillermo Ávila _____

Rol del entrevistado: _IT Ops and Compliance Manager _____

Fecha: _4 setiembre 2023_____ Hora Inicio: ___9:30 am_____ Hora Final: ___10:30 am__

Lugar de la entrevista: _ Oficinas administrativas de Symbiotic Los Yoses, San Pedro. Montes de Oca. Condominio Emalfin. A#7____

Preguntas:

Pregunta 1 ¿Podría ofrecer una descripción detallada de cómo la organización actualmente aborda la gestión de Vulnerabilidades de Red en sus sistemas y procesos?

R/ Actualmente, Symbiotic aborda la gestión de Vulnerabilidades de Red mediante un enfoque relacionado a la gestión de riesgos, sin hacer diferencia de ambos procesos. Además, se usan herramientas de escaneo de Vulnerabilidades de Red para identificar posibles debilidades en nuestros sistemas y aplicaciones.

Pregunta 2 ¿Cuáles son los objetivos principales que se persiguen al diseñar un proceso de Gestión de Vulnerabilidades de Red basado en las mejores prácticas internacionales?

R/ Los objetivos que la empresa busca alinear con la práctica:

- Identificar y mitigar proactivamente las Vulnerabilidades de Red antes de que puedan ser explotadas.
- Cumplir con los requisitos regulatorios y normativos aplicables.
- Establecer un enfoque de mejora continua en la gestión de Vulnerabilidades de Red.
- Establecer un conjunto de indicadores de desempeño que permita medir el rendimiento de las diferentes fases del ciclo de vida de las Vulnerabilidades de Red.

Pregunta 3 En relación con el diseño del proceso, ¿cómo se están tomando en cuenta las mejores prácticas internacionales para la Estandarización de las actividades del ciclo de vida de las Vulnerabilidades de Red?

R/ Actualmente dentro la organización, se está pasando por un proceso de certificación por ende se busca que el proceso de Vulnerabilidades de Red se adapte o cumpla según las mejores prácticas internacionales.

Pregunta 4 ¿Cuáles componentes considera esenciales y tiene previsto que se incorporen en el plan de gestión de Vulnerabilidades de Red para garantizar una administración completa y eficaz?

R/ Según lo definido por el CTO y IT Ops and Compliance Manager se deben considerar los siguientes componentes para el proceso de gestión de Vulnerabilidades de Red.

- Procedimientos claros para la identificación y evaluación de Vulnerabilidades de Red.
- Un sistema de priorización basado en el impacto y la criticidad.
- Procesos claro y definido de las etapas del ciclo de vida de las Vulnerabilidades de Red.
- Mecanismos de seguimiento y documentación de las acciones tomadas.
- Comunicación efectiva con partes interesadas internas y externas.

Pregunta 5 ¿Qué estrategias se están evaluando para llevar a cabo la identificación, clasificación y priorización de Vulnerabilidades de Red, tomando en consideración su impacto en las operaciones del negocio?

R/ Estamos evaluando estrategias que incluyen el uso de herramientas de escáneres de Vulnerabilidades de Red, análisis de amenazas y Vulnerabilidades de Red.

Pregunta 6 ¿De qué manera se tiene previsto que se gestionen las fases de mitigación y resolución de Vulnerabilidades de Red dentro del marco del proceso de gestión que se vaya a establecer?

R/ Planeamos gestionar las fases de mitigación y resolución de Vulnerabilidades de Red estableciendo un proceso escalonado que incluye:

- Evaluación y priorización de la vulnerabilidad.
- Planificación y asignación de recursos.
- Implementación de soluciones o parches.
- Pruebas y validación de la mitigación.

Pregunta 7 Con respecto a la fase de evaluación posterior a la mitigación, ¿cuál es la perspectiva que la empresa busca garantizar para que las Vulnerabilidades de Red se aborden de manera eficaz?

R/ La prioridad que tiene Symbiotic es asegurar que las Vulnerabilidades de Red sean abordadas de forma efectiva y asegurar el rendimiento de los procesos. Para esto Symbiotic busca establecer indicadores de desempeño que permita medir el rendimiento de las diferentes fases del ciclo de vida de las Vulnerabilidades de Red, ya que actualmente el ningún proceso cuenta con indicadores definidos.

Pregunta 8 ¿Cómo se pretende que se aborde la comunicación tanto de las Vulnerabilidades de Red identificadas como de las medidas adoptadas con las partes interesadas, incluyendo la protección de información sensible?

R/ A través de informes de seguridad periódicos, promoviendo el uso de plantillas de comunicación internas y comunicados de seguridad a las partes interesadas internas y externas.

Pregunta 9 ¿Qué estrategias se contemplan para instaurar un proceso de mejora continua que permita mantener la vigencia y eficacia del proceso a lo largo del tiempo?

R/ De momento lo acordado con reuniones de la alta gerencia se busca que planear alrededor de revisiones periódicamente del proceso de gestión de Vulnerabilidades de Red para aprender de incidentes pasados.

Pregunta 10 En términos de alineación con buenas prácticas internacionales, ¿cómo se planea garantizar que el proceso diseñado esté en consonancia con los estándares de seguridad reconocidos y las regulaciones aplicables?

R/ Debido al proceso de certificación que está pasando la empresa, Symbiotic se compromete a seguir las directrices y regulaciones establecidas por organizaciones PCI y NIST.

Fuente: Elaboración propia (2023).

9.17. Apéndice Q Factores Críticos de Éxito de los KPIs

Entrevistador: Ariel Enrique Rodriguez Cruz

Entrevistado: _Guillermo Ávila_____

Rol del entrevistado: ___IT Ops ans Compliance Manager_____

Fecha: ___13 -9-2023_____ Hora Inicio: ____10:00 am__ Hora Final: ____10:20 am___

Lugar de la entrevista: _Google Meets_____

Preguntas:

Pregunta 1 ¿Cuál considera que es el objetivo principal de implementar KPIs en la gestión de Vulnerabilidades de Red?

Medir y evaluar el desempeño del proceso de gestión de Vulnerabilidades de Red.

Identificar las amenazas cibernéticas en tiempo real.

Optimizar la comunicación con las partes interesadas.

Otro (especifique): _____

Pregunta 2 Desde su experiencia, ¿cuáles son los factores críticos que contribuyen al éxito en la definición y uso efectivo de los KPIs para la gestión de Vulnerabilidades de Red?

Definición clara de objetivos y metas.

Participación de la alta dirección.

Asignación adecuada de recursos.

Uso adecuado de herramientas de monitoreo.

Otro (especifique): _____

Pregunta 3 ¿Qué tipos de KPIs considera efectivos para medir el desempeño de la gestión de Vulnerabilidades de Red en una organización como Symbiotic?

Tiempo de respuesta a Vulnerabilidades de Red críticas.

Porcentaje de Vulnerabilidades de Red mitigadas con éxito.

Cumplimiento con estándares y regulaciones.

Nivel de conciencia de seguridad del personal.

Pregunta 4 En su opinión, ¿cómo deberían los KPIs reflejar la alineación con estándares reconocidos como el NIST 800-40, el CyBOK y el PCI DSS en el contexto de la propuesta del Plan de Gestión de Vulnerabilidades de Red?

Deben reflejar la adhesión a estándares específicos.

Deben medir la efectividad en la mitigación de Vulnerabilidades de Red.

Deben evaluar la comunicación de amenazas a las partes interesadas.

Otro (especifique): _____

Pregunta 5 ¿Qué desafíos anticipa en la implementación y seguimiento de los KPIs en el Departamento de IT Operations and Compliance de Symbiotic?

Falta de apoyo de la alta dirección.

Complejidad técnica en la medición.

Resistencia al cambio por parte del personal.

Otro (especifique): _____

Pregunta 6 ¿Qué factores organizacionales considera que podrían influir en la definición, medición y uso exitoso de los KPIs en la gestión de Vulnerabilidades de Red?

Cultura de seguridad sólida.

Colaboración interdepartamental.

Recursos financieros suficientes.

Otro (especifique): _____

Pregunta 7 ¿En qué medida cree que los KPIs podrían contribuir a la mejora continua de la seguridad informática y la mitigación de riesgos en la organización?

En gran medida.

Moderadamente.

En cierta medida.

En poca medida.

Fuente: Elaboración propia (2023).

9.18. Apéndice R Entrevista Sobre Definición de Indicadores

Entrevistador: Ariel Enrique Rodriguez Cruz

Entrevistado: _Guillermo Ávila_____

Rol del entrevistado: ___IT Ops ans Compliance Manager_____

Fecha: ___16 -9-2023_____ Hora Inicio: ____2:00 pm__ Hora Final: ____2:30 pm___

Lugar de la entrevista: _Google Meets_____

Preguntas:

Pregunta 1 ¿Qué aspectos consideraría relevantes para la implementación de indicadores clave de desempeño (KPI) para medir la efectividad de su proceso de gestión de Vulnerabilidades de Red?

R/ Que se utilice algún estándar para definir los indicadores, para que las personas responsables del proceso tengan un mismo nivel de entendimiento sobre la función de cada indicador.

Pregunta 2 ¿Cuáles de los siguientes aspectos del proceso de gestión de Vulnerabilidades de Red considera más críticos para la medición a través de KPI? (Seleccione todas las que apliquen)

Identificación de Vulnerabilidades de Red

Clasificación y priorización de Vulnerabilidades de Red

Mitigación y resolución de Vulnerabilidades de Red

Evaluación posterior a la mitigación

Comunicación de Vulnerabilidades de Red y medidas

Otros (por favor especificar) _____

Pregunta 3 ¿Qué tipo de indicadores clave de desempeño (KPI) cree que serían más efectivos para medir la identificación de Vulnerabilidades de Red?

R/ Cantidad de Vulnerabilidades de Red detectadas

Pregunta 4 ¿Cuáles serían los KPI más relevantes para medir la clasificación y priorización de Vulnerabilidades de Red?

Porcentaje de Vulnerabilidades de Red clasificadas según su impacto

Tiempo promedio de clasificación y priorización

Porcentaje de Vulnerabilidades de Red clasificadas que fueron mitigadas

Otros indicadores (por favor especificar) _____

Pregunta 5 ¿Qué KPI consideraría esenciales para medir la efectividad de la mitigación y resolución de Vulnerabilidades de Red?

Tiempo promedio para aplicar medidas de mitigación

Porcentaje de Vulnerabilidades de Red mitigadas con éxito

Tiempo promedio para implementar parches o soluciones temporales

Otras métricas (por favor especificar) _____

Pregunta 6 ¿Cuáles de los siguientes KPI serían valiosos para medir la evaluación posterior a la mitigación?

Número de incidentes relacionados con Vulnerabilidades de Red tras la mitigación

Porcentaje de Vulnerabilidades de Red reincidentes

Tiempo promedio de verificación de efectividad de mitigación

Otros indicadores (por favor especificar) _____

Pregunta 7 ¿Qué KPI serían apropiados para medir la efectividad de la comunicación de Vulnerabilidades de Red y medidas a las partes interesadas?

Tiempo promedio para comunicar Vulnerabilidades de Red críticas

Porcentaje de partes interesadas informadas a tiempo

Calidad de la documentación de comunicación

Otras métricas (por favor especificar) _____

Pregunta 8 ¿Qué KPI serían efectivos para medir la capacidad del proceso de gestionar Vulnerabilidades de Red en concordancia con políticas y regulaciones internas y externas?

Porcentaje de Vulnerabilidades de Red abordadas conforme a políticas internas

Cumplimiento con regulaciones externas (ej. GDPR, HIPAA, CyBOK, NIST, PCI)

Evaluación de conformidad con estándares de seguridad reconocidos

Otras métricas (por favor especificar) _____

Pregunta 9 ¿Considera relevante medir el impacto financiero del proceso de gestión de Vulnerabilidades de Red a través de indicadores clave de desempeño?

R/ Si, si es posible definir indicadores alrededor de los Costos del Grupo de Gestión Responsable de Vulnerabilidades de Red y el Costo de las herramientas de gestión de Vulnerabilidades de Red.

Pregunta 10 ¿Qué KPI serían relevantes para medir la capacidad del proceso de comunicar y divulgar adecuadamente las Vulnerabilidades de Red identificadas y las medidas tomadas?

Porcentaje de Vulnerabilidades de Red comunicadas a tiempo

Satisfacción de las partes interesadas con la comunicación

Número de Vulnerabilidades de Red con medidas comunicadas vs. sin comunicar

Otros indicadores (por favor especificar) _____

Pregunta 11 ¿Cómo se planea utilizar los resultados de los indicadores clave de desempeño para la toma de decisiones en la mejora del proceso de gestión de Vulnerabilidades de Red?

Identificar áreas de mejora y ajustar el proceso

Reconocer buenas prácticas y éxitos

Tomar decisiones estratégicas a nivel organizativo

No se ha definido aún

Otro_____

Fuente: Elaboración propia (2023).

