UNIVERSIDAD SAN SEBASTIAN

ESTUDIO DE PREFACTIBILIDAD TÉCNICA IMPLEMENTACIÓN DE SERVICIO SOC

Proyecto de título para optar al Título de Ingeniero en ciberseguridad y auditoria Informatica

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

CARRERA INGENIERIA EN CIBERSEGURIDAD Y AUDITORIA INFORMATICA

SEDE BELLAVISTA

Profesor guía: Mg. Rene Galarce Godoy
Estudiante: Claudio Maturana Paz

Santiago, Chile

2025

HOJA DE CALIFICACIÓN

En _____ Chile, el __ de _____ del 20__, los abajo firmantes dejan constancia que el estudiante _____ de la carrera _____ ha aprobado el proyecto de título para optar al título de _____ con una nota de _____

_____

Profesor Evaluador

_____

Profesor Evaluador

_____

Profesor Evaluador

AGRADECIMIENTOS

Al culminar esta importante etapa de mi vida académica, quiero detenerme un momento para agradecer profundamente a todas aquellas personas que, de una u otra forma, fueron parte de este camino. Este proyecto no solo representa el cierre de una etapa formativa, sino también el reflejo del esfuerzo compartido, el apoyo incondicional y el cariño de quienes estuvieron junto a mí en los momentos decisivos.

En primer lugar, agradezco con todo mi corazón a mi hermana **Karen Maturana**, quien ha sido un pilar fundamental durante este proceso. No solo me brindó su apoyo emocional y familiar incondicional, sino que también fue clave en la revisión y corrección gramatical de este trabajo. Su paciencia, compromiso y cariño fueron una gran fuente de motivación, especialmente en los momentos más exigentes.

A mi hermano **Mauricio Maturana**, le agradezco sinceramente su orientación y conocimientos en el ámbito de las tecnologías de la información. Cada conversación con él fue una oportunidad para aclarar dudas, fortalecer ideas y avanzar con mayor seguridad en los aspectos técnicos del proyecto. Pero más allá de su ayuda profesional, valoro profundamente su cercanía, su apoyo fraterno y el ejemplo que siempre ha sido para mí.

A mi hermano **Guido Maturana**, gracias por estar presente, por tu compañía silenciosa pero constante, por tu apoyo como familia y por ser parte esencial de la red de contención que me sostuvo en este camino. Tu presencia, aunque a veces discreta, fue siempre un impulso para seguir adelante.

A mi amigo **Andrés Galaz**, quiero agradecerte especialmente por tu disposición y colaboración en los análisis financieros y económicos que fueron esenciales para estructurar este proyecto. Tu visión crítica, tu experiencia y tu apoyo desinteresado hicieron una gran diferencia en la calidad del trabajo. Pero más allá de lo técnico, valoro tu amistad, tu empatía y tu generosidad en compartir tu tiempo y conocimientos.

A mi profesor guía, **René Galarce**, en especial le expreso mi más profundo agradecimiento por su acompañamiento constante, por su comprensión en los

momentos difíciles y, sobre todo, por su motivación permanente. Su confianza en mis capacidades y su forma cercana de guiarme me permitieron avanzar con claridad y convicción en cada etapa del proyecto. Fue un verdadero honor contar con su apoyo.

Finalmente, al profesor **Juan Huichipoco**, a quien considero una figura clave en mi formación académica. Desde los primeros años de la carrera, su orientación, sus consejos y su disposición para guiarme han sido fundamentales. Gracias por confiar en mí, por impulsarme a superarme y por haber sido una inspiración a lo largo de este proceso.

A todos ustedes, gracias por creer en mí, por no dejarme solo, y por ser parte de este logro que hoy me llena de orgullo. Este proyecto no sería lo que es sin su presencia, y cada página escrita lleva, de alguna forma, el reflejo de su apoyo.

RESUMEN

En un contexto global donde las amenazas cibernéticas aumentan en frecuencia y complejidad, las organizaciones industriales enfrentan un desafío creciente para proteger sus activos digitales, mantener la continuidad operativa y resguardar información crítica. Este escenario se ha vuelto especialmente evidente en el caso de una empresa del rubro metalúrgico, que fue víctima de un ataque de *phishing* que desencadenó un grave incidente de seguridad. A través del engaño a uno de sus usuarios, se logró la instalación de un *malware* que permitió el secuestro de información alojada en varios servidores críticos, incluyendo aquel que contenía la base de datos del sistema SAP, esencial para la operación y gestión empresarial.

Ante la urgencia del evento y con el objetivo de recuperar la información comprometida, la organización accedió a pagar inicialmente 300.000 dólares como rescate. Sin embargo, esta cifra fue luego elevada unilateralmente a 500.000 dólares por parte de los atacantes, quienes, tras recibir el pago, no retomaron contacto alguno, provocando la pérdida total de la información secuestrada. Entre los datos afectados se encontraban planos de estructuras metálicas, documentación técnica de maquinarias, licencias de software, contratos legales y otra información estratégica de alto valor. Un peritaje posterior estimó las pérdidas directas e indirectas en aproximadamente 1,7 millones de dólares, dejando en evidencia la falta de mecanismos eficaces de prevención, monitoreo y respuesta ante incidentes cibernéticos.

Frente a este panorama, la empresa tomó la decisión de realizar un análisis de brechas (GAP Analysis) para determinar su nivel de madurez en ciberseguridad, identificando importantes deficiencias en la gestión de riesgos, políticas internas, monitoreo de eventos y control de accesos. Como resultado de este diagnóstico, se propuso ampliar el alcance del área de Tecnologías de la Información (TI), incluyendo la creación de un Centro de Operaciones de Seguridad (SOC) que permita centralizar la supervisión de los sistemas, detectar amenazas de manera temprana y responder ante incidentes en forma oportuna y coordinada.

Este proyecto tiene como objetivo diseñar una propuesta de implementación de un SOC para esta empresa, integrando procesos, tecnologías y recursos humanos especializados. La solución estará fundamentada en buenas prácticas y marcos normativos internacionales, especialmente los controles establecidos por la norma ISO/IEC 27001, con el fin de asegurar una gestión sistemática y sostenible de la seguridad de la información. Además, se contempla la elaboración de procedimientos y políticas internas que respalden la operación del SOC, fomentando una cultura organizacional consciente de los riesgos cibernéticos y preparada para enfrentarlos.

La presente investigación no solo busca entregar una respuesta técnica a un problema real y urgente, sino también convertirse en un referente aplicable a otras organizaciones del sector industrial que aún no han desarrollado capacidades formales en ciberseguridad, y que enfrentan hoy una creciente exposición a las amenazas del entorno digital.

ABSTRACT

El propósito de este proyecto propone la implementación de un Centro de Operaciones de Seguridad (SOC) para una empresa del sector metalúrgico, tras un incidente de ciberseguridad que generó pérdidas económicas por alrededor de un total de 1,7 millones de dólares. Este hecho puso en evidencia importantes brechas de seguridad y las debilidades en los mecanismos de defensa ante un ataque de ciberseguridad, ya que en la actualidad no existe detección o respuesta ante ciberataques, afectando la continuidad operacional y con ello comprometiendo la información crítica de la organización.

Tras investigar cuáles son las mejores opciones para mitigar nuevas amenazas. se llegó a la conclusión que la creación de este SOC es la mejor opción para robustecer la seguridad de la información y activos críticos, con el diseño de una solución integral personalizada que permitirá a la empresa contar con capacidades de forma permanente de monitoreo, análisis y respuesta ante incidentes de seguridad adecuados a las necesidades del negocio, recursos de la empresa y mejores prácticas basada en la cultura de la industria.

El método abarca la revisión del estado de madurez de la empresa en el ámbito de la ciberseguridad, el estudio de las brechas, la detección de riesgos y la elaboración de políticas y procedimientos que engloben los procesos, tecnología y capital humano especializado.

Por lo tanto, este proyecto tiene como objetivo contribuir de forma específica a las mejoras constante de la administración en la ciberseguridad, creando procesos personalizados y claros para ejecutarlos en la empresa, protegiendo así, los activos que están expuestos a las amenazas de ciberseguridad que aumentan día a día.

GLOSARIO

Análisis de Vulnerabilidades:

Proceso que permite identificar, evaluar y priorizar debilidades en sistemas, redes o aplicaciones que podrían ser explotadas por amenazas.

Ataque de Día Cero (Zero-Day):

Vulnerabilidad desconocida por el fabricante o proveedor, para la cual no existe aún un parche disponible, y que puede ser explotada por atacantes.

Centro de Operaciones de Seguridad (SOC):

Infraestructura centralizada encargada de monitorear, detectar, analizar y responder a incidentes de seguridad cibernética en tiempo real.

Ciberseguridad:

Conjunto de prácticas, procesos y tecnologías orientadas a proteger los sistemas, redes y datos frente a accesos no autorizados, ataques o daños.

Consultor en Ciberseguridad:

Profesional especializado en identificar riesgos, diseñar estrategias de protección y mejorar la postura de seguridad de una organización.

Costos Fijos:

Gastos constantes que no cambian con el nivel de producción u operación, como salarios, licencias anuales o mantenimiento programado.

Costos Variables:

Gastos que varían según la actividad operativa, como capacitaciones, insumos de oficina o servicios de soporte puntuales.

Criptografía:

Técnica que permite proteger la confidencialidad e integridad de la información mediante el uso de algoritmos de cifrado.

DMZ (Demilitarized Zone):

Subred perimetral que actúa como zona intermedia entre la red interna segura y la externa, permitiendo exponer servicios sin comprometer la red principal.

Firewall de Próxima Generación (NGFW):

Dispositivo de seguridad que ofrece capacidades avanzadas como inspección profunda de paquetes, filtrado de aplicaciones y detección de amenazas.

HH (Horas Hombre):

Unidad que representa el tiempo de trabajo que una persona dedica a una tarea en una hora. Se utiliza para estimar esfuerzo y costos de personal.

IDS (Intrusion Detection System):

Sistema diseñado para monitorear el tráfico de red y generar alertas cuando se detectan actividades sospechosas o maliciosas.

Infraestructura Crítica:

Conjunto de componentes tecnológicos indispensables para el funcionamiento seguro y eficiente del SOC (servidores, almacenamiento, redes, etc.).

Licencia de SIEM:

Costo asociado a la adquisición y uso de un sistema SIEM, normalmente calculado en base a cantidad de eventos procesados o almacenamiento requerido.

Malware:

Software malicioso que incluye virus, gusanos, troyanos, spyware y ransomware, diseñado para dañar, infiltrarse o interrumpir sistemas informáticos.

Monitoreo 24/7:

Práctica de vigilancia constante que permite a un SOC operar de forma continua, asegurando la detección inmediata de amenazas en cualquier momento.

NAS (Network Attached Storage):

Sistema de almacenamiento conectado a la red que permite acceso y gestión centralizada de archivos desde múltiples dispositivos.

Phishing:

Técnica de ingeniería social mediante la cual los atacantes engañan a las víctimas para que revelen información confidencial, como credenciales o datos bancarios, haciéndose pasar por entidades legítimas.

Plan de Continuidad del Negocio (BCP):

Conjunto de estrategias y acciones que aseguran la operación de una empresa frente a interrupciones significativas, como ataques o desastres.

Plan de Recuperación ante Desastres (DRP):

Procedimiento técnico y organizacional para restaurar servicios críticos después de incidentes graves o fallos tecnológicos.

Ransomware:

Tipo de malware que cifra los archivos del usuario o del sistema y exige un rescate económico para devolver el acceso.

Red Team / Blue Team:

Prácticas donde un equipo simula ataques (Red Team) y otro se encarga de la defensa (Blue Team), con el objetivo de fortalecer la seguridad organizacional.

Respuesta ante Incidentes:

Proceso estructurado para contener, mitigar y recuperar la operación normal tras la ocurrencia de un incidente de seguridad.

ROI (Return on Investment):

Indicador financiero que mide el rendimiento de una inversión comparando los beneficios obtenidos con los costos incurridos.

SIEM (Security Information and Event Management):

Herramienta que centraliza la recolección, análisis y correlación de eventos de seguridad para facilitar la detección y respuesta a amenazas.

SOC-as-a-Service:

Modelo de contratación donde un proveedor externo opera el SOC para una empresa cliente, ofreciendo monitoreo, análisis y respuesta como servicio.

TTPs (Tactics, Techniques and Procedures):

Modelo utilizado para describir cómo los atacantes llevan a cabo sus campañas, basado en el marco MITRE ATT&CK.

UPS (Uninterruptible Power Supply):

Sistema de alimentación ininterrumpida que garantiza el funcionamiento de equipos críticos ante cortes de energía.

Vulnerabilidad:

Debilidad técnica o de configuración que puede ser explotada por un atacante para comprometer un sistema o red.