9.19. Apéndice S Bitácora de Observación Proceso de Identificación

Id	Actividad Observada	Hallazgo
RevO-01	*Proceso de Identificar y Priorizar Vulnerabilidades de Red*	Al realizar la observación se encuentran hallazgos como: • No existe coordinación entre los dueños del proceso, además no hay una definición de plazos de respuesta en el proceso. • No se encuentran definidos los aspectos de priorización en general. • No existe un objetivo claro definido para la identificación de Vulnerabilidades de Red. • Actualmente no existe una persona o entidad responsable de garantizar que el proceso cumpla.
		1. El proceso inicia cuando la herramienta de monitoreo IDS genera una señal de actividad sospechosa. 2. El *Security and Monitoring Agent* recibe una señal de actividad sospechosa de la herramienta de monitoreo IDS. 3. El *Security and Monitoring Agent* se encarga de generar un informe específico sobre la señal de actividad sospechosa identificada. a. El informe debe contener: el nombre del evento, tipo de evento ocurrió, fecha del evento, componente dónde ocurrió el evento. 4. El *Security and Monitoring Agent* envia el informe al *Security and Monitoring Manager.* 5. El *Security and Monitoring Manager* genera una aprobación del informe. 6. El *Security and Monitoring* envía el informe al Programador jefe para reportar la actividad sospechosa. 7. El Programador jefe genera una respuesta de aprobación sobre el informe. 8. El Programador jefe envía la respuesta generada. 9. El *Security and Monitoring Manager* recibe la respuesta del Programador jefe. a. Si no se recibe una respuesta de aprobación, se vuelve a enviar el correo al Programador jefe. 10. El proceso termina cuando se validan las dos aprobaciones del informe generado.

Fuente: Elaboración propia, 2023.

9.20. Apéndice T Bitácora de Observación Proceso de Análisis

Id	Actividad Observada	Hallazgo
RevO-02	*Proceso de Analizar Vulnerabilidades de Red*	Al realizar la observación del proceso se encuentran hallazgos que están relacionados con el análisis de la Tabla 10: • El documento no tiene definido una categorización de Vulnerabilidades de Red, por ende, esto no se hace en la ejecución del proceso. • No se encuentran definidos los aspectos de priorización de Vulnerabilidades de Red para los diferentes componentes del sistema. • El objetivo del proceso es: Analizar los componentes del sistema que son afectados directamente por la vulnerabilidad identificada por la herramienta Google Cloud Intrusion Detection System IDS. • Actualmente no existe una persona o entidad responsable de garantizar que el proceso cumpla. • El proceso no cuenta con KPI´s definidos para su monitoreo.
		El proceso de análisis tiene el siguiente flujo: 1. El proceso inicia cuando *Security and Monitoring Manager* afirma la validación de aprobaciones sobre el informe generado. 2. El *Security and Monitoring Manager* agenda una reunión con Programador jefe y *IT Ops and Compliance Manager* para realizar el análisis de la vulnerabilidad. 3. El *Security and Monitoring* notifica sobre la reunión. 4. El Programador jefe y *IT Ops and Compliance Manager* reciben la notificación de la reunión. 5. El *Security and Monitoring Manager* se agrupa con el Programador jefe y *IT Ops and Compliance Manager* para realizar el análisis de la vulnerabilidad. a. El informe de análisis consta de investigar a que componente del sistema afecta directamente la vulnerabilidad y definir si afecta o no la operación de la aplicación. 6. El *Security and Monitoring Manager* envía el informe de análisis de la vulnerabilidad al *Chief Technology Officer,* para tener una aprobación.

		7. El *Chief Technology Officer* se encarga de tomar la decisión de aprobación. a. En caso de no tener aprobación, se solicita una reunión con el *Security and Monitoring* para obtener información con el fin de generar la respuesta. 8. El proceso termina cuando el El *Chief Technology Officer* la comunica la respuesta de aprobación.

Fuente: Elaboración propia, 2023.

9.21. Apéndice U Bitácora de Observación Proceso de Mitigación

Id	Actividad Observada	Hallazgo
RevO-03	*Proceso de Mitigar Vulnerabilidades de Red*	Mediante la observación encuentran los siguientes hallazgos: • No existe una metodología alineada a las buenas prácticas de la industria para la mitigación que englobe las pruebas de remediación. • No existe documentación (manuales de usuario o guías técnicas) acerca del uso de las herramientas que cuenta la organización. • El uso inadecuado de las herramientas o métodos de escaneo de Vulnerabilidades de Red tienen la posibilidad de dar lugar a falsos negativos o positivos. • No se toma en cuenta la aplicación de parches de seguridad, esto genera inconsistencia en la protección de los componentes de los sistemas.
		El proceso de mitigación tiene el siguiente flujo: 1. El proceso inicia una vez se recibe la respuesta de aprobación del *Chief Technology Officer.* 2. El *Security and Monitoring Manager* y el Programador jefe desarrollan una estrategia de pruebas para la vulnerabilidad. 3. El Programador jefe se encarga de realizar las pruebas de mitigación. 4. El *IT Ops and Compliance Manager* se encarga de supervisor las pruebas de mitigación. 5. El *IT Ops and Compliance Manager* se encarga de crear un reporte sobre los puntos clave obtenidos en las pruebas realizadas.

Id	Actividad Observada	Hallazgo
		a. El reporte contiene: nombre de la vulnerabilidad, componente de afectación, estrategia establecida, herramienta utilizada, fecha de pruebas y hallazgos. 6. El Programador jefe valida que se haya mitigado la vulnerabilidad. a. Si no, se vuelve a generar una estrategia de pruebas nuevas. b. Si se mitiga, se informa al *Security and Monitoring Manager* con el reporte de pruebas de mitigación realizado. 7. El proceso termina cuando *IT Ops and Compliance Manager*, sube el reporte de pruebas de mitigación al gestor de conocimiento de la empresa (Confluence).

Fuente: Elaboración propia, 2023.

9.22. Apéndice V Plantilla Análisis Valor Añadido

Actividad	VA	BVA	NVA
Actividad 1			
…..			
Actividad n			

Fuente: Elaboración propia, 2023.

9.23. Apéndice W Plantilla Análisis de Desperdicio

Act	Transporte innecesario	Movimiento	Tiempo de Espera	Inventario	Errores	Sobreproducción	Sobre procesar

Fuente: Elaboración propia, 2023.

9.24. Apéndice X Plantilla Análisis de Flujo

Actividad	Tiempo promedio de ejecución (minutos)	Tiempo promedio de espera (minutos)

Fuente: Elaboración propia, 2023.

9.25. Apéndice Y Plantilla del Catálogo de KPI

Campo	Data
Nombre del Indicador	Nombre en específico del indicador
Código del Indicador	Código de identificación del indicador
Objetivo Estratégico	Describe un logro deseado a nivel organizacional.
Objetivo de TI	Declaración de los resultados específicos que una organización busca lograr en relación con la seguridad de la información
Medida	Medida a que aplica el indicador
Tipo de Medida	
Formula	Cálculo del indicador
Aplicación Pruebas	Indicar en qué circunstancias se aplica que indicador
Frecuencia	Periodicidad de aplicación del indicador
Responsables	Personal encargado del indicador
Fuente de Datos	Lugar donde se acceden los datos para la aplicación del indicador
Formato del Informe	Tipo de representación gráfica que se utilizará para representar el indicador en la creación del reporte.

Fuente: Adaptado de (Chew et al., 2008, p. 51)

9.26. Apéndice Z Vulnerability Detection Report

	Document Template	Code VM-03	Last Review 19. 09. 2023	Page 1 de 1
	Vulnerability Detection Report	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Symbiotic Vulnerability Detection Report

Vulnerability Detection Report			
Report By		**Date of Report**	
Position		**Report Number**	

Vulnerability Alert Information

Alert Name	The name or title that uniquely identifies the event.
Alert Type	The category or classification of the event, such as security incident, system error, access violation, etc.
Date of the Alert	The date and time when the event occurred. It's important to provide both the date and time to accurately track and analyze events.
Location of the Alert	Specific environment or location where the event or alert was generated.
Alert Description	A detailed description of what happened during the event.

Involved Parties Information

People Involved		**Other Witnesses**	
Contact Involved		**Contact Witness**	

Approval

Supervisor Name	Signature	Date

Fuente: Realización propia 2023.

9.27.

9.28. Apéndice AA Plantilla Symbiotic Vulnerability Analysis Report

	Document Template	Code VM-04	Last Review 19. 09. 2023	Page 1 de 3
	Vulnerability Analysis Report	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Vulnerability Analysis Report

Vulnerability Analysis Report			
Report By		**Date of Report**	
Position		**Report Number**	

Vulnerability Analysis Information

Alert Name	The name or title that uniquely identifies the event.
Alert Type	The category or classification of the event, such as security incident, system error, access violation, etc.
Alert Description	A detailed description of what happened during the event. Include relevant information about any actions taken, consequences, or impacts.

Vulnerability Categorization

The system is based on understanding the level of importance of the system component, allowing the responsible parties for the process to prioritize more quickly and effectively.

- **Low** represents a basic component in the system, which means that this component does not significantly impact the availability level of the service that Symbiotic provides.
- **Medium** represents a medium-level component in the system, meaning that this component moderately affects the availability level of the service that Symbiotic offers.
- **Critical** is a critical component in the system, being a component that directly and significantly impacts the availability of the service provided by Symbiotic.

Location of the Alert	Specify the specific environment or location where the event or alert was generated.	
Specific Place of Vulnerability		
Critic Component	**Medium Component**	**Low Component**
Client Management Service (CMS)	*Gateways (Load Balancer)*	*SDK*
Payment Management Service (PMS)	*Cloud VPN*	
Cloud Run		
Cloud SQL		
Cloud Firebase		

	Document Template	Code VM-04	Last Review 19. 09. 2023	Page 1 de 3
	Vulnerability Analysis Report	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Vulnerability Prioritization

To contrast the risk prioritization levels of the vulnerabilities defined by Symbiotic, the "ASINZS 4360: 1999 Risk Management" standard defined by the (Council of Standards Australia, 2003) is used as a basis, based on this standard, the impact and probability criteria to be used in vulnerability management are defined, which are explained below.

Impact (I): This refers to the impact of the vulnerability on the project. Three levels are defined for this purpose, which are explained below:

Impact Table

Impact	Qualitative Value	Quantitative Value	Value
Low	Represents a low impact on component system availability	Financial loss of less than $10,000	1
Medium	It represents a medium impact on the availability of the component system.	Economic loss of more than $10,000 and less than $30,000	2
High	It represents a critical impact on the availability of the component system.	Economic loss greater than $30,000	3

Probability (P): It refers to the probability of a vulnerability occurring in the project, the probability refers to the level of access that an attacker could have to our components, on a scale of one to three, where:

Probability Table

Probability	Description	Quantitative Value	Qualitative Value
Unlikely	Represents the minimum possibility of occurrence, ranges from 0% to 33%.	1	Possibility of occurrence once in the project, components such as KMS, DB, Firebase should be considered.
Possible	There is a possibility of occurrence, this possibility occurs at an infrequent time and its ranges are defined between 33% and 66%.	2	Possibility of repeated occurrences or related to library deprecations or security patches.
HIgh	Represents the highest possibility of occurrence ranges from 66% to 100%.	3	High possibility of occurrence or significant probability of occurrence in the component exposed to the network SDK, Gateways, API's.

	Document Template	Code VM-04	Last Review 19. 09. 2023	Page 1 de 3
	Vulnerability Analysis Report	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Vulnerability Prioritization

Heat Map (I*P): It refers to the multiplication of the Impact by the probability, to obtain a real value.

- **Low Priority**: it is represented with green color and alludes to the result of the multiplication would be the values one and two.
- **Medium Priority:** it is represented by the color yellow and refers to the result of the multiplication, which would be values three or four.
- **High Priority:** it is represented with the color red and alludes to the result of the multiplication would be values six or nine.

Vulnerability Name	Impact	Probability	P * I	Priority

Additional Information

Comments or details

Approval

Supervisor Name	Signature	Date

Fuente: Elaboración propia, 2023.

9.29. Apéndice BB Symbiotic Vulnerability Remediation Report

	Document Template	Code VM-05	Last Review 29. 09. 2023	Page 1 de 2
	Vulnerability Remediation Report	Process Vulnerability Management	Date 29. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Vulnerability Remediation Report

Vulnerability Remediation Report			
Report By		**Date of Report**	
Position		**Report Number**	

Vulnerability Remediation Information

Vulnerability Name	The name or title that uniquely identifies the event.		
Affected Component	Name or description of the affected component		
Priority	High	Medium	Low
Status	Mitigated	No Mitigated	
Tools Employed	Detailed description of the tools used in the tests.		
Strategy Used	Detailed description of the strategy or methodology used in the tests.		
Recommendations	Provide clear and specific recommendations for mitigating or remediating this vulnerability. A detailed description of what happened during the event. Include relevant information about any actions taken, consequences, or impacts.		

	Document Template	Code VM-05	Last Review 29. 09. 2023	Page 1 de 2
	Vulnerability Remediation Report	Process Vulnerability Management	Date 29. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Additional Information

Comments or details

Approval

Supervisor Name	Signature	Date

Fuente: Elaboración propia, 2023.

10. Anexos

10.1. Anexo I Ciclo de Vida de BPM

1.4 The BPM Lifecycle 23

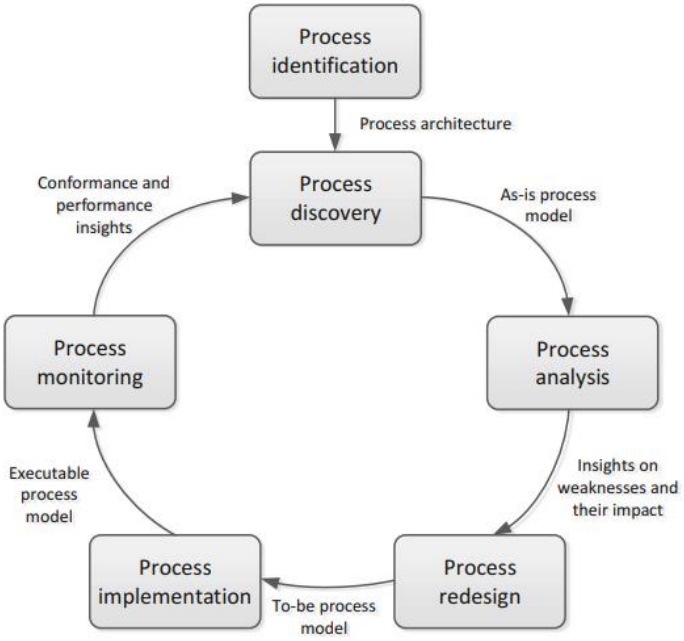
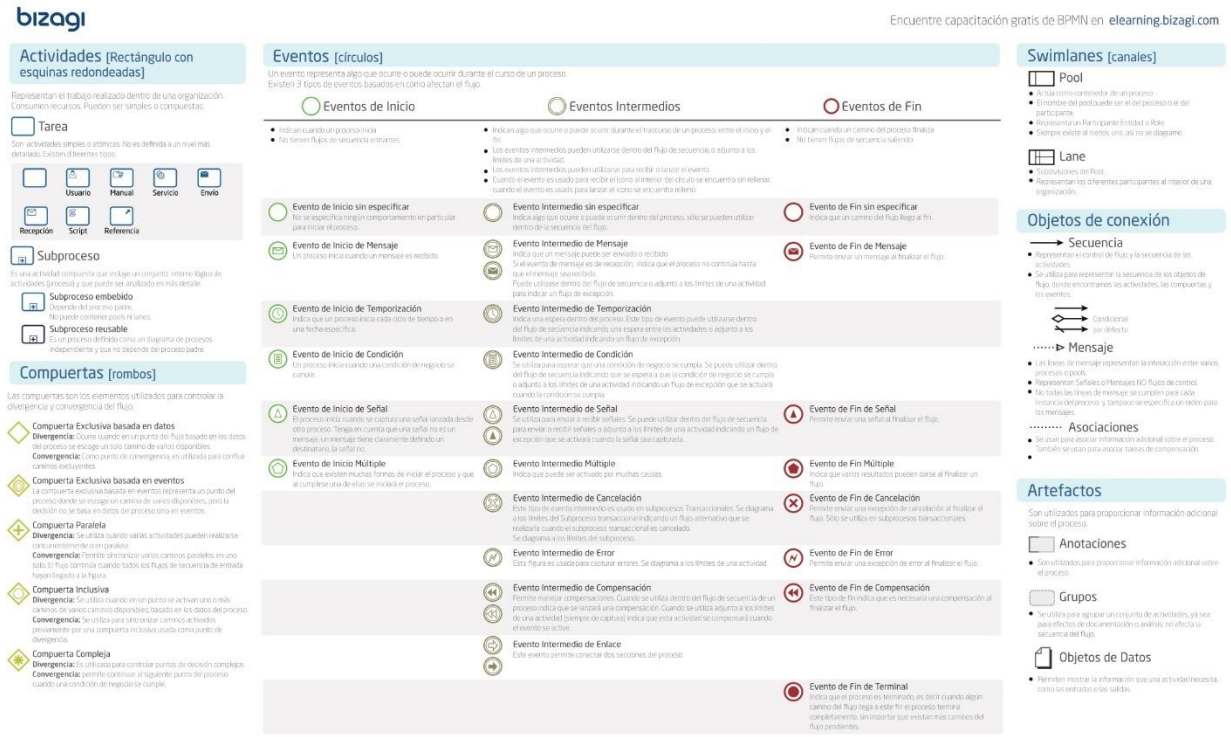


Fig. 1.7 The BPM lifecycle

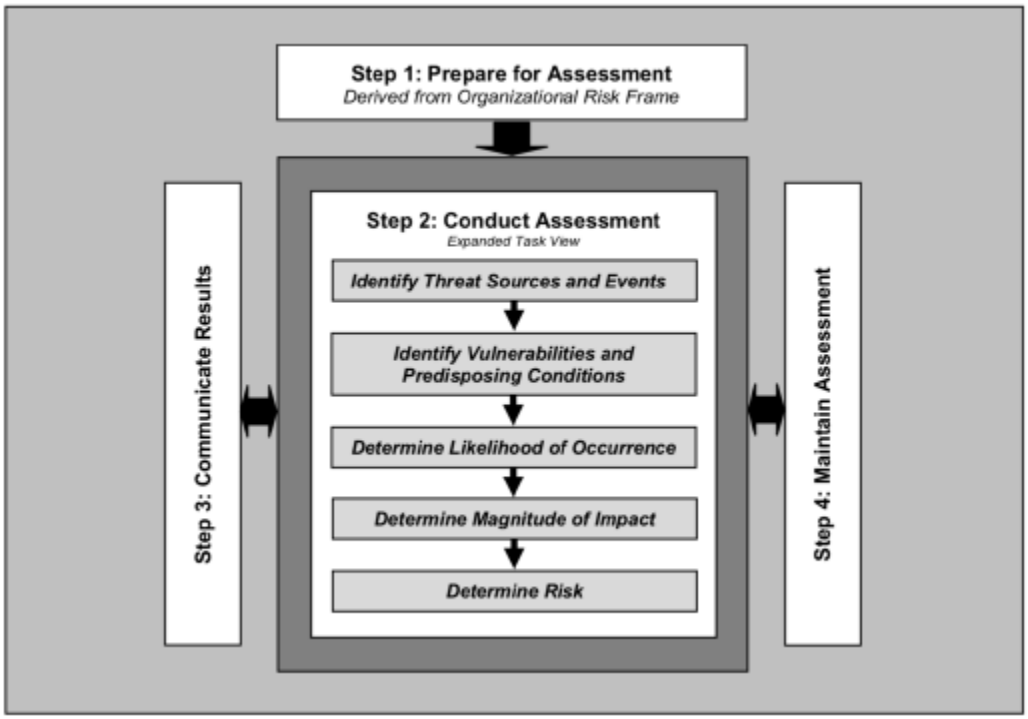
Fuente: Dumas, M. La Rosa, M (2018) *Fundamentals of Business Process Management*, pág. 51.

10.2. Anexo II BPMN Guía de Referencia



Fuente: Bizagi (2023) BPMN Guía de Referencia, tomado de: StencilBPMN_Esp'13 (bizagi.com).

10.3. Anexo III Ciclo de Gestión de Riesgos del CyBOK



Fuente: (Hallet & Chen, 2021, p. 34) *The Cyber Security Body of Knowledge*.

10.4. Anexo IV Política de Gestión de Vulnerabilidades de Red

	Document Policy	Code VM-01	Last Review 20. 09. 2023	Page 1 de 9
	Symbiotic Vulnerability Management Policy	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Vulnerability Management Policy

Introduction

The following document presents the policy and procedure for vulnerability management developed in Symbiotic. The objective of this document is to establish the working basis on which the IT Operations and Compliance department together with the security team in charge of Symbiotic defines the plans and mechanisms of action for vulnerability control.

With the implementation of this framework Symbiotic seeks to implement a generic vulnerability management model aligned with industry best practices, specifically aligned with the NIST SP 800-40 standard and the CyBOK. This document presents several sessions related to vulnerability management, which will be addressed in detail for the compliance process.

Likewise, the framework defined in this document seeks to simplify effective decision making in circumstances where it may be difficult to achieve information technology objectives that are affected by the presence of vulnerabilities, which could ultimately affect the achievement of business objectives.

Objective

Establish a structured framework for the vulnerability management process that is effective for the stages of its life cycle and provides standardization of activities that address vulnerabilities according to internationally recognized standards.

Scope

The intent of this framework is to strengthen the organization's cybersecurity by addressing all stages of the vulnerability management lifecycle, from identification to mitigation and continuous monitoring.

The established procedure for vulnerability management follows the steps established by NIST SP 800-40 Creating a patch and vulnerability management program. The scope of this document extends to the documentation of specific procedures, policies and guidelines to guide the execution of activities related to vulnerability management, as well as to the definition of roles and responsibilities of the actors involved.

Definitions

The following section presents a list of terms along with their respective meanings, with the aim of achieving a proper understanding of this document.

System Administrator: A person who manages the technical aspects of a system. (Mell et al., 2005)

Alert: An alert should reference an event or group of events of interest from a security perspective, representing both a symptom and a consequence of an attack. (Hallet & Chen, 2021)

	Document Policy	Code VM-01	Last Review 20. 09. 2023	Page 1 de 9
	Symbiotic Vulnerability Management Policy	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Threat: According to the authors (Mell et al., 2005), they define the concept of exploitation as follows: "Any circumstance or event, deliberate or not, with the potential to cause harm to a system."

Static Code Analysis (SAST): Miranda, C (2021) in his article "Static Code Analysis (SAST)" defines this concept as follows: "Static Application Security Testing (SAST), or static analysis, is a testing methodology that analyzes source code to find security vulnerabilities."

Vulnerability Risk Appetite: According to (Alfaro, 2017), it is the level of risk that an organization is prepared to accept, tolerate, or withstand at a given point in time (quantitative or qualitative).

Attack: (Hallet & Chen, 2021) define an attack as an attempt to gain unauthorized access to the services, resources, or information of an Information System, or an attempt to compromise the integrity of the system.

Confidentiality: (Hallet & Chen, 2021) defines this concept as the property that ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Consensus: Consensus (and similarly for consistency) refers to the mechanisms and property of achieving various types of agreement in values or coordination of states/entities, usually in the presence of specified failures. (Hallet & Chen, 2021)

Consumer: (Hallet & Chen, 2021) explains that a consumer is a natural person participating in a transaction that is not for commercial or professional purposes. A person may act as a consumer in some transactional contexts and as a non-consumer in others.

Control: (Alfaro, 2017) The term control defines policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives will be achieved, and unwanted events will be prevented, detected, and corrected.

Delegation: The act of granting access rights that one possesses to another principal. (Hallet & Chen, 2021)

Exploitation: According to NIST (2005) Special Publication 800-40 V2, exploitation is defined as follows: "It is a program that allows attackers to enter a system automatically." (Mell et al., 2005)

Event: Any observable occurrence in a network or system. It is a record of activity provided by a computer environment. (Hallet & Chen, 2021)

Impact: The result of a threat exploiting a vulnerability. (Hallet & Chen, 2021)

Impact: The magnitude of damage expected as a result of the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or availability of the information system. (Hallet & Chen, 2021)

	Document Policy	Code VM-01	Last Review 20. 09. 2023	Page 1 de 9
	Symbiotic Vulnerability Management Policy	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Incident: Actions conducted through computer networks resulting in a real or potential adverse effect on an information system and/or the information residing within it. (Hallet & Chen, 2021)

Integrity: The property that ensures that data is genuine, accurate, and protected against unauthorized modifications by users. (Hallet & Chen, 2021)

Patch and Vulnerability Management: According to (Mell et al., 2005) in NIST SP 800-40, this concept is defined as follows: It is a security practice designed to proactively prevent the exploitation of computer vulnerabilities existing within an organization.

Malware: According to the authors (Hallet & Chen, 2021), it is a program inserted into a system, usually covertly, with the intention of compromising the confidentiality, integrity, or availability of data, applications, or the victim's operating system, or otherwise disrupting or interfering with the victim.

Malware Analysis: The process of analyzing malware code and understanding its intended functionalities. (Hallet & Chen, 2021)

Malware Detection: The process of detecting the presence of malware on a system. (Hallet & Chen, 2021)

Security Model: High-level specifications of a system designed to enforce certain security policies. (Hallet & Chen, 2021)

Patches: According to NIST (2005) Special Publication 800-40 V2, this concept is defined as follows: "Additional code developed to resolve a problem in existing software." (Mell et al., 2005)

Penetration Test: According to Catoira, F (2012) in his article "Penetration Test, What Is It?" explains this concept as follows: "A penetration test consists of offensive tests against the existing defense mechanisms in the environment being analyzed. These tests range from analyzing physical and digital devices to analyzing the human factor using Social Engineering."

Security Policies: According to the (PCI Security Standards Council, 2022), security policies are defined as "the objectives and security principles of the entity."

Remediation Plan: (Mell et al., 2005) defines this concept as a plan to carry out the remediation of one or more threats or vulnerabilities facing an organization's system. The plan generally includes options for eliminating threats and vulnerabilities, as well as priorities for carrying out the remediation.

Probability: According to (Alfaro, 2017), probability is the measure or description of the likelihood of an event occurring.

Operational Procedures: According to the (PCI Security Standards Council, 2022), operational procedures describe how to perform activities and define the controls, methods, and processes followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

	Document Policy	Code VM-01	Last Review 20. 09. 2023	Page 1 de 9
	Symbiotic Vulnerability Management Policy	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

System Owner: An individual with managerial, operational, technical, and often budgetary responsibility in all aspects of an information technology system. (Mell et al., 2005)

Security: The authors (Hallet & Chen, 2021) define security in the context of malware analysis as a requirement that malware does not cause harm to connected systems and networks while running in the analysis environment.

System: According to (Mell et al., 2005), a system is a collection of information technology assets, processes, applications, and related resources that are under the same management and direct budgetary control; have the same mission or objective; have essentially the same security needs; and reside in the same general operational environment.

Intrusion Detection System (IDS): (Hallet & Chen, 2021) define IDS as a hardware or software product that collects and analyzes information from various areas within a computer or network to identify potential security breaches.

Remediation: The act of correcting a vulnerability or removing a threat. Three possible types of remediation are patch installation, configuration adjustment, and uninstallation of software applications. (Mell et al., 2005)

Risk: According to (Mell et al., 2005), risk is the probability of a particular threat exploiting a particular vulnerability.

Vulnerabilities: Vulnerabilities are flaws that malicious actors can exploit. These exploits can be used to gain more power or access, exceeding the allowed capacity of the computer system. (Mell et al., 2005)

Roles and Responsibilities

In the section, roles and responsibilities for Vulnerability Management are defined, considering the roles mentioned in the research subject's section:

Security and Monitoring Manager:

- Responsible for leading vulnerability management at Symbiotic.
- Define the strategy and security objectives related to vulnerability management.
- Oversee the vulnerability lifecycle process.
- Ensure a culture of security within the organization.