Zero Trust:

Modelo de seguridad que asume que ninguna entidad, interna o externa, debe ser confiada por defecto, aplicando verificaciones continuas.

INDICE

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

El presente proyecto tiene como finalidad evaluar la factibilidad estratégica, técnica y económica de la implementación de un servicio SOC (Centro de Operaciones de Seguridad). En los últimos años, el aumento sostenido de ataques de ciberseguridad tanto a grandes empresas como PYYMES (Pequeñas y medianas empresas), ha puesto en evidencia la necesidad imperiosa de que estas, sin importar su tamaño o rubro, robustezcan sus capacidades de protección y tiempo de respuesta frente a ataques de ciberseguridad. Este proyecto se enfoca en el diseño de la implementación de un Centro de Operaciones de Seguridad (SOC) en una empresa del sector metalúrgico llamada METALIM.

Este proyecto no solo busca una solución inmediata a los posibles ataques de ciberseguridad que puedan estar ocurriendo en este momento y los ataques futuros, sino también sentar las bases para robustecer las estrategias de ciberseguridad en el tiempo, que permita a la empresa enfrentar con mayor solidez los desafíos que actualmente ocurren con los avances de la ciberdelincuencia. Se espera que la implantación del SOC contribuya a disminuir los tiempos de respuesta ante ataques, reducir los costos asociados a futuros incidentes y generar una cultura organizacional más preparada frente a los riesgos de ciberseguridad.

Finalmente, a lo largo de la implantación de este proyecto se pretende ser un ejemplo y una referencia para otras organizaciones del rubro que enfrentan escenarios similares, para evitar los problemas ocurrido en esta organización, destacando la importancia de implementar procesos de ciberseguridad como un pilar fundamental en la gestión del negocio.

2. ANTECEDENTES DEL PROYECTO

El siguiente caso evidencia cómo la falta de capacidades de ciberseguridad y sus consecuencias que puede traducirse en pérdidas significativas en la operación y pérdidas económicas considerables.

2.1 Justificación de la problemática o proyecto

Tras un ciberataque (phishing) reciente que al final ocasionó pérdidas estimadas en 1,7 millones de dólares, afectando tanto la continuidad operativa de la empresa como la reputación a la vista de sus clientes y socios estratégicos. Tal fue el caso de esta empresa, la cual enfrentó este ataque de tipo *phishing* que derivó en la ejecución de un *malware* con capacidad de cifrado, que terminó comprometiendo varios servidores críticos, entre ellos el servidor que alojaba la base de datos de su sistema ERP SAP.

El incidente no solo interrumpió operaciones clave como la entrega de productos finales, sino que también generó una pérdida masiva de información estratégica, incluyendo planos de estructuras metálicas entre ellas antenas celulares de distintas compañías de telecomunicaciones que solicitaron su producción con los modelos y standard de cada una de estas compañías, documentación técnica de maquinaria adquiridas en el extranjero como manuales de uso y documentación de garantías, licencias de software utilizados en el modelamiento de planos, servicios de facturación y sistemas de automatización de remuneración y compensaciones a los empleados utilizados en el área de RRHH; por último, documentos legales esenciales para el funcionamiento de la empresa administrados por el área de finanzas. A pesar de haber aceptado el pago inicial de 300.000 dólares, posteriormente el o los cibercriminales elevaron el monto a 500.000 dólares— con la esperanza de recuperar la información secuestrada, se realizó el pago y los atacantes, los cuales no restablecieron el acceso a la información secuestrada y se perdió el contacto con estos ciberdelincuentes. Tras no poder recuperar la información, se contrató una empresa especializada en la recuperación de datos, los cuales indicaron en su informe que la totalidad de estos fue considerada irrecuperable. Este mismo informe llevó un anexo con

un informe pericial que estimó el impacto económico en un total del ataque en aproximadamente 1,7 millones de dólares, sumando pérdidas operativas, de propiedad intelectual y de daños físicos en algunos de los activos.

Este ataque reveló importantes debilidades en los mecanismos de ciberseguridad, (que en su momento fueron presentadas desde el área de TI a la gerencia de la empresa donde se hizo caso omiso a estas observaciones).

Las debilidades en la detección temprana y reacción ante eventos de seguridad, exponiendo activos críticos como información de procesos industriales, planos de propiedad intelectual y sistemas de producción, llevan a la necesidad de estructurar una solución que permita mitigar y fortalecer la gestión de la seguridad de la información en esta organización, con un enfoque proactivo y coordinado.

A partir de este análisis, se consolida un informe que da como resultado la solución de realizar una implantación de un SOC que incluye dentro de los objetivos definir roles, responsabilidades y correlación de eventos (SIEM), mecanismos de respuesta automatizada, y métricas para la mejora continua. Además, se incluyen políticas, procedimientos de ciberseguridad, la creación de SGSI y concienciación enfocada a los usuarios finales.

2.2 Objetivos

Es fundamental fortalecer la capacidad de la empresa metalúrgica para anticiparse y reaccionar de manera efectiva ante las amenazas cibernéticas. Esto se puede lograr a través de la creación de un Centro de Operaciones de Seguridad (SOC), que garantice la protección integral de sus activos críticos de información. Así, se asegura la resiliencia operativa, el cumplimiento de normativas y una mejora continua en la gestión de la ciberseguridad.

2.2.1 Objetivo general

Diseñar un servicio de Centro de Operaciones de Seguridad (SOC) orientado a la detección, análisis y respuesta oportuna ante incidentes de ciberseguridad, para la empresa METALIM, con el fin de fortalecer su capacidad de defensa,

reducir riesgos operacionales y mejorar la continuidad del negocio.

2.2.2 Objetivos financieros

Tabla 1 Objetivos financieros

Objetivo	Descripción
Reducción del costo de incidentes de ciberseguridad	Disminuir pérdidas financieras derivadas de interrupciones operacionales, robo de información, multas regulatorias o rescates por ransomware. Meta: **Reducir en un 50% el costo anual promedio de incidentes** en los primeros 12 meses.
Optimización del presupuesto de seguridad	Centralizar las herramientas y procesos de seguridad, eliminando redundancias y mejorando la eficiencia operativa. Meta: **Optimizar un 20% del gasto TI en herramientas desconectadas.**
Asegurar la continuidad operacional y evitar pérdidas por detenciones de producción	En industrias como la metalúrgica, una hora de detención puede tener un costo elevado. Meta: **Reducir en un 80% las interrupciones no planificadas por ciberincidentes.**
Mejorar la rentabilidad del negocio a través del cumplimiento normativo y reputacional	Evitar sanciones legales y fortalecer la imagen corporativa para atraer contratos con exigencias de seguridad. Meta: **Posicionar a METALIM como proveedor confiable en licitaciones de alto nivel.**
Justificar el retorno sobre inversión (ROI) del SOC	Demostrar que el SOC no es solo un centro de costos, sino una inversión estratégica. Meta: **Obtener un ROI positivo en el año 2**, al contrastar el ahorro en pérdidas evitadas versus el costo de operación del SOC.
Análisis de costo-beneficio	Realizar un estudio que contraste el costo de inversión y operación del SOC frente a las pérdidas evitadas por incidentes, multas y

	detenciones de operación; con el fin de verificar la factibilidad económica del proyecto

Fuente: Elaboración propia. Referencia: https://blog.hubspot.es/sales/ejemplos-objetivos-financieros-empresa

2.2.3 Objetivos específicos

Crear un plan detallado para poner en marcha el SOC, que defina claramente los roles, responsabilidades y protocolos de actuación, poniendo especial énfasis en la detección temprana y la respuesta a incidentes.

Diseñar e implementar un sistema de monitoreo proactivo utilizando un SIEM (Gestión de Información y Eventos de Seguridad), que permita correlacionar eventos de seguridad en tiempo real, identificando y analizando amenazas antes de que puedan comprometer activos críticos.

Desarrollar políticas y procedimientos de ciberseguridad que sean claros y efectivos, enfocados en proteger la información confidencial y la infraestructura tecnológica de la empresa, con un enfoque en la prevención y mitigación de riesgos cibernéticos.

Implementar mecanismos de respuesta automatizada para incidentes de seguridad, reduciendo el tiempo de reacción y evitando posibles daños a los activos de la empresa.

Establecer un programa de capacitación y concienciación continua en ciberseguridad para todos los empleados, asegurando que estén listos para detectar y reaccionar ante posibles amenazas.

Crear un Sistema de Gestión de Seguridad de la Información (SGSI) que permita una gestión integral y eficiente de los riesgos relacionados con la ciberseguridad, alineado con las mejores prácticas y normativas internacionales.

2.2.4 Alcances y delimitaciones

El proyecto se centrará en el diseño y la factibilidad de una implementación de un SOC para proteger los activos críticos de la empresa METALIM, limitándose a la infraestructura de red y sistemas internos sin abordar aspectos de producción

ni ciberseguridad de terceros.

- **Alcances:** La implementación de este Centro de Operaciones de Seguridad (SOC) para la empresa METALIM. Incluye una plataforma SIEM (Security Information and Event Management) herramientas de código abierto, llamada Wasuh en el área de monitoreo, Wireshark en el área de Análisis y en el área de Data, Alert Data. Esto permitirá monitorear los activos como equipos endpoint, cuentas de correo, cuentas de AD (active directory), activos tecnológicos críticos (servidores) estas herramientas al ser *opensourse* (código abierto) son tareas desafiantes, pero proporcionan a las organizaciones mejorar su control a un bajo precio. Esto ayudará a detectar amenazas, vulnerabilidades e incidentes de ciberseguridad en tiempo real. Este SOC tiene una división que realizará:

  Monitoreo Continuo 24/7.

  Integración de TI y OT.

  Gestión de Incidentes de Seguridad.

  Implementación de Herramientas Avanzadas de Seguridad.

  Capacitación del Personal Interno.

  Cumplimiento de Normativas y Estándares de Seguridad.

- **Delimitaciones**

  La planeación y las recomendaciones entregadas para la implementación del SOC se basan en los controles establecidos en la norma **ISO/IEC 27001**, inicialmente comenzaremos con el proceso de implementar los siguientes controles:

  A.5: Políticas de seguridad de la información.

  A.6: Organización de la seguridad de la información.

  A.9: Control de acceso.

  A.12: Seguridad en las operaciones.

  A.16: Gestión de incidentes de seguridad de la información.

- **Delimitaciones del SOC:** Estas actividades que se implementará para poner en marcha un Centro de Operaciones de Seguridad (SOC) en METALIM, tiene un objetivo bien definido y ciertas limitaciones que vienen dadas por temas técnicos, de presupuesto y cómo está organizada la empresa, A continuación, se describen las principales delimitaciones:

  Personal inicial necesario escaso.
  Uso de herramientas de código abierto.
  capacitación limitada al personal interno.

- **Alcances Tecnológicos:** Se utilizarán herramientas de código abierto **(open source)** para la construcción del SOC, como **Wazuh** (SIEM y monitoreo), **Wireshark** (análisis de tráfico) y **Alert Data** (gestión de alertas).
  La solución está dirigida al **monitoreo de endpoints, cuentas de correo electrónico, cuentas de Active Directory y servidores críticos**, tanto del entorno TI como de la red OT.
  No se contempla la adquisición de soluciones propietarias ni licenciamiento comercial, lo que implica una dependencia de configuraciones personalizadas y mayor esfuerzo en integración técnica.
- **Limitaciones Operativas:** El SOC estará orientado a una **operación 24/7**, pero en una primera etapa se delimita a la **fase de marcha blanca**, donde se realizarán pruebas, ajustes de herramientas, generación de indicadores y validación de procesos.
  La integración entre los entornos **TI (tecnología de la información)** y **OT (tecnología operativa)** estará limitada a los activos críticos previamente definidos, no incluyendo todos los sistemas de control industrial debido a restricciones presupuestarias y de acceso.
- **Limitaciones Organizacionales**

A pesar del compromiso actual, la empresa ha demostrado históricamente **baja cultura de ciberseguridad** y resistencia al cambio, lo que podría impactar en la adopción de políticas, capacitación del personal y cumplimiento de procesos.

No se contempla en esta fase la creación de un equipo SOC interno completo. Se espera una **capacidad operativa inicial mínima**, con posibilidad de expansión futura según los resultados de esta implementación.

- **Limitaciones Normativas**

  La evaluación del cumplimiento se enfoca en **estándares de referencia como ISO/IEC 27001 y NIST CSF**, pero **no se implementará una certificación formal** en esta etapa del proyecto.

  Las políticas y controles establecidos serán orientativos y adaptativos, no vinculantes desde el punto de vista legal o contractual.

- **Limitaciones Temporales**

  El proyecto está delimitado por el marco temporal de una tesis de título, por lo tanto, **las actividades se concentran en el diseño, prueba piloto (marcha blanca), recolección de indicadores y análisis de viabilidad técnica** del SOC, no contemplando aún su escalamiento operativo completo ni su formalización contractual.

2.3 Marco Teorico

En el proyecto impulsado por la organización para fortalecer y evitar nuevos ataques de ciberseguridad como es la creación de un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) se ha considerado como estrategia utilizar 4 metodologías existentes para cumplir con una eficiente implementación (Ahmad, Maynard & Park, 2014).

Este marco teórico explica los conceptos de estas herramientas elegidas para dicho proyecto.

2.3.1 ISHIKAWA

Diagrama de Ishikawa y su aplicación en ciberseguridad.

El diagrama de Ishikawa, también conocido como **diagrama de espina de pescado**, es una herramienta eficaz para la resolución de problemas. Su metodología se basa en la generación de ideas (lluvia de ideas) orientadas a identificar la causa raíz de un problema, en lugar de limitarse a soluciones rápidas o superficiales (Ishikawa, 1986). El nombre “diagrama de pescado” proviene de la similitud visual con el esqueleto de un pez.

En el contexto de la **ciberseguridad**, este diagrama puede adaptarse a través del análisis de las **6 M**, cada una representando un factor crítico que puede influir en la aparición de incidentes:

Método: Incluye las políticas, procesos y procedimientos relacionados con la seguridad de la información.

Mano de obra: Hace referencia a la competencia técnica del personal del Centro de Operaciones de Seguridad (SOC), la asignación de turnos y la carga de trabajo.

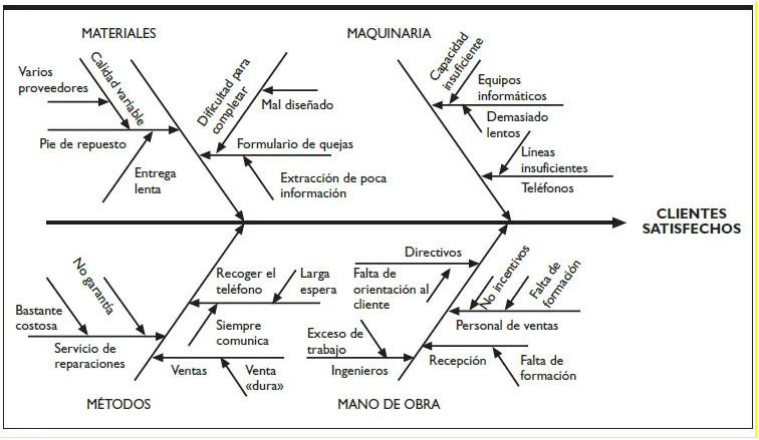
Máquina: Se refiere a las herramientas tecnológicas como SIEM, firewalls, sistemas IDS/IPS y servidores.

Material: Comprende los recursos informativos como registros (logs), configuraciones y reglas de correlación.

Medición: Incluye los indicadores clave de desempeño (KPIs) y las métricas de eficiencia en la respuesta a incidentes.

Medio ambiente: Considera la infraestructura de red, la ubicación física del centro de datos y el cumplimiento del entorno normativo o regulatorio.

Ilustración 1 Diagrama de Ishikawa



Ubatuba. (s.f.). Recuperado el 20 de abril de 2025, https://miro.com/es/diagrama/que-es-diagrama-ishikawa/

2.3.2 Ciclo de Deming

Es una herramienta que permite que las organizaciones configuren sus planes de gestión y de mejoras continuas para aumentar sus competencias en el marco de la calidad de sus procesos**,** logrando así reducir los costos y fallos, aumentando la productividad y mitigando riesgos.

El **ciclo de Deming (PDCA)** ofrece un marco para gestionar la mejora continua en el funcionamiento del SOC (Deming, 1986)

Ilustración 2 Ciclo de Deming

Recuperado el 20 de abril de 2025, de https://www.eurofins-environment.es/es/el-ciclo-deming-que-consiste-y-como-ayuda-gestion-procesos/

- **Planificar (Plan)**

En esta fase se identifican oportunidades de mejora, se establecen objetivos claros y se desarrolla un plan de acción para lograr los cambios deseados. Se analiza el problema, se recopila información relevante y se definen los procesos y recursos necesarios.

- **Hacer (Do)**

Se implementa el plan en una escala controlada. Esta etapa permite ejecutar las acciones planificadas, capacitar a los involucrados y comenzar a recolectar datos sobre el desempeño del nuevo proceso.

- **Verificar (Check)**

Se evalúan los resultados obtenidos en la etapa anterior comparándolos con los objetivos propuestos. Esta fase permite analizar qué aspectos funcionaron correctamente y cuáles requieren ajustes.

- **Actuar (Act)**

  Si los resultados fueron positivos, se estandariza e implementa el cambio a mayor escala. En caso contrario, se revisa el plan y se reinicia el ciclo. El objetivo es fomentar una cultura de mejora continua dentro de la organización.

2.3.3 Norma ISO/IEC 27001

Es una estándar internacional reconocida que su propósito es proteger la confidencialidad, integridad y disponibilidad de los datos**.** De cara a las actuales amenazas de ciberseguridad existentes en la actualidad.

La ISO/IEC27001 establece requisitos mínimos para implementar un SGSI: Sistema de Gestión de Seguridad de la Información, esto facilita a las organizaciones gestionar los posibles riesgos de ciberataque mediante controles técnicos de la organización y de los recursos humanos sus pilares fundamentales son:

- Evaluación y tratamiento de riesgos.
- Políticas de seguridad.
- Control de acceso.

- Gestión de incidentes de seguridad.
- Mejora continua.

Ilustración 3 Diagrama ISO 27001

Recuperado el 20 de abril de 2025, de https://www.dnv.cl/services/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-3327/

3. ANALISIS DE LA SITUACION ACTUAL

La empresa METALIM ha enfrentado un ciberataque considerable que resultó en la pérdida de información crítica y financiera, afectando tanto su operativa diaria como su reputación. Este incidente puso de manifiesto varias debilidades en las capacidades de ciberseguridad de la organización, especialmente en lo que respecta a la detección temprana de amenazas y la respuesta ante incidentes. Las principales fallas que se observaron fueron:

Falta de detección temprana: El ataque no fue detectado a tiempo, lo que permitió a los atacantes comprometer servidores críticos y robar información sensible, incluyendo planos industriales y documentos legales esenciales.

Deficiencias en la respuesta ante incidentes: La empresa carecía de protocolos claros y herramientas adecuadas para mitigar el impacto del ataque, lo que resultó en la pérdida total de información y la interrupción de operaciones clave.

Carencia de una infraestructura de seguridad adecuada: La ausencia de un SOC y de un sistema SIEM dificultó la gestión eficiente de los eventos de seguridad y la identificación de amenazas en tiempo real.

Desinformación sobre ciberseguridad: A pesar de que el área de TI había advertido sobre la necesidad de fortalecer las capacidades de ciberseguridad, las recomendaciones fueron pasadas por alto, dejando a la empresa expuesta a ciberataques de gran escala.

3.1 descripción de situación actual

METALIM es una empresa dedicada a la fabricación de torres, monopolos y camuflajes para telecomunicaciones, con la última tecnología en galvanizado, estricto control de calidad, ensamble perfecto, logística de avanzada hacen que la calidad de sus antenas alcance los requerimientos más difíciles de cumplir y que cada estructura sea de fácil montaje y dure para siempre. así como la construcción de radio bases, con operaciones en Centro, Norte y Sur América.

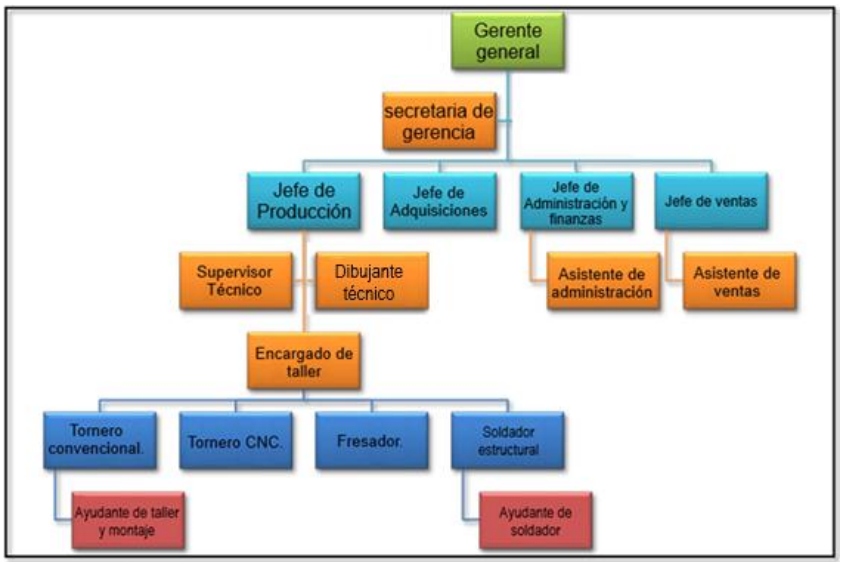
Más de 40 años (desde 1982) en la industria hace a METALIM líderes del mercado y los mayores expertos en infraestructura para telecomunicaciones.

3.1.1 Misión: Proporcionar servicios de gestión que permitan la materialización de los proyectos de inversión de empresas del área industrial (Minería, Energía, Alimentos, Celulosa, Papel, Combustible y Otros), del sector público y privado, en el mercado nacional, mediante el diseño, adquisición, construcción, montaje, puesta en marcha y operación, y entregar una propuesta de valor sustentada en el desarrollo de capacidades que permitan satisfacer las expectativas de nuestros clientes, más allá de lo meramente contractual.

3.1.2 Visión: Posicionarnos entre las principales empresas de construcción y montaje industrial en el mercado nacional y que esta mirada y aspiraciones de futuro sean atrayentes, desafiantes y contribuyan al desarrollo de las personas que conforman nuestra empresa.

3.1.3 Organigrama:

Ilustración 4 Organigrama empresarial



Elaboración: empresa Metalim

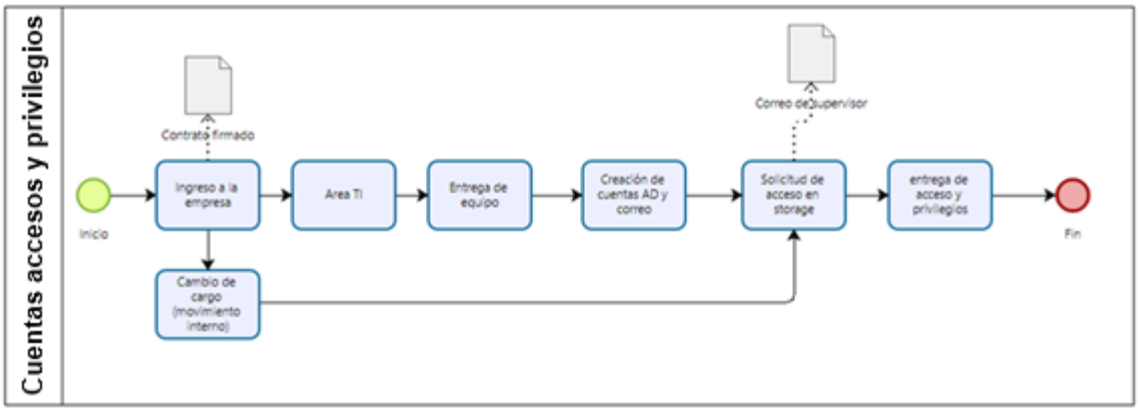
3.2 Procesos actuales de la empresa

La empresa mantiene un área de TI administrada por un solo analista los procesos que presentaremos abarcan la actualidad de la empresa en base a su seguridad de la información. Procesos alcances y privilegios.

3.2.1 Área de Tecnologías de la Información (TI) (Accesos y privilegios)

- **Paso 1:** Creación de cuentas a usuario nuevo: Un usuario nuevo en la organización de presentarse en el departamento de TI para solicitar su credencial, equipo notebook, cuenta de AD y correo corporativo.
- **Paso 2:** Al presentarse con su contrato se verifica cual es el área que trabajará, ya que solamente los dibujantes técnicos usaran equipos notebook de la marca Apple. El resto usara equipos Windows.
- **Paso 3:** Se busca dentro de bodega un equipo con las características acorde a su cargo y se realizará la instalación de los programas básicos para sus labores dentro de la organización.
- **Paso 4:** En una tabla Excel se deja registro de número de serie, modelo y nombre de la persona responsable que se entregó el equipo.
- **Paso 5:** Su jefatura deberá informa al área TI, cuales son las carpetas compartidas y los privilegios que se le deben entregar al nuevo usuario.
- **Paso 5.1:** En caso de que un colaborador realice un movimiento interno dentro de la empresa se realizará las mismas actividades que en el paso 5.