IT Ops and Compliance Manager:

- Ensure that IT operations comply with security policies and standards.
- Monitor the execution of vulnerability management procedures.
- Coordinate with IT teams for the proper implementation of mitigation measures.

	Document Policy	Code VM-01	Last Review 20. 09. 2023	Page 1 de 9
	Symbiotic Vulnerability Management Policy	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

IT Ops and Compliance Agent:

- Assist the IT Ops and Compliance Manager in implementing and monitoring security policies related to vulnerability management.
- Aid in identifying and reporting vulnerabilities in systems and applications.

Cloud Engineers:

- Ensure security in the cloud services used by Symbiotic.
- Collaborate in identifying and mitigating vulnerabilities related to cloud infrastructure.
- Implement security measures defined specifically in cloud environments.

Security and Monitoring Agent:

- Contribute to the identification and analysis of vulnerabilities.
- Participate in vulnerability tracking and monitoring activities.
- Assist in communicating vulnerabilities and their current status to relevant teams.

Project Manager IT Operations:

- Coordinate with other roles to ensure that projects adequately consider security and vulnerability management.

Security Awareness Training

This section defines the measures that Symbiotic as an organization takes to ensure the training and knowledge of employees on safety issues.

Employee Training

- All Symbiotic IT employees are required to undergo regular security awareness training, covering PCI DSS compliance requirements and best practices.
- The training seeks to empower employees with the knowledge necessary to effectively identify, report and address security vulnerabilities in the organization's systems and processes.
- The training covers topics such as security best practices, company policies and procedures related to vulnerability management, and will foster a culture of security throughout the organization.
- The training and coaching aim to strengthen the company's security posture and reduce the risk of potential security breaches.

	Document Policy	Code VM-01	Last Review 20. 09. 2023	Page 1 de 9
	Symbiotic Vulnerability Management Policy	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Policy Review

This policy will be reviewed annually or whenever there are significant changes in implementation or regulatory requirements, to ensure its relevance and effectiveness in maintaining PCI DSS compliance.

Compliance with the Policy

A finding of non-compliance with this policy will result in disciplinary action, as established by the organization.

Policy Acknowledgement

Acceptance of the Policy: All employees and relevant stakeholders must read and acknowledge their understanding and acceptance of this Vulnerability Management Policy.

Availability Levels

To understand the prioritization and categorization criteria established, it is necessary to understand how it affects the availability levels, which are established in conjunction with the Security and Monitoring Manager and the IT Ops and Compliance Manager, as listed below:

- Low: Service availability is less than 90%.
- Medium: Service availability is between 90% and 98%.
- High: Service availability is above 98%.

Categorization System

The following section defines the categorization system for the vulnerability analysis process. This system is based on knowing the degree of importance of the system component, allowing those responsible for the process to make a faster and more effective prioritization in the analysis report.

- **Low** represents a basic component in the system, this means that this component does not affect to a high degree the level of availability of the service that Symbiotic provides.
- **Medium** represents a medium component in the system, this means that this component affects to a medium degree the level of availability of the service that Symbiotic provides.
- **Critical** a critical component in the system, it is that component that directly affects in a high level of importance the availability of the service that Symbiotic provides.

Critic Component	Medium Component	Low Component
Client Management Service (CMS)	*Gateways (Load Balancer)*	*SDK*
Payment Management Service (PMS)	*Cloud VPN*	*Databases*
Cloud Run		
Cloud SQL		
Cloud Firebase		

	Document Policy	Code VM-01	Last Review 20. 09. 2023	Page 1 de 9
	Symbiotic Vulnerability Management Policy	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Prioritization System

To contrast the risk prioritization levels of the vulnerabilities defined by Symbiotic, the "ASINZS 4360: 1999 Risk Management" standard defined by the (Council of Standards Australia, 2003) is used as a basis, based on this standard, the impact and probability criteria to be used in vulnerability management are defined, which are explained below.

Impact (I): This refers to the impact of the vulnerability on the project. Three levels are defined for this purpose, which are explained below.

Impact	Qualitative Value	Quantitative Value	Value
Low	Represents a low impact on component system availability	Financial loss of less than $3,000	1
Medium	It represents a medium impact on the availability of the component system.	Economic loss of more than $3,000 and less than $10,000	2
High	It represents a critical impact on the availability of the component system.	Economic loss greater than $10,000	3

Probability (P): It refers to the probability of a vulnerability occurring in the project, the probability refers to the level of access that an attacker could have to our components, on a scale of one to three, where:

Probability	Description	Quantitative Value	Qualitative Value
Unlikely	Represents the minimum possibility of occurrence, ranges from 0% to 33%.	1	Possibility of occurrence once in the project, components such as KMS, DB, Firebase should be considered.
Possible	There is a possibility of occurrence, this possibility occurs at an infrequent time and its ranges are defined between 33% and 66%.	2	Possibility of repeated occurrences or related to library deprecations or security patches.
HIgh	Represents the highest possibility of occurrence ranges from 66% to 100%.	3	High possibility of occurrence or significant probability of occurrence in the component exposed to the network SDK, Gateways, API's.

	Document Policy	Code VM-01	Last Review 20. 09. 2023	Page 1 de 9
	Symbiotic Vulnerability Management Policy	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Heat Map (I*P): It refers to the multiplication of the Impact by the probability, to obtain a real value.

- **Low Priority:** it is represented with green color and alludes to the result of the multiplication would be the values 1 - 2.
- **Medium Priority:** it is represented by the color yellow and refers to the result of the multiplication, which would be values 3 - 4.
- **High Priority:** it is represented with the color red and alludes to the result of the multiplication would be values 6 - 9.

Heat Map		**Impacto**		
		Low	Medium	High
Probabilidad	Valor	1	2	3
High	3	3	6	9
Possible	2	2	4	6
Unlikely	1	1	2	3

Bylaws applicable to the Vulnerability Management Procedure

This section defines the internal regulations for the execution of the vulnerability management process in Symbiotic's organizational environment.

Identification Process:

- Symbiotic establishes the use of vulnerability scanning and analysis tools to identify potential exposure points.
- Symbiotic's goal is to foster collaboration between development and operations teams to detect and report vulnerabilities.

Analysis Process:

- Analysis on vulnerabilities should understand their scope and potential impact.
- The root causes of vulnerabilities should be determined to address them effectively.
- The results of the vulnerability analysis should be documented in detail.
    - The analysis report consists of investigating which component of the system is directly affected by the vulnerability and defining whether it affects the operation of the application.

	Document Policy	Code VM-01	Last Review 20. 09. 2023	Page 1 de 9
	Symbiotic Vulnerability Management Policy	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Prioritization Process:

- Those responsible for the prioritization process shall assign priority levels to identified vulnerabilities based on their severity and potential risk.
- Prioritization shall be carried out in accordance with the security policies and standards established in the Prioritization System section.
- It is established that critical vulnerabilities, which have a quantitative rating of 6 or 9 according to the heat map, will be addressed as a matter of urgency.

Mitigation Process:

Those responsible for the mitigation process must plan and execute the mitigation strategy established to solve the vulnerability.

- The mitigation strategy vulnerabilities are established according to the priority levels assigned.
- Mitigation actions should be monitored to ensure that they are effectively implemented.
- Mitigation measures should be adequately documented in the mitigation report.
    - The report should contain at a minimum: the name of the vulnerability, component that was affected, strategy established, tool used, date of testing and findings.

Communication Process:

- Symbiotic defines a communication plan to inform stakeholders, further defines the mechanisms and tools to be used, ensuring a constant and effective communication flow for the Vulnerability Management Plan process.
- The communication plan will be carried out in accordance with the internal standards established by Symbiotic.
- The implementation of the vulnerability communication plan is subject to any project that Symbiotic, with the objective of prioritizing communication between team members and with the client.

Control process:

- Symbiotic proposes a catalog of performance indicators which defines KPI's for each stage of the vulnerability lifecycle.
- Continuous monitoring will be performed to ensure that vulnerabilities are handled in accordance with Symbiotic's security policies and standards.
- Periodic updates to this policy will be made to reflect changes in the threat environment and regulations.

10.5. Anexo V Plan de Comunicación de Vulnerabilidades de Red

	Document Plan	Code VM-02	Last Review 20. 09. 2023	Page 1 de 4
	Symbiotic Vulnerability Management Communication Plan	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Vulnerability Management Communication Plan

Abstract

This document defines the Symbiotic vulnerability communication plan. This document is an important component of an effective management strategy to help mitigate the risks associated with software vulnerabilities.

Communication Approach

The implementation of the vulnerability communication plan is subject to any Symbiotic project, with the objective of prioritizing communication between team members and with the client. It is necessary to define from the beginning the mechanisms and tools to be used, ensuring a constant and effective communication flow for the main process of the Vulnerability Management Plan.

Communication Strategy Planning

The following section defines the communication strategy that Symbiotic will apply for all communication related to vulnerability management.

Communication Strategy Planning Table

Strategy	Description
Communication with senior collaborators	Planned and scheduled meetings are implemented in advance, Symbiotic's directors and department managers will be informed of the strategies and tools that are part of the proposal for the management of vulnerabilities.
Communication in each department	Each manager, after being duly informed about the strategies and the way in which the vulnerability mitigation and control process will be carried out, will hold meetings with the staff of each department. These meetings will focus on communicating the proposal discussed and the tasks that correspond to the departmental level with respect to the objectives.
Sending information and training	It is proposed to send detailed information to the collaborators, through Symbiotic's email. In turn, if the process or department warrants it, employees will be informed about workshops and training, so that it will not be more difficult for them to implement the changes or work with the tools.

	Document Plan	Code VM-02	Last Review 20. 09. 2023	Page 1 de 4
	Symbiotic Vulnerability Management Communication Plan	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Roles and Responsibilities

This section defines the roles and responsibilities for Vulnerability Management, considering the roles mentioned in the research subject's section:

Security and Monitoring Manager:

- Responsible for communicating the classification and coordination of the resolution of reported vulnerabilities.

IT Ops and Compliance Manager:

- Responsible for communicating the monitoring and control of the resolution of vulnerabilities.

IT Ops and Compliance Agent:

- Responsible for supporting the monitoring and control, as well as creating the mitigation report.

Lead Programmer:

- Responsible for communicating the coordination resolution of reported vulnerabilities.

Security and Monitoring Agent:

- Responsible for identifying and notifying vulnerabilities that are detected in the company's IDS tool.

Vulnerability Communication Management Process

The following section defines the vulnerability communication management process.

- The Security and Monitoring Monitor analyzes the different vulnerability reports generated by Security and Monitoring Agent, these are centralized in a Slack channel called top-support.
- The Security and Monitoring Monitor will review and classify the reported vulnerabilities based on their severity and impact.
- The Security and Monitoring Monitor will work with the software development team to verify reported vulnerabilities and develop a remediation plan.
- The Security and Monitoring Monitor will periodically report back to the notifier on the status of the vulnerability.

	Document Plan	Code VM-02	Last Review 20. 09. 2023	Page 1 de 4
	Symbiotic Vulnerability Management Communication Plan	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Communication Channels

The following defines the communication channels that Symbiotic establishes as official for notifying and informing about actions related to vulnerability management.

- Definition of communication channels: Email, Slack, Jira ServiceDesk.
- Users who are or have access to the Symbiotic account and participate in the types of meetings related to vulnerability management will be sent regular updates on vulnerability strategy, service and response activities.
- Vulnerability coordinators and the software development team will communicate via a secure messaging system.
- Vulnerability notifiers will be contacted by email to provide updates on vulnerability status.

Meeting Plan

The meetings included in the vulnerability management process, the attendees and the purpose of each meeting are listed below.

Meeting	Description	Assistants
Acceptance criteria	Acceptance criteria are defined for each remediation strategy that is part of the vulnerability mitigation process.	*Security and Monitoring Manager* *IT Ops and Compliance Manager* *Project Manager IT Operations* *Lead Programmer*
Retrospective	At the end of the process, the results obtained by applying the tests are analyzed and the Product Owner validates whether he agrees with them.	*Security and Monitoring Manager* *Security and Monitoring Agent* *IT Ops and Compliance Manager* *IT Compliance Agent* *Project Manager IT Operations* *Lead Programmer*
Vulnerability analysis	The purpose of the meeting is to create the vulnerability analysis report, which consists of investigating which component of the system is directly affected by the vulnerability, categorizing the level of the component and defining whether or not it affects the operation of the application.	*Security and Monitoring Manager* *IT Ops and Compliance Manager* *Lead Programmer*
Vulnerability remediation strategy planning meetings	Meetings to define task accomplishment, the team meets to develop activities and planning strategies to address vulnerabilities. Likewise, the meeting should assign remediation tasks to each working member related to vulnerability management.	*Security and Monitoring Manager* *Lead Programmer*

	Document Plan	Code VM-02	Last Review 20. 09. 2023	Page 1 de 4
	Symbiotic Vulnerability Management Communication Plan	Process Vulnerability Management	Date 20. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Meeting	Description	Assistants
Control and follow-up meetings	Meetings that are responsible for supervising the execution of the mitigation tests.	*IT Ops and Compliance Manager* *Lead Programmer*

Response Time

- Vulnerability managers will acknowledge receipt of a vulnerability report within one business day.
- Periodic updates on the status of the vulnerability shall be provided to the reporter every 5 working days.
- Approval of vulnerability identification reports, vulnerability analysis and mitigation reporting should take no more than two business days.
- Vulnerability remediation plans shall be approved and verified in no more than two business days for execution.