Ilustración 5 Proceso creación de cuentas, acceso y privilegios



Elaboración propia Referencia: https://www.youtube.com/watch?v=MHR4Rtpi-QU&pp=0gcJCdgAo7VqN5tD

3.3 Descripción del problema

En vista del proceso presentados en el punto anterior, se detecta de la ausencia

de una estructura proactiva de ciberseguridad.

- **Dependencia de un solo analista**

El área de servicios y funciones TI dependen de un solo colaborador, lo que representa un riesgo en la continuidad operacional y de los servicios. No existe redundancia de procedimientos ni respaldo ante su ausencia.

- **Falta de documentación de procesos críticos**

No se han estandarizado ni documentado los procedimientos operacionales y técnicos, lo que impide que otro colaborador pueda asumir funciones en ausencia del analista principal.

- **Ausencia de planes de continuidad operativa o contingencia**

La organización no cuenta con planes formales que aseguren la continuidad de los servicios TI ante eventos como licencias médicas, vacaciones o desvinculación del analista clave.

- **Limitaciones en la capacitación y asignación de roles dentro del equipo**

No se ha capacitado a otros integrantes del equipo ni se ha promovido la rotación de funciones, generando una concentración del conocimiento y habilidades en una sola persona.

- **Falta de documentación y procedimientos**

La inexistencia de manuales, políticas, procedimientos y la falta de creación de una base de conocimientos impide una gestión disciplinada, cíclica y auditable para el área TI.

- **Desconocimiento de la importancia de la gestión del conocimiento**

El equipo TI no ha priorizado la creación y mantenimiento de documentación formal, debido a una cultura organizacional centrada en la resolución inmediata de problemas en lugar de la estandarización de procesos.

- **Falta de asignación de tiempo y recursos para la documentación**

Las cargas operativas diarias absorben la mayor parte del tiempo del personal TI, impidiendo que se dediquen recursos específicos a la elaboración de manuales, políticas o bases de conocimiento.

- **Gestión reactiva en la operación, no orientada a la ciberseguridad**

El trabajo está orientado exclusivamente a la operación (equipos, usuarios, accesos), sin la capacidad de realizar monitoreos internos de la red o de las actividades realizadas por los usuarios.

- **Falta de integración de herramientas de monitoreo de seguridad (SIEM, IDS/IPS)**

La organización carece de soluciones tecnológicas que permitan visualizar, correlacionar y responder a eventos de seguridad en tiempo real.

- **Enfoque operacional centrado en la disponibilidad y no en la seguridad**

Las prioridades del área TI están orientadas a mantener la infraestructura y la atención a usuarios, dejando en segundo plano los controles preventivos y detectivos de ciberseguridad.

- **Ausencia de un modelo de gestión basado en riesgos**

No existe un enfoque estratégico que considere la evaluación y mitigación de riesgos de seguridad de la información como parte de la operación diaria del equipo TI.

- **Sistemas críticos (SAP, AD, almacenamiento) sin monitoreo de seguridad**

Se administran plataformas de carácter sensibles como SAP sin monitoreo sobre las actividades sospechosas, accesos indebidos.

- **Falta de integración entre sistemas críticos y plataformas de monitoreo de seguridad**

Los sistemas como SAP o Active Directory no están conectados a herramientas SIEM u otras soluciones que permitan correlacionar eventos de seguridad en tiempo real.

- **Carencia de políticas de auditoría y registro de eventos**

No se han definido ni habilitado configuraciones para el registro, almacenamiento y revisión de logs de seguridad, dificultando la detección de accesos indebidos o comportamientos anómalos.

- **Limitaciones presupuestarias o de licenciamiento para módulos de seguridad avanzados**

Las funcionalidades de seguridad adicionales, como monitoreo de actividades o alertas automáticas, no están habilitadas por restricciones económicas o desconocimiento técnico.

- **Falta de políticas y controles basados en estándares de ciberseguridad.**

Sin una estructura SOC, no existe control de logs, trazabilidad, análisis de vulnerabilidades, procesos de parchados, ni un plan de trabajo como respuesta ante un incidente.

- **Ausencia de un marco normativo o estándares de ciberseguridad implementados**

La organización no ha adoptado marcos de ciberseguridad como NIST, ISO 27001 o CIS, lo que dificulta la implementación de controles efectivos de protección, monitoreo y respuesta ante incidentes.

- **Carencia de un proceso formal para el análisis de vulnerabilidades y gestión de parches**

No existen procedimientos establecidos para realizar análisis periódicos de vulnerabilidades ni un plan definido para gestionar parches y actualizaciones en los sistemas críticos.

- **Falta de definición de roles y responsabilidades en el proceso de respuesta a incidentes**

No se han asignado responsabilidades claras dentro del equipo de TI ni se ha desarrollado un plan de respuesta ante incidentes, lo que impide una reacción organizada y eficaz ante posibles brechas de seguridad.

No existe una base de conocimientos documentada que permita consultar soluciones a problemas recurrentes o buenas prácticas.

- **Falta de tiempo y recursos dedicados a la documentación**

El personal de TI se ve abrumado por las tareas operativas diarias, lo que impide que se destine tiempo y recursos a crear y mantener una base de conocimientos organizada.

- **Ausencia de una cultura organizacional centrada en la documentación**

No se ha promovido dentro de la organización la importancia de compartir conocimiento y documentar soluciones a problemas recurrentes, lo que genera una dependencia de la memoria individual en lugar de recursos compartidos.

- **Desconocimiento de herramientas y plataformas para gestionar el conocimiento**

La organización no utiliza herramientas adecuadas, como wikis, sistemas de gestión del conocimiento o bases de datos, que faciliten la creación, el acceso y la actualización de la información técnica y las mejores prácticas.

No se cuenta con manuales de usuario ni procedimientos operativos Que se entreguen como capacitaciones a los nuevos colaboradores para alineamiento de criterios en base a la ciberseguridad y el debido uso de los activos de la empresa.

- **Falta de un proceso estructurado para la creación de manuales y documentación**

La ausencia de un proceso formal para la creación y actualización de manuales de usuario y procedimientos operativos lleva a que no se cuente con material de referencia consistente y accesible para nuevos colaboradores.

- **Desconocimiento de la importancia de la formación continua en ciberseguridad**

La falta de enfoque en la formación y el alineamiento de criterios de seguridad con los nuevos empleados limita la comprensión de las mejores prácticas en ciberseguridad y el uso adecuado de los activos, lo que aumenta el riesgo de errores humanos o fallos operativos.

- **Recursos limitados para la creación de material educativo**

La falta de recursos dedicados, como personal especializado o tiempo, impide la creación de manuales de usuario y procedimientos operativos detallados, lo que afecta la capacidad de integrar la ciberseguridad como parte de la cultura

organizacional.

- **No hay políticas documentadas**

relacionadas con la gestión de TI, lo que en caso de una ausencia del analista no existe un plan de trabajo a seguir como backup.

- **Falta de gobernanza en la gestión de TI**

No existe una estructura formal de gobierno que defina responsabilidades, procesos y normativas para asegurar la continuidad operativa y la estandarización de tareas en ausencia del personal clave.

- **Dependencia del conocimiento tácito del analista**

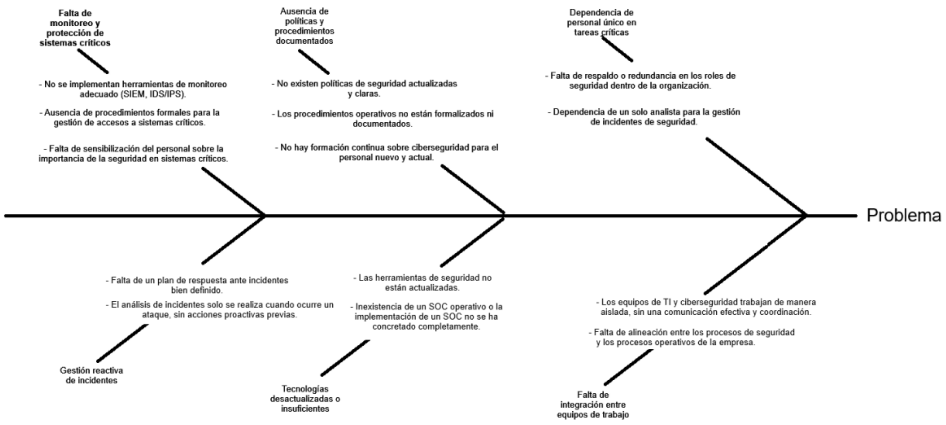
Las operaciones dependen del conocimiento individual del analista, que no ha sido documentado ni traspasado al resto del equipo, lo que impide replicar su trabajo de forma sistemática.

- **Ausencia de una cultura de documentación y respaldo operativo**

No se ha promovido una cultura organizacional orientada a la documentación, la redundancia operativa ni a la preparación ante contingencias, lo que deja a la organización vulnerable ante ausencias o rotación de personal.

3.4 Diagrama Ishikawa

Ilustración 6 Diagrama Ishikawua



Elaboración Propia Referencia: https://miro.com/es/diagrama/que-es-diagrama-ishikawa/

El análisis mediante el Diagrama de Ishikawa permite identificar con claridad la raíz de los múltiples problemas que afectan la gestión de tecnologías de la información en la organización. Uno de los problemas más críticos que se ha identificado es la excesiva concentración de funciones clave en un solo analista de TI. Esto puede desencadenar una serie de riesgos que amenazan la continuidad operativa y la seguridad de la información.

Entre las consecuencias más notables se encuentran la falta de documentación formal de los procesos, la ausencia de planes de continuidad y respuesta ante incidentes, y la falta de un enfoque preventivo en ciberseguridad. Además, se observa una gestión reactiva que se limita a mantener la disponibilidad de los servicios, sin implementar buenas prácticas ni controles técnicos y organizacionales que estén alineados con estándares internacionales.

Esta situación deja a la organización en una posición de alta vulnerabilidad ante posibles incidentes, errores humanos o la falta de personal clave. La carencia de políticas, manuales, procedimientos, planes de formación y herramientas tecnológicas adecuadas complica cualquier intento de escalar, automatizar o madurar la gestión de TI.

En resumen, el Diagrama de Ishikawa pone de manifiesto que la dependencia del conocimiento tácito, la falta de gobernanza y la ausencia de una cultura organizacional que valore la documentación y la ciberseguridad son las principales causas del problema. Si no se abordan de manera estructurada, estas deficiencias podrían resultar en pérdidas operativas, brechas de seguridad y un impacto directo en la continuidad del negocio.

3.5 Análisis de criticidad

A partir del análisis de causa raíz y las subcausas identificadas, se destaca una alta criticidad en varios aspectos, como la dependencia de un solo analista, la falta de documentación y políticas de respaldo, y la ausencia de monitoreo en sistemas críticos como SAP o Active Directory. tos factores impactan directamente en la continuidad operativa, la capacidad de respuesta ante incidentes y la protección de los activos más valiosos de la organización. Los

elementos más críticos que se han identificado son: Recursos humanos no redundantes: La falta de reemplazos o protocolos claros para la ausencia del único analista crea un punto único de falla. Sistemas críticos sin monitoreo: Plataformas clave funcionan sin vigilancia activa, lo que representa un alto riesgo en caso de accesos no autorizados o ciberataques. Falta de documentación formal: La ausencia de manuales, procedimientos y políticas limita la estandarización operativa y disminuye la capacidad de respuesta ante eventos. Este análisis ayuda a establecer prioridades de mejora, asignar recursos y definir medidas urgentes para mitigar riesgos, asegurando la resiliencia del sistema TI y su alineación con principios fundamentales de ciberseguridad.

Tabla 2 Matriz de criticidad

Valor	Probabilidad	Descripción
1	Muy baja	Actividades con muy baja probabilidad de ocurrencia
2	Baja	Baja probabilidad de ocurrencia
3	Media	Probabilidad media de ocurrencia
4	Alta	Alta probabilidad
5	Muy alta	Muy probable de ocurrir

Fuente: Elaboración propia. Referencia: https://www.youtube.com/watch?v=OUtmT8DPT3Q

Tabla 3 Matriz de probabilidad causa raíz

6 M	Causa raíz	Valor	Probabilidad	Descripción
Método	Falta de políticas y procedimientos documentados	4	Alta	La falta de procedimientos y políticas estandarizadas eleva la probabilidad de incidentes críticos.
Mano de obra	Dependencia de un solo analista	5	Muy alta	La falta de personal alternativo para cubrir el análisis de seguridad

6 M	Causa raíz	Valor	Probabilidad	Descripción
				aumenta significativamente el riesgo.
Máquina	Falta de integración de herramientas de monitoreo de seguridad (SIEM)	3	Media	La ausencia de estas herramientas reduce la capacidad de respuesta ante incidentes.
Material	No existe una base de conocimientos documentada	4	Alta	La falta de una base de conocimientos estructurada dificulta la resolución rápida de problemas recurrentes.
Medición	Falta de KPIs de ciberseguridad	3	Media	La ausencia de métricas para evaluar el desempeño de seguridad incrementa el riesgo, aunque no es inmediato.
Medio ambiente	Infraestructura de red débil o desactualizada	4	Alta	La infraestructura débil puede ser fácilmente vulnerada, aumentando la probabilidad de incidentes.