Disclosure policies

The following section defines the standards that Symbiotic personnel must follow for the disclosure of information related to vulnerability management:

- The Security and Monitoring Monitor and Lead Software Programmer will develop and implement a remediation strategy communication plan for each identified vulnerability.
- The Security and Monitoring Monitor and Lead Programmer determine whether and how to disclose vulnerability information to customers and other interested parties.
- Vulnerability managers will follow a responsible disclosure process to ensure that customers have sufficient time to apply updates and patches before vulnerabilities are publicly disclosed.

10.6. Anexo VI Catálogo de KPI's

	Document KPI's Catalog	Code VM-06	Last Review 19. 09. 2023	Page 1 de 7
	Vulnerability Management KPI's Catalog	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Symbiotic Vulnerability Management KPI's Catalog

KPI's Catalog

This document aims to ensure that the Key Performance Indicators (KPIs) defined for vulnerability management are aligned with the strategic objectives and information security goals of Symbiotic.

Metrics for the Identification Process

Based on the use of the KPI Table "Number of Vulnerabilities Detected," the metric for the identification process is defined. This metric provides a quantitative view of the effectiveness of the vulnerability identification process.

Indicator Name	Number of Vulnerabilities Detected
Indicator Code	GV-001
Strategic Objective	Strengthen the organization's security posture.
IT Objective	Ensure the security of Symbiotic's Tap on Phone system components against threats.
Measurement	Total number of vulnerabilities detected.
Measurement Type	Quantitative.
Formula	None.
Application in Testing	The metric will be used during regular security reviews of system components.
Frequency	Bi-weekly.
Responsible Party	*Security and Monitoring Agent.*
Data Source	Security alarm reports regarding suspicious activity signals.

	Document KPI's Catalog	Code VM-06	Last Review 19. 09. 2023	Page 1 de 7
	Vulnerability Management KPI's Catalog	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Metrics for the Analysis Process

The objective of the metric defined in the KPI Table "Percentage of Classified Vulnerabilities" is to measure the effectiveness in categorizing vulnerabilities so that they are addressed appropriately.

KPI Table: Percentage of Classified Vulnerabilities

Indicator Name	Percentage of Vulnerabilities Classified by System Component
Indicator Code	GV-002
Strategic Objective	Strengthen the organization's security posture.
IT Objective	Efficiently categorize detected vulnerabilities according to the system component they belong to.
Measurement	Percentage
Measurement Type	Quantitative
Formula	(Number of vulnerabilities classified by component / Total number of vulnerabilities) x 100
Application in Testing	The metric will be used during regular security reviews of system components.
Frequency	Monthly
Responsible Party	*Security and Monitoring Manager.* *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Data Source	Vulnerability analysis report.

	Document KPI's Catalog	Code VM-06	Last Review 19. 09. 2023	Page 1 de 7
	Vulnerability Management KPI's Catalog	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Metrics for the Prioritization Process

The metric related to the prioritization process is linked to the rate of critical vulnerabilities prioritized. The KPI Table "Rate of Prioritized Critical Vulnerabilities" provides more detailed information about this metric.

KPI Table: Rate of Prioritized Critical Vulnerabilities

Indicator Name	Critical Vulnerabilities Prioritization Rate
Indicator Code	GV-003
Strategic Objective	Enhance Symbiotic's security through the mitigation of critical vulnerabilities.
IT Objective	Ensure the security of critical information assets held by system components.
Measurement	Percentage
Measurement Type	Quantitative
Formula	(Number of Prioritized Critical Vulnerabilities / Total Number of Critical Vulnerabilities) x 100
Application in Testing	The metric will be used during regular security reviews of system components.
Frequency	Monthly
Responsible Party	*Security and Monitoring Manager.* *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Data Source	Vulnerability analysis report

	Document KPI's Catalog	Code VM-06	Last Review 19. 09. 2023	Page 1 de 7
	Vulnerability Management KPI's Catalog	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Metrics for the Mitigation Process

In the following section, performance indicators related to the vulnerability mitigation process are defined. The KPI Table "Percentage of Successfully Mitigated Vulnerabilities" allows for the definition of the percentage of vulnerabilities successfully mitigated, and the KPI Table "Average Time to Apply Mitigation Measures" establishes characteristics related to the average time to apply mitigation measures. In addition to supporting informed decision-making, these metrics also help assess the effectiveness of security measures within an organization and track potential risks.

KPI Table: Percentage of Successfully Mitigated Vulnerabilities

Indicator Name	Percentage of Successfully Mitigated Vulnerabilities
Indicator Code	GV-004
Strategic Objective	Enhance vulnerability resilience through effective mitigation.
IT Objective	Increase the percentage of successfully mitigated vulnerabilities that ensure a reduction in exposure to security threats.
Measurement	Percentage
Measurement Type	Quantitative
Formula	(Number of Successfully Mitigated Vulnerabilities / Number of Vulnerabilities Detected) x 100
Application in Testing	The metric will be used during regular security reviews of system components and whenever the mitigation process and subsequent monitoring process are performed.
Frequency	Monthly
Responsible Party	*Security and Monitoring Manager.* *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Data Source	Vulnerability analysis report, vulnerability mitigation report, and monitoring report

Below, the KPI Table "Average Time to Apply Mitigation Measures" is defined, allowing for the establishment of characteristics related to the average time it takes to apply mitigation measures.

	Document KPI's Catalog	Code VM-06	Last Review 19. 09. 2023	Page 1 de 7
	Vulnerability Management KPI's Catalog	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

KPI Table: Average Time to Apply Mitigation Measures

Indicator Name	Average Time to Apply Mitigation Measures
Indicator Code	GV-005
Strategic Objective	Improve vulnerability resilience through effective mitigation.
IT Objective	Reduce the time from detection to successful mitigation of vulnerabilities.
Measurement	Average time in days from detection to successful application of mitigation measures.
Measurement Type	Quantitative.
Formula	This indicator is directly measured in days.
Application in Testing	This metric applies to vulnerability monitoring and any mitigation cycle.
Frequency	Each time a new vulnerability is detected.
Responsible Party	*Security and Monitoring Manager.* *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Data Source	Security alarm reports regarding suspicious activity signals, vulnerability mitigation report

	Document KPI's Catalog	Code VM-06	Last Review 19. 09. 2023	Page 1 de 7
	Vulnerability Management KPI's Catalog	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Metrics for the Communication Process

This section establishes metrics for the communication process related to vulnerability management. These metrics help ensure information security within an organization. The defined metrics relate to the assessment of efficiency and speed in reporting vulnerabilities found in critical systems and applications.

KPI: Percentage of Vulnerabilities Communicated on Time

Indicator Name	Percentage of Vulnerabilities Communicated On Time
Indicator Code	GV-006
Strategic Objective	Improve the vulnerability communication process.
IT Objective	Ensure that all stakeholders in vulnerability management are effectively communicated with.
Measurement	Percentage
Measurement Type	Quantitative
Formula	(Number of vulnerabilities communicated on time / Total vulnerabilities detected) x 100
Application in Testing	This metric will be used during regular security reviews.
Frequency	Monthly
Responsible Party	*Security and Monitoring Manager.* *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Data Source	Vulnerability mitigation report and follow-up report

Below, the KPI Table "Average Time to Report Critical Vulnerabilities" is defined, allowing for the establishment of characteristics related to the average time it takes to report critical vulnerabilities. This metric aids in taking quick and effective measures in information security management.

	Document KPI's Catalog	Code VM-06	Last Review 19. 09. 2023	Page 1 de 7
	Vulnerability Management KPI's Catalog	Process Vulnerability Management	Date 19. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

KPI Table: Average Time to Report Critical Vulnerabilities

Indicator Name	Average Time to Communicate Critical Vulnerabilities
Indicator Code	GV-007
Strategic Objective	Enhance the efficiency of critical vulnerability communication.
IT Objective	Ensure that critical vulnerabilities are communicated in a timely manner for mitigation.
Measurement	Average time in hours (h)
Measurement Type	Quantitative
Formula	(Sum of times to communicate critical vulnerabilities) / (Number of critical vulnerabilities communicated)
Application in Testing	This metric will be used during regular security reviews.
Frequency	Monthly
Responsible Party	*Security and Monitoring Manager.* *Security and Monitoring Agent.* *IT Ops and Compliance Agent.*
Data Source	Vulnerability mitigation report and follow-up report

10.7. Anexo VII Procedimiento de Identificación de Vulnerabilidades de Red

	Document Policy	Code VM-07	Last Review 10. 09. 2023	Page 1 de 4
	Identification Vulnerability Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Vulnerability Identification Procedure

Introduction

The following document outlines the systematic approach to detecting and responding to security alerts generated by the Google Cloud Intrusion Detection System (IDS) tool. This procedure focuses on aligning all its activities and steps with what is established in the company's vulnerability management policy. This means that every action taken in the process, from the detection of suspicious activities to the generation and approval of detection reports, is designed to comply with the principles and guidelines set out in the vulnerability management policy.

Objective

To detect all vulnerability signals generated by the Google Cloud Intrusion Detection System (IDS) tool.

Process Owner

Security and Monitoring Agent.

Client

IT Operations and Compliance Department.

Client's Expectations

To ensure rigorous identification of the identified security alert.

Trigger

Suspicious activity signal generated by the IDS tool.

Input Interfaces

There are no processes preceding the process in question.

Output

Interfaces Analysis and Prioritization Process.

Human Resources

Security and Monitoring Agent.

Security and Monitoring Manager.

Information, Documents, Knowledge need it

The detection report for the alert signal.

Working Environment, Materials, Infrastructure

Google Cloud Intrusion Detection System IDS Tool.

KPIs

Number of Detected Vulnerabilities (Defined in the document Vulnerability Management KPI's Catalog)

	Document Policy	Code VM-07	Last Review 10. 09. 2023	Page 1 de 4
	Identification Vulnerability Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Procedure

Below is the proposed workflow for the vulnerability identification process using Google's Intrusion Detection System (IDS) tool. The following flow has been designed with the idea of ensuring that all signs of suspicious activity are identified, documented, and communicated in a timely manner.

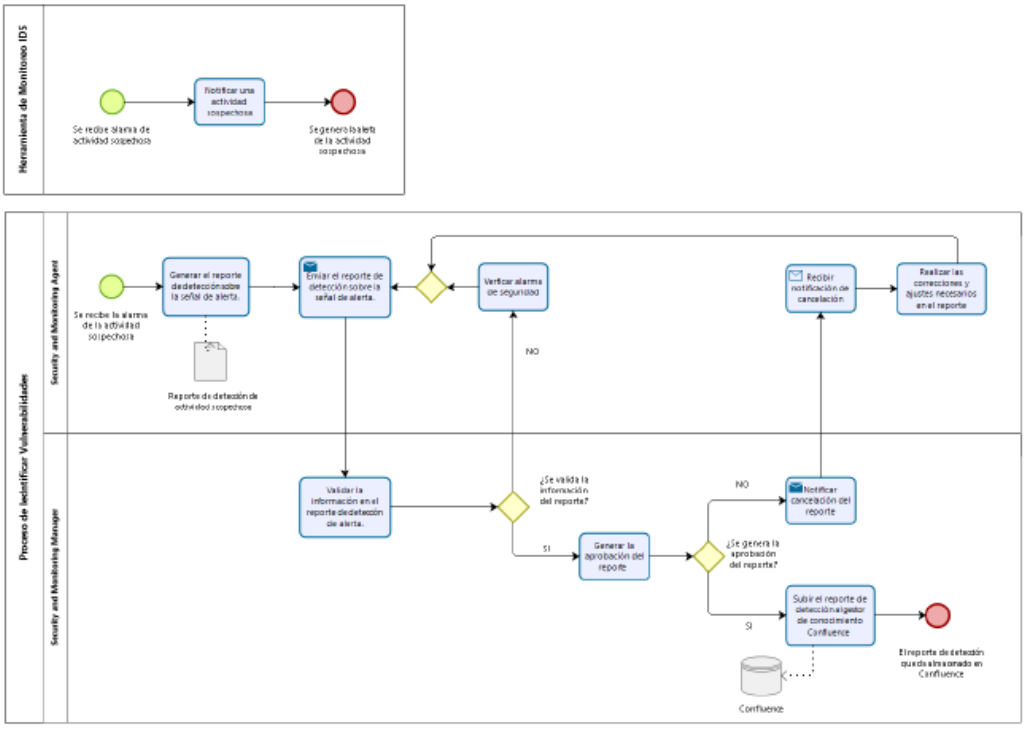
Process	Vulnerability Management		
Procedure	Vulnerability Identification Procedure		
ID	Activities	Responsible	Observation
Start Tool Process			
1	The IDS tool detects suspicious activity.	Google Cloud Intrusion Detection System	
2	The IDS tool notifies the suspicious activity.		
3	The suspicious activity alarm is generated		
Start			
1	The process begins when the suspicious activity alarm is received	Google Cloud Intrusion Detection System	
2	The Security and Monitoring Agent generates the detection report for the alert signal.	Security and Monitoring Agent	The detection report includes the event name, event type, event date, event description, environment where the alert signal was generated.
3	Send the detection report for the alert signal to the Security and Monitoring Manager.	Security and Monitoring Agent	
4	Validates the information in the alert detection report.	Security and Monitoring Manager	
4.a	If not approved, verifies the alert and repeats steps from activity one to activity three.	Security and Monitoring Agent	
4.b	If approved, the process proceeds to the next step.	Security and Monitoring Manager	
5	Approval of the alert detection report.	Security and Monitoring Manager	

	Document Policy	Code VM-07	Last Review 10. 09. 2023	Page 1 de 4
	Identification Vulnerability Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

5.a	If the report is not approved, the decision is notified to the Security and Monitoring Agent, and necessary corrections and adjustments are made to the report.	Security and Monitoring Manager	The Security and Monitoring Agent makes the corrections and adjustments of the report.
5.a.1	The corrected report is sent to the Security and Monitoring Manager.	Security and Monitoring Agent	
5.b	If the report is approved, the process proceeds to the next step.	Security and Monitoring Manager	
6	Uploads the detection report to the Confluence knowledge manager.	Security and Monitoring Manager	
7	The process ends with the approved report uploaded to Confluence.	Security and Monitoring Manager	The report must be upload in the Vulnerability Detection Database carpet in the sub carpet of Vulnerability Management in Confluence.
End			

	Document Policy	Code VM-07	Last Review 10. 09. 2023	Page 1 de 4
	Identification Vulnerability Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Workflow Diagram



10.8. Anexo VIII Procedimiento de Análisis y Priorización de Vulnerabilidades de Red

	Document Policy	Code VM-08	Last Review 10. 09. 2023	Page 1 de 4
	Vulnerability Analysis Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Vulnerability Analysis Procedure

Introduction

The following document outlines the analysis process. The document also tries to categorizes and prioritizes the system components directly impacted by vulnerabilities detected through the Google Cloud Intrusion Detection System IDS. This systematic approach ensures that all reports of suspicious activity signals are categorized, prioritized, thoroughly documented, and promptly communicated. The process aims to enhance the organization's ability to proactively address vulnerabilities and bolster its cybersecurity posture.

Objective

Analyze the system components that are directly affected by the vulnerability identified by the Google Cloud Intrusion Detection System IDS.

Process Owner

Security and Monitoring Manager.

Client

IT Operations and Compliance Department.

Client's Expectations

Ensure a proper analysis of components affected by identified vulnerabilities.

Trigger

Receive the approved report on suspicious activity signals.

Input Interfaces

Vulnerability Identification Process.

Output

Vulnerability Mitigation Process.

Human Resources

Security and Monitoring Agent.

Security and Monitoring Manager.

Chief Technology Officer.

Information, Documents, Knowledge need it

The detection report for the alert signal.

Working Environment, Materials, Infrastructure

Google Cloud Intrusion Detection System IDS Tool.

Page 1 | 4

	Document Policy	Code VM-08	Last Review 10. 09. 2023	Page 1 de 4
	Vulnerability Analysis Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

KPIs

Percentage of Classified Vulnerabilities. (Defined in the document Vulnerability Management KPI's Catalog)

Critical Vulnerabilities Prioritization Rate. (Defined in the document Vulnerability Management KPI's Catalog)

Procedure

The process flow of Analyze and Prioritize has been designed with the aim of ensuring that all reports of suspicious activity signals are categorized, prioritized, documented, and communicated in a timely manner.

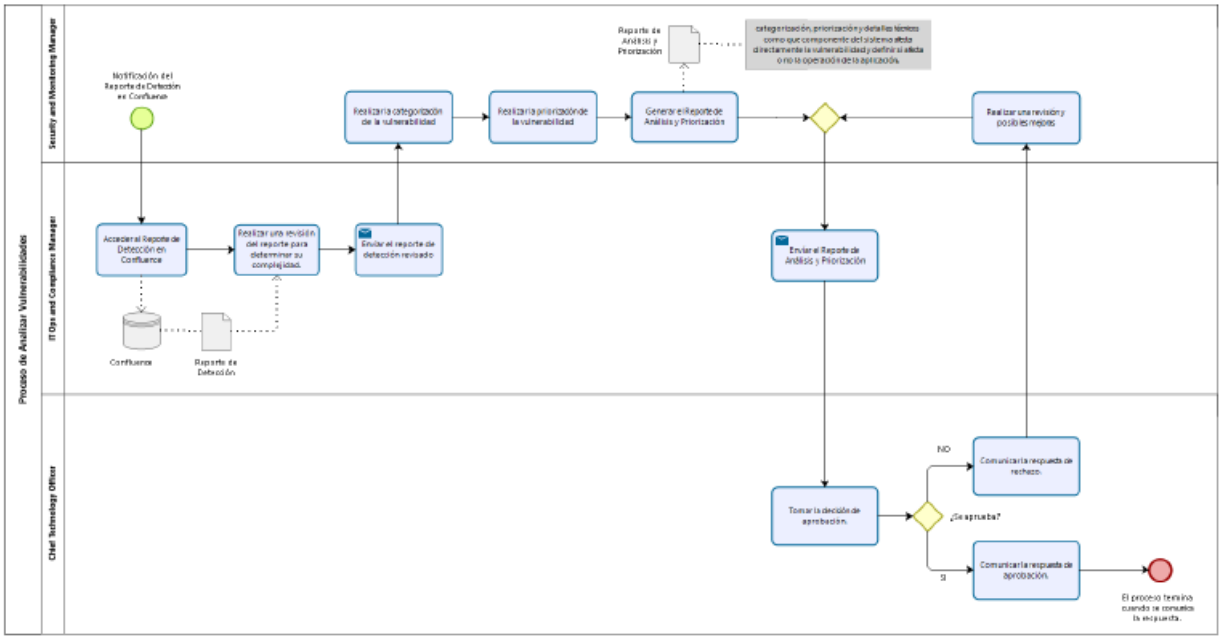
Process	Vulnerability Management		
Procedure	Vulnerability Analysis Procedure		
ID	Activities	Responsible	Observation
Start			
1	The process begins when the Security and Monitoring Manager notifies the IT Ops and Compliance Manager that the Detection Report is available on Confluence.	Security and Monitoring Manager	
2	Access the Signal Alert Detection Report on Confluence.	IT Ops and Compliance Manager	
3	Review the report to determine its complexity.	IT Ops and Compliance Manager	
4	Sends the revised report to the Security and Monitoring Manager.	IT Ops and Compliance Manager	
5	Categorizes the identified vulnerability in the report.	The Security and Monitoring Manager	
6	Prioritizes the vulnerability based on its categorization, probability of exploitation, and potential impact defined in the Vulnerability Management Policy.	The Security and Monitoring Manager	

	Document Policy	Code VM-08	Last Review 10. 09. 2023	Page 1 de 4
	Vulnerability Analysis Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

7	Generates the Analysis and Prioritization report.	The Security and Monitoring Manager, along with the IT Ops and Compliance Manager	The vulnerability analysis report includes categorization, prioritization, and technical details such as which system component is directly affected by the vulnerability and whether it affects the operation of the application.
8	Sends the vulnerability analysis report to the Chief Technology Officer for review.	IT Ops and Compliance Manager	
9	Make the approval decision.	Chief Technology Officer	
9.1	If the report is approved, the decision is communicated to the Security and Monitoring Manager.	Chief Technology Officer	
9.2	If the report is rejected, the report is returned to the Security and Monitoring Manager for further review and possible improvement.	Chief Technology Officer	
9.2.1	The Security and Monitoring Manager resends the revised report to the CTO for approval.	Chief Technology Officer	
10	The process concludes with the communication of the CTO's decision.	Chief Technology Officer	
End			

	Document Policy	Code VM-08	Last Review 10. 09. 2023	Page 1 de 4
	Vulnerability Analysis Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Workflow Diagram



10.9. Anexo IX Procedimiento de Remediación de Vulnerabilidades de Red

	Document Policy	Code VM-09	Last Review 10. 09. 2023	Page 1 de 4
	Vulnerability Remediation Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

Vulnerability Remediation Procedure

Introduction

The remediation procedure outlined here aims to effectively address vulnerabilities identified through the Google Cloud Intrusion Detection System (IDS) while adhering to industry best practices. It is owned by the Security and Monitoring Manager and serves the IT Operations and Compliance Department as its client.

Objective

Mitigate vulnerabilities identified by the Google Cloud Intrusion Detection System IDS in accordance with industry best practices.

Process Owner

Security and Monitoring Manager.

Client

IT Operations and Compliance Department.

Client's Expectations

Ensure appropriate mitigation of identified vulnerabilities.

Trigger

Receipt of approval from the Chief Technology Officer.

Input Interfaces

Vulnerability Analysis and Prioritization Process.

Output

No one.

Human Resources

Security and Monitoring Manager.

IT Ops and Compliance Agent.

Lead Programmer.

Information, Documents, Knowledge need it

Approved report of suspicious activity signal.

Analysis report on components affected by identified vulnerabilities.

Working Environment, Materials, Infrastructure

Company's knowledge management system (Confluence).

Page 1 | 4

	Document Policy	Code VM-09	Last Review 10. 09. 2023	Page 1 de 4
	Vulnerability Remediation Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

KPIs

Percentage of Successfully Mitigated Vulnerabilities. (Defined in the document Vulnerability Management KPI's Catalog)

Average Time to Apply Mitigation Measures. (Defined in the document Vulnerability Management KPI's Catalog)

Procedure

The process aims to enhance the organization's ability to proactively remediate vulnerabilities and bolster its cybersecurity posture.

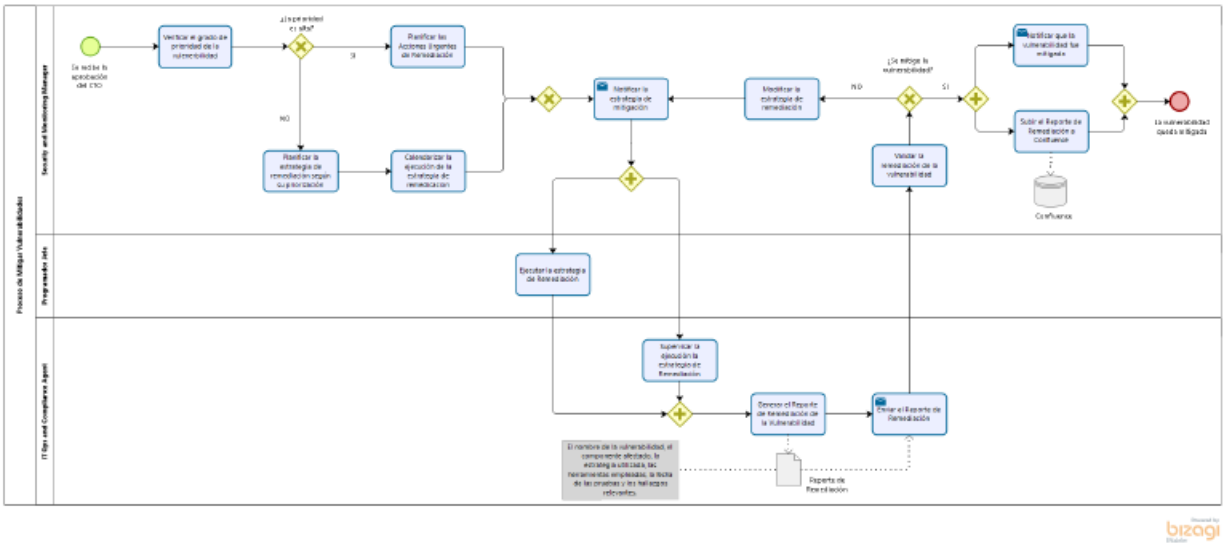
Process	Vulnerability Management		
Procedure	Vulnerability Remediation Procedure		
ID	Activities	Responsible	Observation
Start			
1	The process begins with approval from the CTO.		
2	Validates the vulnerability's priority.	Security and Monitoring Manager	
2.1	If the prioritization is high, urgent remediation actions are planned.	Security and Monitoring Manager	
2.2	If the prioritization is not high, a remediation strategy is planned based on its priority.	Security and Monitoring Manager	
2.2.1	The execution of the strategy is scheduled.	Security and Monitoring Manager	
3	Notifies the mitigation strategy.	Security and Monitoring Manager	
4	Executes the remediation strategy.	Lead Programmer	
5	Monitor the execution of the remediation strategy.	IT Ops and Compliance Agent	
6	Generates the Vulnerability Remediation Report.	IT Ops and Compliance Agent	The Remediation Report must have the name of the vulnerability, the affected component, the strategy used, the tools employed, the date of the tests, and the relevant findings.