Fuente: https://www.youtube.com/watch?v=OUtmT8DPT3Q

3.6 Matriz de Impacto

Tabla 4 Matriz de impacto

Valor	Impacto	Descripción
1	Bajo	Impacto bajo
2	Medio	Impacto medio
3	Alto	Impacto alto

Fuente: Elaboración propia. Referencia: https://www.youtube.com/watch?v=OUtmT8DPT3Q

3.7 Matriz en función de probabilidad e impacto

Una vez que hemos definido las dimensiones de impacto y probabilidad, pasamos a realizar el análisis de riesgo. Este análisis se basa en multiplicar ambos factores, lo que nos permite calcular la magnitud del riesgo (M) utilizando la fórmula: M = P × I, donde P es la probabilidad de que ocurra un evento y I representa el impacto asociado. A continuación, se muestra la tabla con los valores que hemos obtenido.

Tabla 5 Matriz en funcion de probabilidad e impacto

Probabilidad / Impacto	Muy bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy alto (5)
Muy alta (5)	5	10	15	20	25
Alta (4)	4	8	12	16	20
Media (3)	3	6	9	12	15
Baja (2)	2	4	6	8	10
Muy baja (1)	1	2	3	4	5

Fuente: Elaboración propia. Refrencia: https://www.youtube.com/watch?v=OUtmT8DPT3Q

3.8 Matriz de Magnitud del Riesgo

La categorización de la magnitud (M) debe tener relación con la modificación y mejora de los procesos y servicios de la empresa, lo que se muestra en la siguiente tabla.

Tabla 6 Matriz de magnitud de riesgo

Magnitud (M)	Nivel de Riesgo	Acción recomendada
1 – 4	Bajo	Monitorear. No requiere acción inmediata.
5 – 8	Moderado	Evaluar y aplicar controles básicos.
9 – 16	Alto	Requiere mitigación prioritaria.
17 – 25	Crítico	Acción inmediata. Revisión urgente.

Fuente: Elaboración propia. Referencia: https://www.youtube.com/watch?v=2qX7PfQ1gc8

3.9 Riesgos identificados

- **Dependencia de un solo analista:** La operativa del área de TI se sostiene únicamente en una persona, lo que crea un punto crítico de falla. Si esa persona se ausenta por enfermedad, vacaciones o decide renunciar, no hay respaldo técnico ni procedimientos establecidos, lo que pone en riesgo la continuidad de servicios esenciales. Impacto: Esto puede llevar a una interrupción total de los servicios, un aumento en el tiempo de respuesta ante incidentes y un daño a la reputación debido a la baja disponibilidad de recursos de TI.

- **Falta de documentación y procedimientos:** La ausencia de manuales, políticas y procedimientos dificulta una gestión que sea estandarizada, auditable y replicable. Además, complica la incorporación de nuevos miembros al equipo y la transferencia de conocimientos técnicos. Impacto: Esto resulta en un incremento de errores operativos, pérdida de trazabilidad, dependencia del conocimiento tácito y una eficiencia reducida del equipo de TI.

- **Gestión reactiva no orientada a la ciberseguridad:** El área de TI solo reacciona ante incidencias operativas, sin una perspectiva preventiva ni un enfoque en ciberseguridad. No se llevan a cabo análisis proactivos, monitoreo de comportamientos ni identificación de amenazas internas. Impacto: Esto aumenta la vulnerabilidad ante ataques, provoca una detección tardía de incidentes y genera un incumplimiento de los estándares de seguridad.

- **Sistemas críticos sin monitoreo de seguridad:** Plataformas como SAP, Active Directory y sistemas de almacenamiento funcionan sin un monitoreo adecuado de eventos de seguridad. No hay alertas para accesos no autorizados, modificaciones sospechosas ni registros consolidados. Impacto: Esto eleva el riesgo de brechas de seguridad, pérdida de datos, robo de información sensible y compromete la integridad de los sistemas.

- **Falta de políticas y controles basados en estándares:** No se han establecido políticas, normativas ni controles que alineen la gestión de TI con estándares como ISO 27001 o NIST. Esto incluye la falta de control de logs, gestión de vulnerabilidades y planes de respuesta.

- **Ausencia de base de conocimientos y buenas prácticas:** No existe una base documental que permita registrar soluciones previas, errores comunes o guías operativas. Esto impide la mejora continua, el aprendizaje organizacional y el soporte ágil ante problemas conocidos.
  Impacto: Reducción de la eficiencia operativa, pérdida de conocimiento valioso, y mayor tiempo en resolver problemas repetitivos.
  Ausencia de capacitación estructurada: No se cuenta con manuales ni capacitaciones formales para nuevos colaboradores en temas de ciberseguridad y operación de TI. Esto genera criterios dispares, uso indebido de recursos y desconocimiento de riesgos

3.10 Resumen de criticidad

Establecidos los riesgos, se ingresan a la matriz con la probabilidad e impacto para obtener el cálculo de la magnitud.

Por medio de la revisión de los riesgos, sus consecuencias y sus valores en las dimensiones de Probabilidad (P) e Impacto (I), se desarrolla la siguiente tabla con el indicé de Magnitud (M) y Criterio de aceptación (CA).

Tabla 7 Matriz de criticidad

N°	RIESGO	P	I	M	C A
1	Dependencia de un solo analista	5	5	25	
2	Falta de documentación y procedimientos	4	4	16	
3	Gestión reactiva no orientada a la ciberseguridad	4	5	20	
4	Sistemas críticos sin monitoreo de seguridad	4	5	20	
5	Falta de políticas y controles basados en estándares	3	5	15	
6	Ausencia de base de conocimientos y buenas prácticas	3	4	12	
7	Ausencia de capacitación estructurada para nuevos colaboradores	3	4	12	

Fuente: Elaboración propia. Referencia: https://tractian.com/es/blog/todo-sobre-la-matriz-de-criticidad

En conclusión, el análisis de criticidad pone de manifiesto una situación alarmante para la continuidad y la seguridad operativa del área de TI, con varios factores que tienen un impacto alto y crítico. Los principales riesgos que se han identificado son:

- **Dependencia de un solo analista (M=25):** Constituye un punto único de falla que puede paralizar los servicios TI ante cualquier ausencia, afectando gravemente la continuidad operativa y la capacidad de

respuesta ante incidentes.

- **Gestión reactiva sin enfoque en ciberseguridad (M=20):** La falta de un enfoque preventivo incrementa la vulnerabilidad frente a amenazas y ataques, elevando el riesgo de incidentes no detectados y el incumplimiento de estándares de seguridad.
- **Sistemas críticos sin monitoreo de seguridad (M=20):** La ausencia de alertas y registros en plataformas clave como SAP y Active Directory expone a la organización a brechas de seguridad, accesos no autorizados y pérdida de datos sensibles.
- **Falta de políticas y controles basados en estándares (M=15):** La carencia de alineamiento con marcos como ISO 27001 o NIST impide una gobernanza efectiva de la seguridad y debilita la gestión de riesgos.
- **Falta de documentación, base de conocimientos y capacitación (M entre 12 y 16):** Estos factores generan una gestión ineficiente, dependencia del conocimiento tácito y dificultad en la incorporación de nuevos colaboradores, impactando directamente en la capacidad operativa y la mejora continua.

En conclusión, La mayoría de los riesgos que hemos identificado tienen un impacto alto o crítico, lo que significa que necesitamos actuar rápidamente para mitigarlos. Es fundamental que prioricemos la implementación de medidas correctivas, como la creación de redundancias en el personal, el monitoreo de sistemas críticos, la estandarización de políticas y procedimientos, y el desarrollo de capacidades internas. Estas acciones son esenciales para garantizar la resiliencia, continuidad y seguridad de los servicios de TI en nuestra organización.

4. PROPUESTA DE MEJORA

4.1 identificación de los procesos

Basado en los procesos que se describen en el punto 3.2, se ha detectado que la gestión de accesos y privilegios en el Área de Tecnologías de la Información tiene varias oportunidades de mejora. Actualmente, este proceso está centralizado en un solo analista y le falta formalización, automatización y trazabilidad. Además, se están utilizando herramientas poco seguras, como hojas de cálculo de Excel, para registrar información sensible, lo que pone en riesgo la confidencialidad, integridad y disponibilidad de los activos de información.

4.1.1 Proceso a mejorar:

Gestión de accesos y privilegios (creación de cuentas, asignación de equipos y permisos en carpetas compartidas).

4.1.2 Motivo de mejora:

- Alta dependencia de un único analista TI (riesgo operativo).
- Ausencia de un sistema de gestión de identidades centralizado.
- Falta de trazabilidad y auditoría de los accesos otorgados.
- Uso de medios manuales (Excel) que impiden eficiencia, control y seguridad.

4.1.3 Objetivo de la mejora:

Diseñar e implementar un proceso estandarizado y documentado para la gestión de accesos, que incluya automatización, trazabilidad y control de privilegios, con el apoyo de herramientas especializadas (por ejemplo, Active Directory con políticas de grupo, herramientas de ticketing, y sistemas de gestión de identidades).

4.2 Equipo de trabajo

Para llevar a cabo esta mejora, se conformará un equipo multidisciplinario con los siguientes roles:

- **Rol 01: Líder de Proyecto TI**

Descripción del cargo: Responsable de la planificación, ejecución y control del proyecto de mejora. Será el enlace entre los stakeholders y el equipo técnico.

Perfil profesional: Ingeniero en Informática, Civil en Computación o afín. Experiencia en gestión de proyectos tecnológicos, metodologías ágiles y conocimiento en procesos ITIL. Deseable certificación PMP o Scrum Master.

- **Rol 02: Especialista en Seguridad de la Información**

Descripción del cargo: Encargado de asegurar que las prácticas de gestión de accesos cumplan con los principios de mínima privilegiación, confidencialidad y auditoría. Diseña políticas de control de accesos y participa en la implementación segura del proceso.

Perfil profesional: Ingeniero en Ciberseguridad o Informático con especialización en seguridad. Conocimientos de ISO/IEC 27001, NIST, gestión de identidades y accesos (IAM), y experiencia en implementación de controles técnicos y normativos.

- **Rol 03: Administrador de Sistemas**

Descripción del cargo: Responsable de la configuración técnica de los sistemas involucrados en la gestión de cuentas, privilegios y equipos. Implementa políticas en Active Directory, automatiza procesos y mantiene los registros técnicos.

Perfil profesional: Técnico o Ingeniero en Administración de Redes o Sistemas. Experiencia con servidores Windows, Active Directory, Group Policy, scripting (PowerShell), herramientas de gestión de inventario y ticketing.

- **Rol 04: Analista de Procesos / Documentador**

Descripción del cargo: Encargado de levantar, documentar y formalizar los procedimientos actuales y futuros. Apoya en el diseño del flujo de trabajo y la mejora continua del proceso.

Perfil profesional: Profesional del área de calidad o informática, con experiencia en levantamiento de procesos, BPM (Business Process Management), elaboración de procedimientos, diagramas de flujo y manuales operativos.

4.3 CICLO DE DEMMING

4.3.1 Plan (Planificar)

Establecer las bases técnicas, operativas, económicas y normativas para la implementación de un SOC ajustado a las necesidades reales de la organización.

- **Análisis de contexto y riesgos:** En esta etapa se examinan los incidentes de seguridad sufridos por la organización, tales como accesos no autorizados, propagación de malware o pérdida de datos sensibles. Se aplican metodologías como OWASP Risk Rating o ISO/IEC 27005 para evaluar el impacto de cada incidente y estimar el riesgo actual.
- **Se identifican:** Vectores de ataque: phishing, explotación de vulnerabilidades, movimiento lateral.
- **Activos comprometidos:** servidores críticos, bases de datos con información personal o financiera.
- **Vulnerabilidades:** configuraciones inseguras, software desactualizado, credenciales débiles.

Este análisis sirve como insumo para definir las capacidades mínimas que el SOC debe tener.

- **Definición de funciones del SOC**

Aquí se especifican los servicios que entregará el SOC. Estos pueden agruparse en:

- **Detección temprana de amenazas** (a través de SIEM y análisis de comportamiento).
- **Gestión y respuesta a incidentes** (con protocolos formales y trazabilidad).
  - Análisis forense digital post-incidente.
  - Reportes ejecutivos sobre métricas clave de seguridad.
  - Cumplimiento regulatorio (ISO/IEC 27001, NIST, etc.).
- **Establecimiento de Línea Base a través de Marcha Blanca**

  Como fase inicial para comenzar la validación, planeamos llevar a cabo una prueba piloto operativa del SOC. Esta fase, con una duración ya establecida de 6 meses, tiene como fin primordial analizar los indicadores que entreguen durante estos 2Q

En este tiempo, llevaremos a cabo una recogida metódica de información relacionada con los indicadores clave de desempeño (KPIs) que se han fijado en este proyecto, por ejemplo:

- MTTD (Mean Time to Detect)
- MTTR (Mean Time to Respond)
- Cobertura del SIEM sobre activos críticos
- Cantidad de eventos detectados
- Nivel de cumplimiento con marcos normativos (ISO/IEC 27001, NIST CSF)
- Tasa de mitigación de vulnerabilidades críticas

- **Disponibilidad operativa del SOC**: Los datos que se recaben a lo largo de esta etapa harán posible crear un punto de partida medible; este servirá como un estándar de contraste claro para las metas de optimización que se fijen en los indicadores clave del SOC.

  A su vez el análisis será complementado mediante una evaluación de brechas (gap analysis) respecto a controles técnicos y de gestión

establecidos por normativas y frameworks reconocidos, lo que permitirá establecer el grado actual de madurez y el nivel presente de desarrollo y a decidir objetivos posibles y verificables.

En consecuencia, la base inicial que arroje este simulacro se presenta como una entrada técnica primordial para:

- Cuantificar el impacto de la implementación del SOC.
- Establecer metas realistas de mejora continua.
- Validar los procesos de monitoreo, respuesta e informes definidos.
- Alinear las capacidades del SOC con requerimientos normativos y de auditoría.

De esta manera las métricas y sus mejoras se miden con los siguientes:

Marcha blanca: Reducir el MTTD (Mean Time To Detect) y MTTR (Mean Time To Respond) al menos en un 40%, respecto de los niveles actuales.
Definición de requisitos técnicos, humanos y financieros
Técnicos: herramientas SIEM (p. ej. Splunk, QRadar), EDRs (CrowdStrike, SentinelOne), firewalls de nueva generación, segmentación de red, autenticación multifactor, servidores de almacenamiento seguro.
Humanos: Analistas SOC N1 (monitorización 24/7).
Analistas N2/N3 (investigación avanzada, respuesta).
Arquitectos de seguridad y consultores especializados.
Financieros: incluye licencias, costos de hardware/software, personal, capacitación, servicios profesionales externos. Se elabora un presupuesto anual y un análisis costo/beneficio proyectado.

- **Definición del Modelo Operativo del SOC**
  Para implementar un Centro de Operaciones de Seguridad (SOC), se contemplan tres modelos operativos posibles:

SOC Interno: El centro es completamente gestionado por personal propio de la organización. Esta modalidad ofrece el mayor control sobre los procesos, decisiones estratégicas y la gestión directa de incidentes.
Requiere inversión significativa en infraestructura, contratación y capacitación de personal especializado.

SOC Externo (SOC-as-a-Service): Todo el servicio es entregado por un proveedor externo, normalmente bajo un modelo 24/7. Reduce los costos iniciales y permite una rápida implementación, pero conlleva riesgos en cuanto a dependencia del proveedor, pérdida de visibilidad y menor alineación con los objetivos estratégicos del negocio.

SOC Híbrido: Combina elementos de los modelos anteriores. Generalmente, se externalizan las operaciones tácticas (monitoreo, respuesta inicial), mientras que el control estratégico, la gestión de políticas y decisiones críticas se mantienen dentro de la organización. Es un enfoque flexible y escalable, especialmente recomendado para organizaciones en transición.

A fin de estructurar adecuadamente la operación del SOC, se definen los flujos de trabajo fundamentales para la gestión de incidentes:
Detección → Análisis → Contención → Erradicación → Recuperación → Lecciones aprendidas
Cada etapa es clave para minimizar el impacto de los incidentes de ciberseguridad y fortalecer continuamente la postura defensiva de la organización.

- **Modalidad definida**

Si bien el modelo híbrido es una opción recomendada por su equilibrio entre control y eficiencia operativa, tras analizar las necesidades específicas de la organización, su madurez tecnológica y los requerimientos estratégicos de seguridad, se concluye que la modalidad más adecuada es el modelo SOC Interno. Esta opción permite:

Control total sobre la gestión de incidentes y activos críticos.
Mayor confidencialidad y resguardo de la información sensible.
Personal alineado con la cultura organizacional y los objetivos del negocio.
Capacidad para adaptar rápidamente políticas y procesos a contextos cambiantes.
Aunque implica una inversión mayor, el modelo interno proporciona mayor autonomía, conocimiento interno acumulado y una respuesta más ágil y contextualizada ante amenazas, elementos fundamentales para una empresa que considera la ciberseguridad como un pilar estratégico de su operación.

- **Marco normativo aplicado:**

ISO/IEC 27001: gestión de seguridad de la información.
NIST CSF: identificación, protección, detección, respuesta y recuperación.

- **Cronograma de implantación**

Dividido en seis fases a lo largo de 21 semanas. Cada fase tiene responsables, tareas específicas y resultados esperados. Se consideran contingencias, y se definen hitos de control.

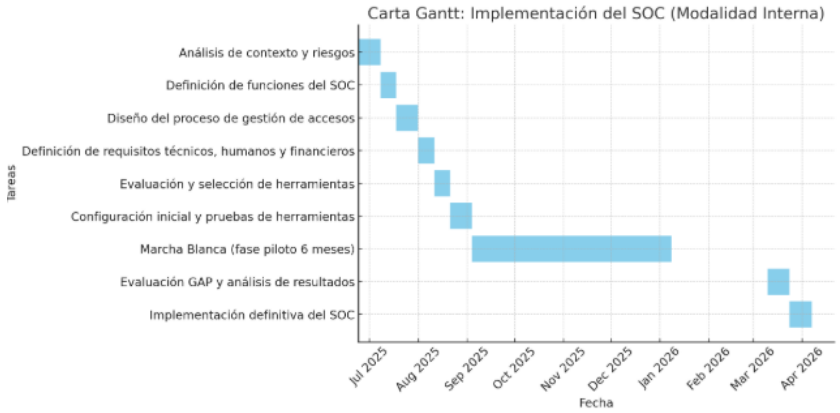
Tabla 8 Cronograma de implementación

Nº	Fase / Tarea	Fecha de Inicio	Duración (días)	Fecha de Término
1	Análisis de contexto y riesgos	24-06-2025	14	08-07-2025
2	Definición de funciones del SOC	08-07-2025	10	18-07-2025
3	Diseño del proceso de	18-07-2025	14	01-08-2025

	gestión de accesos			
4	Definición de requisitos técnicos, humanos y financieros	01-08-2025	10	11-08-2025
5	Evaluación y selección de herramientas	11-08-2025	10	21-08-2025
6	Configuración inicial y pruebas de herramientas	21-08-2025	14	04-09-2025
7	Marcha Blanca (fase piloto de 6 meses)	04-09-2025	126	10-03-2026
8	Evaluación GAP y análisis de resultados	10-03-2026	14	24-03-2026
9	Implementación definitiva del SOC	24-03-2026	14	07-04-2026

Fuente: Elaboración propia. Referencia: https://create.microsoft.com/es-es/templates/diagramas-de-gantt

Ilustración 7 Carta Gantt



Fuente: Elaboración propia. Referencia: https://create.microsoft.com/es-es/templates/diagramas-de-gantt

4.3.2 Do (Hacer)

Ejecutar la implementación técnica y operativa del SOC según el plan.

- **Adquisición e instalación de tecnología**
  - **SIEM:** Se implementa (por ejemplo) **IBM QRadar**, con integración de logs de firewalls, endpoints, AD, correos electrónicos y aplicaciones.
  - **NGFW:** Firewalls con funcionalidades IDS/IPS, inspección profunda (Deep Packet Inspection).
  - **Soluciones EDR:** Desplegadas en estaciones de trabajo y servidores críticos para detección y respuesta avanzada.
  - **Escáneres de vulnerabilidades:** Nessus o Qualys, automatizando los escaneos semanales.
  - **MFA: I**mplementada en accesos críticos como VPN, consolas administrativas, correos corporativos.

- **Integración del SIEM**

Se configuran colectores de logs y agentes para sistemas Windows, Linux, bases de datos, servicios en la nube (p. ej. Microsoft 365 o AWS), routers, switches, etc.

Se crean dashboards personalizados y alertas por tipo de evento:

Login fallidos repetidos

Cambios en cuentas privilegiadas

Transferencia de grandes volúmenes de datos.

- **Capacitación del personal**

Se ejecutan capacitaciones prácticas:

Analistas SOC: uso del SIEM, gestión de incidentes, análisis forense.

Usuarios clave: identificación de phishing, políticas de contraseñas, reporte de incidentes.

Evaluaciones pre y post capacitación aseguran efectividad del aprendizaje.

- **Desarrollo de procedimientos**

Se redactan y validan: Manuales de respuesta a incidentes.

Playbooks específicos: ransomware, phishing, acceso no autorizado.

Protocolos de escalamiento, comunicaciones internas y con clientes.

- **Pruebas piloto**

Se simulan incidentes para verificar detección, reacción, comunicación, documentación y cierre de incidentes. Ejemplos:

Ataque tipo ransomware en entorno controlado.

Exfiltración de datos simulada.

Compromiso de credenciales administrativas.

4.3.3 Check (Verificar)

Evaluar cuantitativa y cualitativamente la eficacia de la implementación del SOC.

- **Análisis de indicadores clave (KPIs)**

Se miden métricas antes y después de la implementación:

Tabla 9 Indicadores KPIs

KPI	Valor Esperado
MTTD	Reducción ≥40%
MTTR	Reducción ≥40%
Cobertura SIEM	≥90% activos críticos

KPI	Valor Esperado
Eventos detectados	+50% de incremento
Cumplimiento ISO/NIST	≥85%
Usuarios capacitados	≥80%
Vulnerabilidades críticas	100% mitigadas
Disponibilidad del SOC	100% (en horario definido)

Referencia: https://asana.com/es/resources/key-performance-indicator-kpi

- **MTTD (Mean Time to Detect)**

¿Qué mide?

El tiempo promedio que tarda el SOC en detectar una amenaza o incidente desde que ocurre.

¿Para qué sirve?

Permite evaluar la **eficiencia del sistema de monitoreo** y alerta temprana. Mientras menor sea el MTTD, más efectiva es la detección.

Formula

$$\text{MTTD} = \frac{\sum(\text{Hora de detección} - \text{Hora de inicio del incidente})}{\text{Total de incidentes}}$$

Valor Esperado: Reducción ≥ 40% respecto a la línea base

Justificación: Un SOC efectivo permite reducir significativamente el tiempo de detección, pasando de días o semanas (sin SOC) a horas o minutos. Esto reduce el daño y facilita respuestas más rápidas.

- **MTTR (Mean Time to Respond)**

¿Qué mide?

El tiempo promedio que tarda el SOC en responder y contener un incidente desde que es detectado.

¿Para qué sirve?

Evalúa la capacidad de respuesta del equipo de seguridad, fundamental para

limitar el impacto de los incidentes.

Formula

$$\text{MTTR} = \frac{\sum(\text{Hora de contención} - \text{Hora de detección})}{\text{Total de incidentes}}$$

Valor Esperado: Reducción ≥ 40% respecto a la línea base

Justificación: Al tener personal especializado y procedimientos definidos, el SOC permite una respuesta más rápida que la observada en ambientes sin monitoreo 24/7.

- **Cobertura SIEM**

¿Qué mide?

El porcentaje de activos críticos de la empresa que están monitoreados y reportando eventos al SIEM (Security Information and Event Management).

¿Para qué sirve?

Garantiza la visibilidad sobre los sistemas más importantes para detectar anomalías o ataques.

Formula

$$\text{Cobertura SIEM} = \left(\frac{\text{Activos críticos monitoreados}}{\text{Total de activos críticos}}\right) \times 100$$

Valor Esperado: ≥ 90%

Justificación: Una cobertura superior al 90% en activos críticos asegura que los puntos más sensibles del negocio estén bajo vigilancia constante.

- **Eventos Detectados**

¿Qué mide?

La cantidad de eventos o incidentes de seguridad detectados tras la implementación del SOC.

¿Para qué sirve?

Indica la efectividad del monitoreo. Un aumento en los eventos detectados

muestra mejor capacidad para identificar amenazas que antes pasaban desapercibidas.