	Document Policy	Code VM-09	Last Review 10. 09. 2023	Page 1 de 4
	Vulnerability Remediation Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

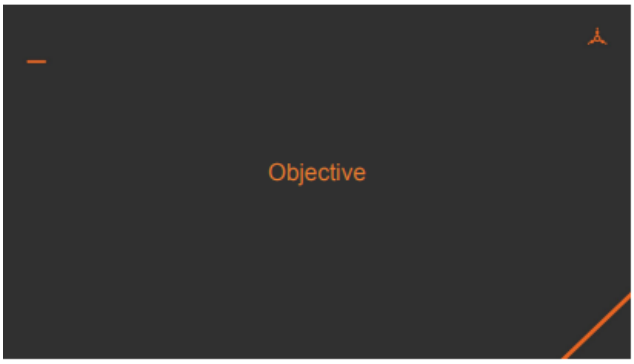
7	Sends the report to the Security and Monitoring Manager	IT Ops and Compliance Agent	
8	Validates vulnerability remediation. a. If it is not mitigated, the remediation strategy is modified, and steps 3 to 7 are executed. b. If it is mitigated, the process continues.	Security and Monitoring Manager	
9	Notifies that the vulnerability has been mitigated.	Security and Monitoring Manager	
10	Uploads the Vulnerability Remediation Report to Confluence.	Security and Monitoring Manager	
11	The process ends when the vulnerability is successfully mitigated.		
End			

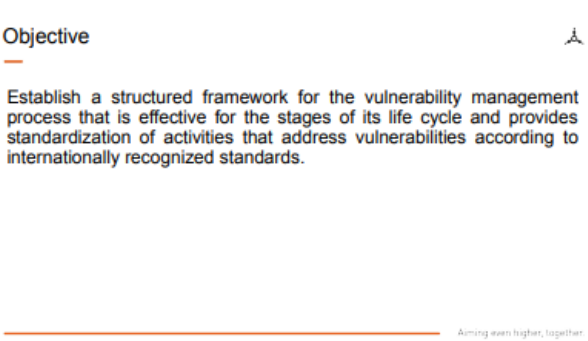
	Document Policy	Code VM-09	Last Review 10. 09. 2023	Page 1 de 4
	Vulnerability Remediation Procedure	Process Vulnerability Management	Date 10. 09. 2023	Version 1.0
		Department IT Operations and Compliance	Review by Security and Monitoring Manager	Approved by IT Ops and Compliance Manager

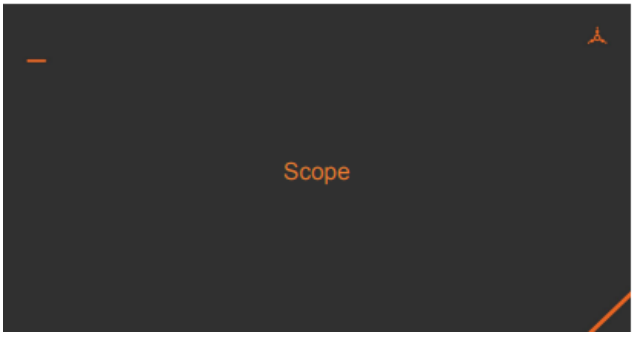
Workflow Diagram

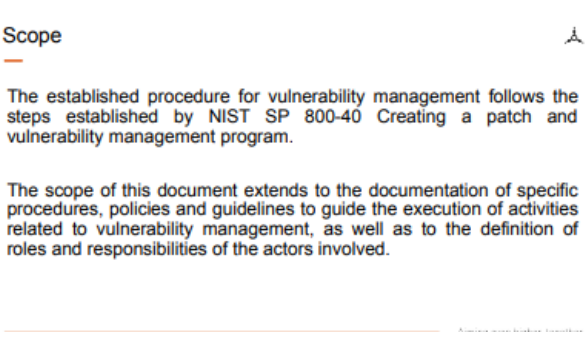


10.10. Anexo X Entrenamiento Política de Gestión de Vulnerabilidades de Red









Roles and Responsibilities

Security and Monitoring Manager:

Responsible for leading vulnerability management at Symbiotic.

Define the strategy and security objectives related to vulnerability management.

Oversee the vulnerability lifecycle process.

Ensure a culture of security within the organization.

IT Ops and Compliance Manager:

Ensure that IT operations comply with security policies and standards.

Monitor the execution of vulnerability management procedures.

Coordinate with IT teams for the proper implementation of mitigation measures.

Roles and Responsibilities

IT Ops and Compliance Agent:

Assist the IT Ops and Compliance Manager in implementing and monitoring security policies related to vulnerability management.

Aid in identifying and reporting vulnerabilities in systems and applications.

Cloud Engineers:

Ensure security in the cloud services used by Symbiotic.

Collaborate in identifying and mitigating vulnerabilities related to cloud infrastructure.

Implement security measures defined specifically in cloud environments.

Roles and Responsibilities

Security and Monitoring Agent:

Contribute to the identification and analysis of vulnerabilities.

Participate in vulnerability tracking and monitoring activities.

Assist in communicating vulnerabilities and their current status to relevant teams.

Project Manager IT Operations:

Coordinate with other roles to ensure that projects adequately consider security and vulnerability management.

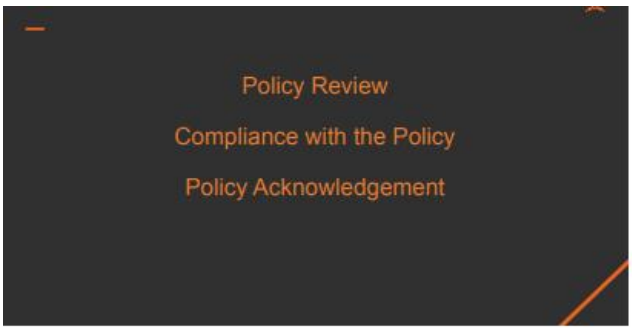
Security Awareness Training

All Symbiotic IT employees are required to undergo regular security awareness training, covering PCI DSS compliance requirements and best practices.

The training seeks to empower employees with the knowledge necessary to effectively identify, report and address security vulnerabilities in the organization's systems and processes.

The training covers topics such as security best practices, company policies and procedures related to vulnerability management, and will foster a culture of security throughout the organization.

The training and coaching aim to strengthen the company's security posture and reduce the risk of potential security breaches.



Policy Review

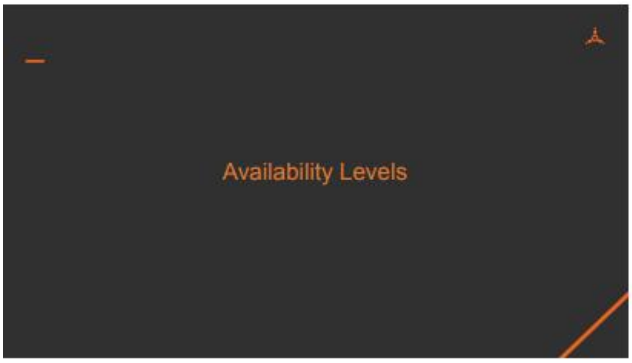
This policy will be reviewed annually or whenever there are significant changes in implementation or regulatory requirements, to ensure its relevance and effectiveness in maintaining PCI DSS compliance.

Compliance with the Policy

A finding of non-compliance with this policy will result in disciplinary action, as established by the organization.

Policy Acknowledgement

Acceptance of the Policy: All employees and relevant stakeholders must read and acknowledge their understanding and acceptance of this Vulnerability Management Policy.



Availability Levels

To understand the prioritization and categorization criteria established, it is necessary to understand how it affects the availability levels, which are established in conjunction with the Security and Monitoring Manager and the IT Ops and Compliance Manager, as listed below:

Low: Service availability is less than 90%.

Medium: Service availability is between 90% and 98%.

High: Service availability is above 98%.

Categorization System

This system is based on knowing the degree of importance of the system component, allowing those responsible for the process to make a faster and more effective prioritization in the analysis report.

Low represents a basic component in the system, this means that this component does not affect to a high degree the level of availability of the service that Symbiotic provides.

Medium represents a medium component in the system, this means that this component affects to a medium degree the level of availability of the service that Symbiotic provides.

Critical a critical component in the system, it is that component that directly affects in a high level of importance the availability of the service that Symbiotic provides.

Categorization System

Critic Component	Medium Component	Low Component
Client Management Service (CMS)	*Gateways (Load Balancer)*	*SDK*
Payment Management Service (PMS)	*Cloud VPN*	
Cloud Run		
Cloud SQL		
Cloud Firebase		

Prioritization System

Impact

Impact (I): This refers to the impact of the vulnerability on the project. Three levels are defined for this purpose, which are explained below:

Impact	Qualitative Value	Quantitative Value	Value
Low	Represents a low impact on component system availability	Financial loss of less than $10,000	1
Medium	It represents a medium impact on the availability of the component system.	Economic loss of more than $10,000 and less than $30,000	2
High	It represents a critical impact on the availability of the component system.	Economic loss greater than $30,000	3

Probability

Probability (P): It refers to the probability of a vulnerability occurring in the project, the probability refers to the level of access that an attacker could have to our components, on a scale of one to three, where:

Probability	Description	Quantitative Value	Qualitative Value
Unlikely	Represents the minimum possibility of occurrence, ranges from 0% to 33%.	1	Possibility of occurrence once in the project, components such as KMS, DB, Firebase should be considered.
Possible	There is a possibility of occurrence, this possibility occurs at an infrequent time and its ranges are defined between 33% and 66%.	2	Possibility of repeated occurrences or related to library deprecations or security patches.
High	Represents the highest possibility of occurrence ranges from 66% to 100%.	3	High possibility of occurrence or significant probability of occurrence in the component exposed to the network SDK, Gateways, APIs.

Heat Map (I * P)

Heat Map (I*P): It refers to the multiplication of the Impact by the probability, to obtain a real value.

Low Priority: it is represented with green color and alludes to the result of the multiplication would be the values one and two.

Medium Priority: it is represented by the color yellow and refers to the result of the multiplication, which would be values three or four.

High Priority: it is represented with the color red and alludes to the result of the multiplication would be values six or nine.

Heat Map (I * P)

Heat Map		Impacto		
		Low	Medium	High
Probabilidad	Value	1	2	3
High	3	3	6	9
Possible	2	2	4	6
Unlikely	1	1	2	3

Identification Process

Symbiotic establishes the use of vulnerability scanning and analysis tools to identify potential exposure points.

Symbiotic goal is to foster collaboration between development and operations teams to detect and report vulnerabilities.

Analysis Process

Analysis on vulnerabilities should understand their scope and potential impact.

The root causes of vulnerabilities should be determined to address them effectively.

The results of the vulnerability analysis should be documented in detail.

The analysis report consists of investigating which component of the system is directly affected by the vulnerability and defining whether it affects the operation of the application.

Prioritization Process

Those responsible for the prioritization process shall assign priority levels to identified vulnerabilities based on their severity and potential risk.

Prioritization shall be carried out in accordance with the security policies and standards established in the Prioritization System section.

It is established that critical vulnerabilities, which have a quantitative rating of 6 or 9 according to the heat map, will be addressed as a matter of urgency.

Mitigation Process

Those responsible for the mitigation process must plan and execute the mitigation strategy established to solve the vulnerability.

The mitigation strategy vulnerabilities are established according to the priority levels assigned.

Mitigation actions should be monitored to ensure that they are effectively implemented.

Mitigation measures should be adequately documented in the mitigation report.

The report should contain at a minimum: the name of the vulnerability, component that was affected, strategy established, tool used, date of testing and findings.

Communication Process

Symbiotic defines a communication plan to inform stakeholders, further defines the mechanisms and tools to be used, ensuring a constant and effective communication flow for the Vulnerability Management Plan process.

The communication plan will be carried out in accordance with the internal standards established by Symbiotic.

The implementation of the vulnerability communication plan is subject to any project that Symbiotic, with the objective of prioritizing communication between team members and with the client.

Control Process

Symbiotic proposes a catalog of performance indicators which defines KPI's for each stage of the vulnerability lifecycle.

Continuous monitoring will be performed to ensure that vulnerabilities are handled in accordance with Symbiotic's security policies and standards.

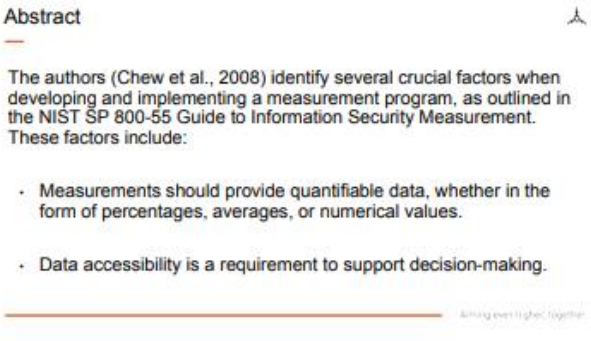
Periodic updates to this policy will be made to reflect changes in the threat environment and regulations.

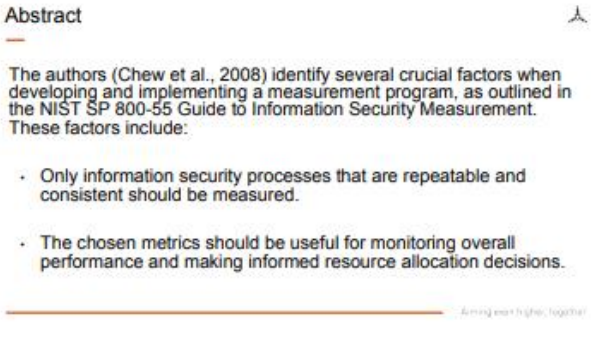
Arming even higher, together.

SYMBIOTIC

Arming even higher, together.

10.11. Anexo XI Entrenamiento Catálogo de KPI





KPI Table: Number of Vulnerabilities Detected

Indicator Name	Number of Vulnerabilities Detected
Indicator Code	SV-001
Strategic Objective	Strengthen the organization's security posture.
IT Objective	Ensure the security of Symbiotic's Tap on Phone system components against threats.
Measurement	Total number of vulnerabilities detected.
Measurement Type	Quantitative.
Formula	None.
Application in Testing	The metric will be used during regular security reviews of system components.
Frequency	Bi-weekly.
Responsible Party	Security and Monitoring Agent.
Data Source	Security alarm reports regarding suspicious activity signals.
Visualization	Bar chart.

KPI Table: Percentage of Classified Vulnerabilities

Indicator Name	Percentage of Vulnerabilities Classified by System Components
Indicator Code	SV-002
Strategic Objective	Strengthen the organization's security posture.
IT Objective	Efficiently categorize detected vulnerabilities according to the system components they belong to.
Measurement	Percentage.
Measurement Type	Quantitative.
Formula	(Number of vulnerabilities classified by component / Total number of vulnerabilities) x 100
Application in Testing	The metric will be used during regular security reviews of system components.
Frequency	Monthly.
Responsible Party	Security and Monitoring Manager. Security and Monitoring Agent. IT Ops and Compliance Agent.
Data Source	Vulnerability analysis report.
Visualization	Bar chart or pie chart showing the distribution of vulnerabilities by system components.