Formula

$$\text{Incremento}\% = \left(\frac{\text{Eventos post-SOC} - \text{Eventos pre-SOC}}{\text{Eventos pre-SOC}} \right) \times 100$$

Valor Esperado: +50% de incremento

Justificación: Un SOC y un SIEM correctamente configurados deberían permitir detectar al menos un 50% más de eventos que antes no eran visibles.

- **Cumplimiento ISO/NIST**

¿Qué mide?

El porcentaje de cumplimiento con controles de seguridad definidos por marcos como ISO/IEC 27001 o NIST CSF.

¿Para qué sirve?

Refleja el nivel de madurez y alineación del SOC con estándares internacionales.

Formula

$$\text{Cumplimiento} = \left(\frac{\text{Controles cumplidos}}{\text{Total de controles aplicables}} \right) \times 100$$

Valor Esperado: ≥ 85%

Justificación: Un SOC bien estructurado debería cumplir al menos el 85% de los controles aplicables, lo que respalda auditorías, certificaciones y gobernanza.

- **Usuarios Capacitados**

¿Qué mide?

El porcentaje de usuarios internos capacitados en seguridad informática y respuesta a incidentes.

¿Para qué sirve?

Evalúa la conciencia y preparación del personal, que es clave para prevenir ataques como phishing o ingeniería social.

Fórmula:

$$\text{Capacitación} = \left(\frac{\text{Usuarios capacitados}}{\text{Total de usuarios}} \right) \times 100$$

Valor Esperado: ≥ 80%

Justificación: La formación del personal reduce significativamente los incidentes causados por error humano, responsables de más del 70% de los ataques exitosos según estudios de Verizon.

- **Vulnerabilidades Críticas Mitigadas**

¿Qué mide?

La mitigación total de vulnerabilidades críticas identificadas en los activos críticos de la organización.

¿Para qué sirve?

Garantiza que las amenazas más graves sean resueltas, reduciendo el riesgo de explotación.

Fórmula:

$$\text{Mitigación\%} = \left(\frac{\text{Vulnerabilidades críticas mitigadas}}{\text{Total de vulnerabilidades críticas detectadas}} \right) \times 100$$

Valor Esperado: 100%

Justificación:

Las vulnerabilidades críticas representan alto riesgo. Su corrección total es una exigencia mínima para mantener la seguridad operativa.

Disponibilidad del SOC

¿Qué mide?

El porcentaje de tiempo en que el SOC estuvo activo y operando dentro del horario definido (ej. 8x5 o 24x7).

¿Para qué sirve?

Asegura que el SOC esté funcionando conforme al SLA, sin interrupciones.

Fórmula:

$$\text{Disponibilidad} = \left(\frac{\text{Tiempo de operación real}}{\text{Tiempo de operación planificado}} \right) \times 100$$

Valor Esperado: 100% en horario definido

Justificación: La continuidad operativa del SOC es crítica. Cualquier caída puede significar un punto ciego en la seguridad de la empresa.

- **Auditorías internas**

Revisión formal de:

Cumplimiento de procedimientos

Configuraciones del SIEM

Trazabilidad de incidentes

Accesos privilegiados

Se utilizan listas de chequeo y evidencia documentada.

- **Retroalimentación cualitativa**

Encuestas a analistas, usuarios, directivos.

Entrevistas semiestructuradas con líderes de TI y Seguridad.

Documento de lecciones aprendidas, insumo para el siguiente ciclo PDCA.

4.3.4 Act (Actuar)

Incorporar ajustes basados en las deficiencias detectadas, con enfoque en la mejora continua.

- **Optimización del SIEM**

Ajuste de reglas: reducción de falsos positivos.

Inclusión de nuevas reglas correladas según tácticas MITRE ATT&CK.

Integración con otras fuentes: soluciones CASB, herramientas de threat

intelligence.

- **Actualización de procedimientos**

Reescritura de manuales de respuesta con base en casos reales.

Inclusión de nuevos escenarios de ataque.

Formalización de políticas de escalamiento técnico y comunicacional.

- **Fortalecimiento de formación**

Nuevos módulos según brechas detectadas (e.g. amenazas internas, phishing dirigido).

Material actualizado por perfil (usuarios, operadores, directivos).

Certificaciones internas o externas (p. ej. CompTIA Security+, SOC Analyst).

- **Ampliación de la cobertura**

Integración de activos omitidos (IoT, SCADA).

Hardening adicional de endpoints críticos.

Revisión de accesos remotos y privilegios.

- **Sostenibilidad y mejora continua**

Establecimiento de comité de seguridad.

Auditorías semestrales del SOC.

Actualización tecnológica progresiva.

Plan de evolución del SOC hacia capacidades de Threat Hunting o SOAR.

- **Proceso de implementación**

La tarea de instalar el Centro de Operaciones de Seguridad (SOC) se desarrollará siguiendo un planteamiento sistemático y progresivo, ya que se optará por descomponerlo en seis fases no simultáneas, que aseguran un despliegue organizado, eficaz y conforme a las pautas que señala la estrategia de la organización. Este despliegue del SOC ocupará seis meses y se desarrollará bajo la gestión de un equipo formado por un director de

proyecto, un consultor en ciberseguridad, técnicos de infraestructura, el responsable de cumplir con la normativa y usuarios clave de las distintas áreas de la organización.

La fase de planificación será la primera de dos que conformarán el proceso, ya que durante esta fase se formalizará el equipo de trabajo siendo asignadas las funciones y responsabilidades de sus integrantes; el jefe de proyecto será el responsable de convocar al equipo y alinear a los integrantes para asegurarse de que todos en la convocatoria comprendan el alcance del SOC y su importancia en la protección de la empresa. Mientras se realiza la alineación del equipo, el consultor en ciberseguridad levantará la información de los procesos actuales de la seguridad de la información, sacando a la luz las prácticas actuales, los débiles, las duplicidades y las carencias de procedimientos y herramientas; a su vez, esta información será recogida por el responsable de cumplimiento, quien revisará las políticas y su alineación con normas como la ISO/IEC 27001 y el marco NIST, generando un informe de brechas normativas que será una de las entradas para la siguiente fase.

Una vez conocido el punto de partida de la organización se pasará a la segunda fase del proyecto, cuyo objetivo es la elaboración de la arquitectura técnica y operativa del SOC. En este momento el consultor en ciberseguridad implementará el modelo operativo (centralizado, híbrido o tercerizado), las principales funciones del SOC, los niveles de monitorización que son necesarios, así como los workflows de detección, análisis, respuesta y recuperación en caso de incidentes. Al mismo tiempo, el especialista en infraestructura determinará las tecnologías que se necesitan para que esa operación sea viable (plataforma SIEM, escáneres de vulnerabilidades, mecanismos de autenticación multifactor, sistemas de detección de intrusos IDS/IPS, etc.) e identificará la posibilidad de que estas herramientas sean integradas en el entorno tecnológico de partida. De igual manera, el responsable de cumplimiento elaborará nuevos documentos normativos (políticas de gestión de incidente, manuales de respuesta, playbooks operativos para abordar diferentes tipos de amenazas, etc.) que serán revisitados

junto con los equipos técnicos y legales.

Una vez que se haya definido la parte técnica de la arquitectura y de las herramientas que componen el SIEM, se llevará a cabo la implementación técnica del mismo. Al igual que con la parte arquitectónica, la implementación técnica del SIEM puede llevarse a cabo tanto como un todo o, como más comúnmente se suele hacer, dividir esta etapa de la implementación del SIEM en sub etapas. La instalación y configuración del SIEM se iniciará siguiendo una implementación basada en el uso de las principales fuentes de eventos tales como firewalls, servidores, endpoints y sistemas de correo, todo ello llevado a cabo por el especialista en infraestructura o por el especialista en SIEM. El especialista en infraestructura o el experto en SIEM comenzará a definir reglas básicas para la correlación de eventos virales o eventuales suplantaciones de la identidad con el mínimo cambio estructural, la configuración de los paneles del SIEM donde se supervisarán todos los eventos, etc. A la par que se lleva a cabo todo lo expuesto, también se rediseñará la segmentación de la red interna, creando zonas clasificadas según niveles de riesgo y aplicación de filtros, así como la configuración de firewalls de nueva generación que contengan reglas de inspección profunda. Seguido de todo esto, el consultor en ciberseguridad, por su parte, liderará la implementación de autenticación multifactor en sistemas críticos, tales como accesos remotos, consolas administrativas y aplicaciones financieras. Esto se hará, como no puede ser de otra forma, en estrecha coordinación con los usuarios que entran en este tipo de procesos, ya que ellos poseen buenas prácticas de gestión del proceso de acceso hacia las aplicaciones. Esto, para que los accesos a tales sistemas se realicen de una forma controlada y ajustada, de modo que anime al usuario, minimizando el riesgo de que lleve a cabo un ataque mediante el robo de credenciales.

Fundada una base tecnológica del SOC, se pasará a la etapa de robustecimiento de procesos y formación de usuarios. En esta fase, se desarrollará una clasificación pormenorizada de los activos tecnológicos, determinando cuáles

son críticos para la operación y se actualizará el inventario de los activos institucionales asignando responsables por cada sistema. Así mismo se revisarán los procesos de gestión de incidentes, con el fin de mejorar los flujos de notificación, de análisis y escalamiento, se definirán mecanismos para su registro, seguimiento y cierre. El entrenamiento del personal será un eje principal durante esta fase, de tal forma que se encontrarán sesiones de práctica para usuarios técnicos y finales abordando temáticas como detección de correos maliciosos, uso seguro de contraseñas, agilidad en el reporte de incidentes. Estas capacitaciones serán dirigidas y llevadas a cabo entre el jefe de proyecto y el área de seguridad, buscando un nivel de participación superior al 80% en usuarios claves de la empresa.

Acompañando la validación de la eficacia de todas las acciones llevadas a cabo, se llevará a cabo una fase de pruebas y ajustes, mediante la cual se llevará a cabo simulacros de incidentes tanto de tipo table-top (ejercicios de forma teórica en sala) como técnicos (pruebas de tipo práctico con herramientas reales). Se simularán ataques como ransomware, exfiltraciones de datos, accesos no autorizados... y la eficacia de detección, respuesta y comunicación del SOC se tendrá que ver validando los tiempos de reacción, la precisión de los análisis y la eficacia de los protocolos. Al término de esta fase de simulaciones el consultor y el especialista en infraestructura tendrán que definir los ajustes correctivos de herramientas, configuraciones y procedimientos que se hayan visto deficientes y como consecuencia el comportamiento general del SOC optimizará su rendimiento.

Por último, tenemos ya la fase de cierre, en la cual el Project Manager recopilará la documentación generada durante la ejecución, es decir, se incorpora en esta documentación los informes de avance, la evidencia de cumplimiento, los manuales técnicos, los registros de las sesiones de formación y los resultados de los simulacros, etcétera. Esa documentación se fusionará en un informe final del proyecto que servirá para auditorías internas y para procesos de mejora continua; además, se hará una presentación ejecutiva al Comité Directivo de la

Organización, en el cual los logros alcanzados, las dificultades enfrentadas, las métricas de éxito conseguidas y las recomendaciones para la sostenibilidad del SOC en el tiempo se expongan.

En definitiva, la forma de implementar el SOC será siguiendo un enfoque sistemático teniendo presente el estado actual de la organización, el diseño de una arquitectura sólida, la integración de tecnología avanzada, el fortalecimiento de los procesos internos de la organización y la formación del personal y todo ello va a estar dentro de un marco de planificación, monitorización y evaluación de resultados. Este enfoque permitirá, a la empresa, elevar muy considerablemente su capacidad de prevenir, detectar y responder a incidentes de ciberseguridad reduciendo los riesgos operativos y proteger proactivamente sus activos críticos.

5. ANÁLISIS ECONOMICO

Costos de la propuesta de mejora

La propuesta a considerar para la implementación del Centro de Operaciones de Seguridad (SOC) conlleva una importante inversión inicial con infraestructura tecnológica, todo el personal, herramientas de monitorización y costes asociados al aseguramiento de la operación continua. Y en el fondo, la propuesta del SOC es el de un SOC capaz de un nivel de monitorización, análisis de incidentes en tiempo real y acciones de respuesta coordinada para eventos de operaciones ciberseguridiad que requiere un enfoque global de recursos, es decir, algo más que tecnología.

5.1 Costos de Infraestructura

En los costos de infraestructura se contemplan servidores físicos o virtuales, ya sean éstos dedicados al procesamiento del evento, almacenamiento de logs, redes seguras de comunicaciones, respaldo energético, etc. Además, se deben considerar los costos de adquisición o licenciamiento de una solución SIEM (Security Information and Event Management), UPS, sistemas de respaldo, firewalls de próxima generación (NGFW) y herramientas de gestión de vulnerabilidades.