KPI Table: Rate of Prioritized Critical Vulnerabilities

Indicator Name	Critical Vulnerabilities Prioritization Rate
Indicator Code	SV-003
Strategic Objective	Enhance Symbiotic's security through the mitigation of critical vulnerabilities.
IT Objective	Ensure the security of critical information assets held by system components.
Measurement	Percentage.
Measurement Type	Quantitative.
Formula	(Number of Prioritized Critical Vulnerabilities / Total Number of Critical Vulnerabilities) x 100
Application in Testing	The metric will be used during regular security reviews of system components.
Frequency	Monthly.
Responsible Party	Security and Monitoring Manager. Security and Monitoring Agent. IT Ops and Compliance Agent.
Data Source	Vulnerability analysis report.
Visualization	Table for understanding the prioritization rate of vulnerabilities.

KPI Table: Rate of Prioritized Critical Vulnerabilities

KPI Table: Average Time to Apply Mitigation Measures

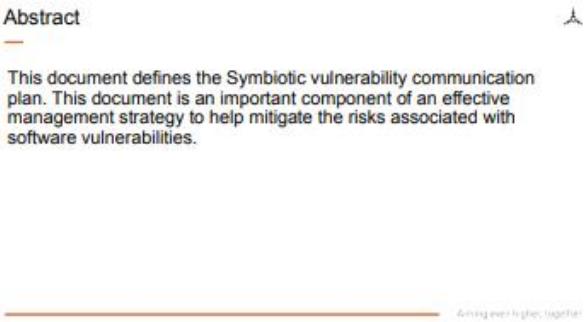
Metrics for the Communication Process

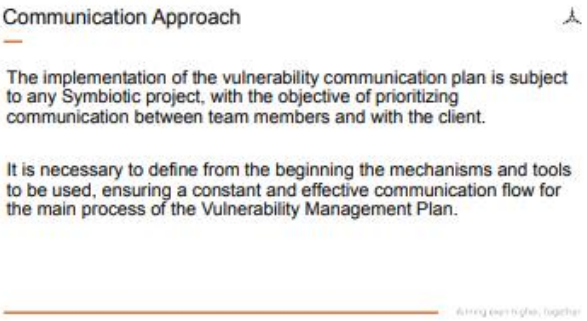
KPI: Percentage of Vulnerabilities Communicated on Time

KPI Table: Average Time to Report Critical Vulnerabilities

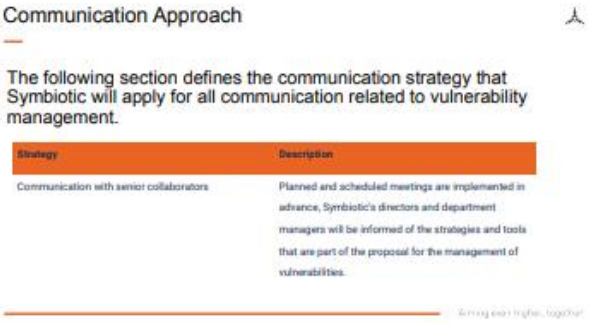
SYMBIOTIC
Aiming even higher, together

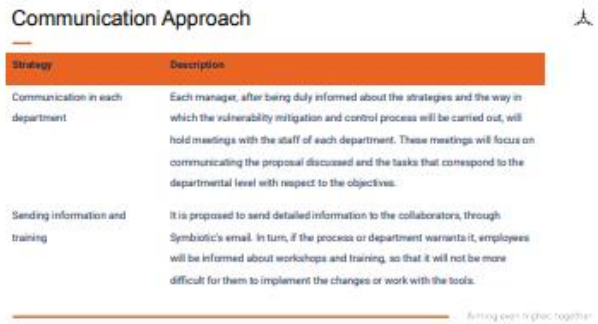
10.12. Anexo XII Entrenamiento Plan de Comunicaciones






Communication Strategy Planning


Communication Approach
The following section defines the communication strategy that Symbiotic will apply for all communication related to vulnerability management.
Strategy
Description
Communication with senior collaborators
Planned and scheduled meetings are implemented in advance, Symbiotic's directors and department managers will be informed of the strategies and tools that are part of the proposal for the management of vulnerabilities.


Communication Approach
Strategy
Description
Communication in each department
Each manager, after being duly informed about the strategies and the way in which the vulnerability mitigation and control process will be carried out, will hold meetings with the staff of each department. These meetings will focus on communicating the proposal discussed and the tasks that correspond to the departmental level with respect to the objectives.
Sending information and training
It is proposed to send detailed information to the collaborators, through Symbiotic's email. In turn, if the process or department warrants it, employees will be informed about workshops and training, so that it will not be more difficult for them to implement the changes or work with the tools.


Roles and Responsibilities


Roles and Responsibilities
Security and Monitoring Manager:
Responsible for communicating the classification and coordination of the resolution of reported vulnerabilities.
IT Ops and Compliance Manager:
Responsible for communicating the monitoring and control of the resolution of vulnerabilities.
IT Ops and Compliance Agent:
Responsible for supporting the monitoring and control, as well as creating the mitigation report.


Roles and Responsibilities
Lead Programmer:
Responsible for communicating the coordination resolution of reported vulnerabilities.
Security and Monitoring Agent:
Responsible for identifying and notifying vulnerabilities that are detected in the company's IDS tool.

Vulnerability Communication Management Process

The following section defines the vulnerability communication management process.

The Security and Monitoring Monitor analyzes the different vulnerability reports generated by Security and Monitoring Agent, these are centralized in a Slack channel called top-support.

The Security and Monitoring Monitor will review and classify the reported vulnerabilities based on their severity and impact.

The Security and Monitoring Monitor will work with the software development team to verify reported vulnerabilities and develop a remediation plan.

The Security and Monitoring Monitor will periodically report back to the notifier on the status of the vulnerability.

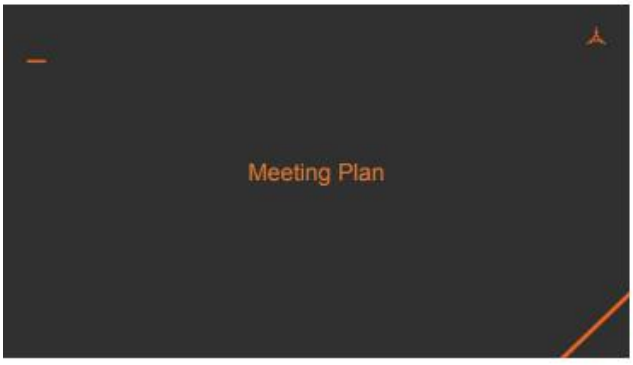
Communication Channels

Definition of communication channels: Email, Slack, Jira ServiceDesk.

Users who are or have access to the Symbiotic account and participate in the types of meetings related to vulnerability management will be sent regular updates on vulnerability strategy, service and response activities.

Vulnerability coordinators and the software development team will communicate via a secure messaging system.

Vulnerability notifiers will be contacted by email to provide updates on vulnerability status.



Meeting	Description	Assistants
Acceptance criteria	Acceptance criteria are defined for each remediation strategy that is part of the vulnerability mitigation process.	*Security and Monitoring Manager* *IT Ops and Compliance Manager* *Project Manager IT Operations* *Lead Programmer*
Retrospective	At the end of the process, the results obtained by applying the tests are analyzed and the Product Owner validates whether he agrees with them.	*Security and Monitoring Manager* *Security and Monitoring Agent* *IT Ops and Compliance Manager* *IT Compliance Agent* *Project Manager IT Operations* *Lead Programmer*

Meeting	Description	Assistants
Vulnerability analysis	The purpose of the meeting is to create the vulnerability analysis report, which consists of investigating which component of the system is directly affected by the vulnerability, categorizing the level of the component and defining whether or not it affects the operation of the application.	*Security and Monitoring Manager* *IT Ops and Compliance Manager* *Lead Programmer*

Meeting	Description	Assistants
Vulnerability remediation strategy planning meetings	Meetings to define task accomplishment, the team meets to develop activities and planning strategies to address vulnerabilities. Likewise, the meeting should assign remediation tasks to each working member related to vulnerability management.	*Security and Monitoring Manager* *Lead Programmer*
Control and follow-up meetings	Meetings that are responsible for supervising the execution of the mitigation tests.	*IT Ops and Compliance Manager* *Lead Programmer*

Response Time

Response Time

Vulnerability managers will acknowledge receipt of a vulnerability report within one business day.

Periodic updates on the status of the vulnerability shall be provided to the reporter every 5 working days.

Approval of vulnerability identification reports, vulnerability analysis and mitigation reporting should take no more than two business days.

Vulnerability remediation plans shall be approved and verified in no more than two business days for execution.

Aiming even higher, together.

Disclosure Policies

Disclosure Policies

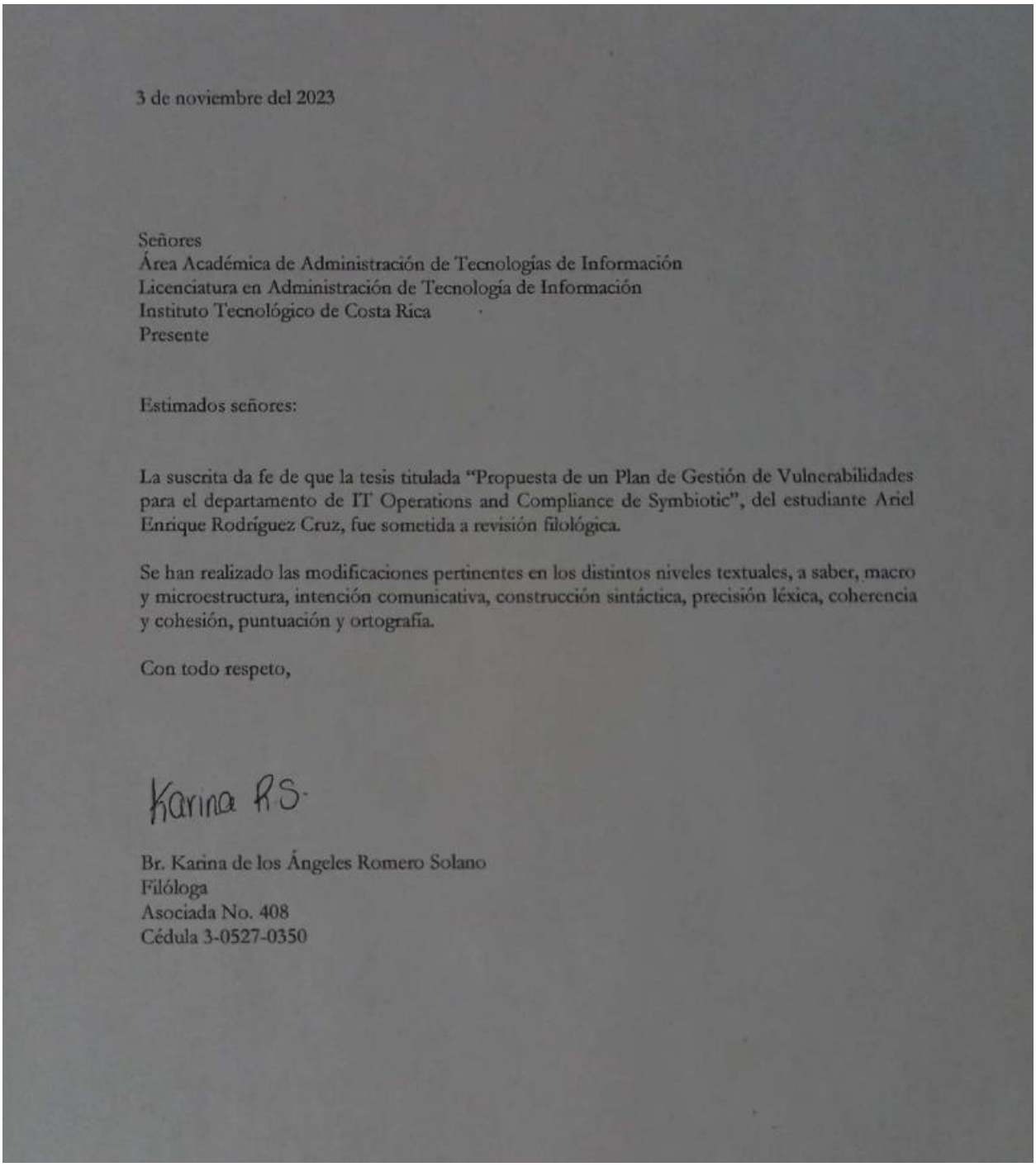
The Security and Monitoring Monitor and Lead Software Programmer will develop and implement a remediation strategy communication plan for each identified vulnerability.

The Security and Monitoring Monitor and Lead Programmer determine whether and how to disclose vulnerability information to customers and other interested parties.

Vulnerability managers will follow a responsible disclosure process to ensure that customers have sufficient time to apply updates and patches before vulnerabilities are publicly disclosed.

Aiming even higher, together.

10.13. Anexo XIII Carta de filología



3 de noviembre del 2023

Señores
Área Académica de Administración de Tecnologías de Información
Licenciatura en Administración de Tecnología de Información
Instituto Tecnológico de Costa Rica
Presente

Estimados señores:

La suscrita da fe de que la tesis titulada "Propuesta de un Plan de Gestión de Vulnerabilidades para el departamento de IT Operations and Compliance de Symbiotic", del estudiante Ariel Enrique Rodríguez Cruz, fue sometida a revisión filológica.

Se han realizado las modificaciones pertinentes en los distintos niveles textuales, a saber, macro y microestructura, intención comunicativa, construcción sintáctica, precisión léxica, coherencia y cohesión, puntuación y ortografía.

Con todo respeto,

Karina RS.

Br. Karina de los Ángeles Romero Solano
Filóloga
Asociada No. 408
Cédula 3-0527-0350