5.2 Detalle estimado de infraestructura:

Tabla 10 Detalle estimado de infraestructura:

Recurso	Costo Estimado (USD)
Servidores para procesamiento (2)	8,000
Almacenamiento NAS	3,000
Firewall de nueva generación	6,500
Licencia de SIEM (anual)	12,000
UPS y respaldo eléctrico	2,000
Redes internas dedicadas (Switch + Cableado)	1,500

Recurso	Costo Estimado (USD)
Equipamiento adicional (monitores, consolas, etc.)	1,500
Total Infraestructura	**34,500**

Fuente: elaboración propia. Referencia: https://capacitacion.uc.cl/articulos/403-4-beneficios-de-aprender-analisis-de-costos-y-punto-de-equilibrio

5.3 Costos del personal

El funcionamiento del SOC requerirá una pequeña organización mínima inicial de un jefe de SOC, un par de analistas de seguridad, un especialista en infraestructura y un consultor externo durante la duración de la implementación.

Tabla 11 Tabla de costos de personal (HH y salarios)

Cargo	Cantidad	HH Mensuales	Costo Mensual (USD)	Meses	Costo Total (USD)
Jefe de SOC	1	160	2,500	6	15,000
Analistas de SOC	2	160	1,800 c/u	6	21,600
Especialista Infraestructura	1	80	2,000	3	6,000
Consultor en Ciberseguridad	1	40	3,000	3	9,000
Totales	5	—	—	—	**51,600**

Fuente: elaboración propia. Referencia: https://capacitacion.uc.cl/articulos/403-4-beneficios-de-aprender-analisis-de-costos-y-punto-de-equilibrio

5.4 Costos fijos

Los costos fijos corresponden a aquellos que no varían según el nivel de operación mensual del SOC, tales como salarios, licencias anuales y mantenimiento de equipos.

5.5 Costos fijos estimados

- Sueldos del equipo de SOC
- Licencias anuales de SIEM
- Mantenimiento y soporte técnico
- Servicios básicos (energía, internet)

Total costos fijos estimados (6 meses): USD **60,000**

5.6 Costos variables

Los costos variables consideran servicios externos por horas, contratación de cursos de capacitación puntuales, insumos de oficina y reposiciones menores durante la operación.

5.7 Costos variables estimados

Capacitaciones específicas: USD 2,000

Reposición de insumos, partes menores: USD 1,000

Servicios de consultoría adicionales: USD 1,500

Total costos variables: USD **4,500**

5.8 Resumen de costos

Tabla 12 Resumen de costos estimados

Categoría	Monto (USD)
Infraestructura	34,500
Personal	51,600
Costos fijos adicionales	8,400
Costos variables	4,500
Total General Estimado	**99,000**

Referencia: https://capacitacion.uc.cl/articulos/403-4-beneficios-de-aprender-analisis-de-costos-y-punto-de-equilibrio

Categoría	Monto (USD)

5.9 Tabla resumen de costos

Tabla 13 Tabla de resumen de costos

Ítem	Costo USD
Infraestructura	34,500
Personal	51,600
Costos fijos adicionales	8,400
Costos variables	4,500
Total	**99,000**

Fuente: elaboración propia. Referencia: https://capacitacion.uc.cl/articulos/403-4-beneficios-de-aprender-analisis-de-costos-y-punto-de-equilibrio

5.10 Análisis costo-beneficio

La utilización del SOC va a permitir disminuir al menos un 70% el tiempo de detección y respuesta ante incidentes críticos. Considerando que la empresa tuvo un impacto de aproximadamente USD 2,700,000 por incidentes cibernéticos en el último año, una reducción de tan sólo el 30% del impacto anual, justificaría plenamente la inversión realizada. También se espera una mejora significativa de la postura de cumplimiento y de la capacidad de recuperación de los activos, lo que resulta en una mejora de la confianza del mercado y de los clientes.

- **Análisis pesimista**

  En un escenario adverso, donde el SOC no logre una eficiencia superior al 30% en el primer año por factores de madurez organizacional o resistencia al cambio, la reducción de pérdidas alcanzaría solo los USD 800,000 anuales. Incluso en ese contexto, la inversión de USD 99,000 representaría un retorno a corto plazo (menor a 1 año), con un valor recuperado casi 8 veces superior al gasto inicial.

- **Análisis optimista**

En el mejor escenario, con un equipo consolidado, tecnologías bien implementadas y colaboración transversal, el SOC podría evitar hasta el 80% de los impactos económicos causados por ciberataques, lo que implicaría una reducción superior a USD 2,000,000 en pérdidas. Esto implicaría un retorno sobre la inversión (ROI) superior al 2,000% en un año y un fortalecimiento sustancial de la reputación corporativa.

- **Análisis de recuperación de inversión (ROI)**

El retorno de inversión se calcula considerando el ahorro por mitigación de impactos y la duración de la implementación. En el escenario base (reducción de daños del 50%):

Ahorro estimado anual: USD 1,350,000

Inversión: USD 99,000

ROI: (1,350,000 – 99,000) / 99,000 = **1263%**

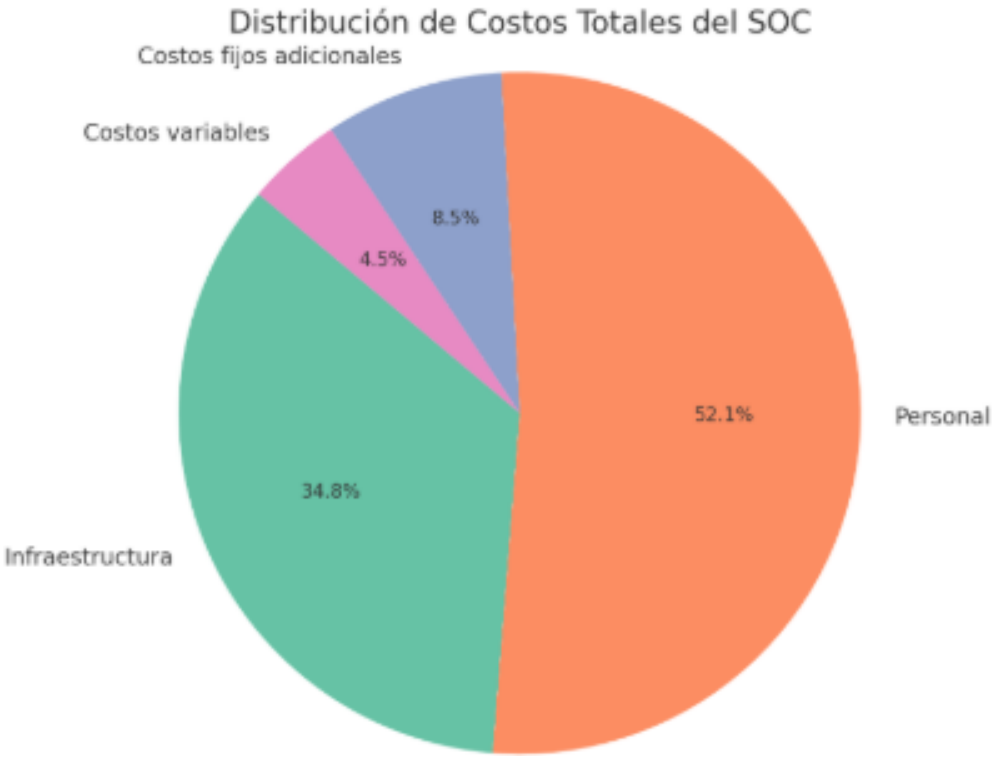
Tiempo estimado de recuperación: **menos de 3 meses**

Beneficios no económicos

Además de los beneficios financieros directos, la implementación del SOC entregará una serie de beneficios cualitativos importantes. Se fortalecerá la cultura organizacional en torno a la ciberseguridad, incrementando la conciencia de los empleados frente a riesgos digitales. También se elevará el nivel de cumplimiento normativo, permitiendo afrontar auditorías externas con mayor solidez. Por último, la percepción de clientes, proveedores y aliados respecto a la madurez tecnológica de la empresa mejorará sustancialmente, aportando a la reputación y ventaja competitiva en el mercado.

Costos totales de la implementación

Ilustración 2 Costos totales de la implementación



Referencia: https://simpliroute.com/es/blog/costos-de-distribucion-que-son-y-como-se-calculan

6. CONCLUSION

La realización de este análisis ha facilitado una exploración profunda y con un enfoque integral de los diversos factores que afectan la factibilidad técnica, económica, organizacional y operativa de establecer un Centro de Operaciones de Seguridad (SOC) en la empresa METALIM. Esta necesidad aparece como consecuencia inmediata de un serio incidente de seguridad relacionado con ingeniería social (phishing) que condujo a un ataque tipo ransomware, afectando la continuidad operacional de la empresa y ocasionando pérdidas calculadas en 1,7 millones de dólares, con repercusiones directas en su sistema SAP, propiedad intelectual, documentos legales y reputación empresarial.

El estudio ha revelado una serie de vulnerabilidades estructurales clave en el modelo vigente de gestión de tecnologías de la información y ciberseguridad, entre las que se encuentran: la dependencia de un único analista, la falta de un sistema de monitoreo 24/7, la inexistencia de políticas formales, la deficiencia en la documentación, la escasa concienciación del personal, y la falta de controles técnicos que cumplan con estándares internacionales como ISO/IEC 27001 y el marco NIST CSF. Estas vulnerabilidades amplían la superficie de ataque de la organización y la hacen fácilmente aprovechable por actores maliciosos.

Desde la perspectiva técnica, se concluyó que la implementación de un SOC facilitaría la centralización de la administración de eventos de seguridad, potenciaría la detección y respuesta, y garantizaría una adecuada trazabilidad de los incidentes. La propuesta presentada incorpora herramientas de código abierto como Wazuh, Wireshark y Alert Data, integradas en una arquitectura operativa escalable que facilitará la monitorización de endpoints, servidores, infraestructura crítica, servicios de correo y directorios activos. El diseño también considera la correlación de eventos en tiempo real, la introducción de mecanismos de respuesta automática y el refuerzo de la segmentación de red y la autenticación.

Desde el punto de vista económico, el estudio de costos revela una inversión total aproximada de USD 99.000 para la fase de implementación y funcionamiento inicial del SOC. En situaciones realistas e incluso pesimistas, el retorno sobre la inversión (ROI) puede recuperarse en menos de un año, teniendo en cuenta una disminución mínima del 30% en el impacto económico causado por incidentes. En contextos favorables, se calcula que el SOC podría prevenir pérdidas que superen los 2 millones de dólares al año, produciendo retornos superiores al 1.000%, lo que evidencia la fortaleza económica del proyecto.

En el contexto organizacional, se identifica que uno de los principales retos será el cambio cultural y la oposición al mismo. La madurez en ciberseguridad en METALIM es deficiente, con una gran dependencia del conocimiento implícito y sin una cultura de documentación o respaldo. No obstante, se reconoce la voluntad de la alta dirección para progresar en esta transformación, lo cual es un aspecto fundamental de apoyo. La formación del personal, el liderazgo en el departamento de TI, y la implantación gradual de un Sistema de Gestión de Seguridad de la Información (SGSI) son factores esenciales para el éxito del SOC.

Este análisis determina que la implementación de un SOC en METALIM no solo es viable, sino también estratégica y urgente. No aplicar este tipo de solución pone a la empresa en riesgo de enfrentar problemas financieros, operativos, legales y de reputación de gran relevancia, con consecuencias ya evidentes. El SOC facilitará la institucionalización de la seguridad como una función integral y no solo como respuesta, alineando la operación tecnológica con las metas empresariales y la sostenibilidad a largo plazo.

Se recomienda avanzar de inmediato a una etapa de diseño e implementación definitiva, basada en las siguientes acciones prioritarias:

- Formalización de un comité de seguridad de la información.
- Aprobación del presupuesto propuesto para implementación tecnológica y contratación de personal clave.
- Inicio de la marcha blanca de seis meses con indicadores claros (MTTD, MTTR, cobertura SIEM, entre otros).
- Adopción paulatina del ciclo de mejora continua PDCA bajo ISO/IEC 27001.
- Establecimiento de una cultura de seguridad transversal con capacitación periódica.

Por último, este proyecto no solo entrega una respuesta concreta al problema vivido por METALIM, sino que también propone una hoja de ruta replicable para otras empresas industriales que enfrentan los mismos desafíos en entornos operacionales híbridos (TI y OT), vulnerables y crecientemente amenazados por actores cibernéticos organizados. La ciberseguridad ya no es una opción, es un requisito para la resiliencia, continuidad y competitividad en el mercado.

7. BILIOGRAFIA

- Ahmad, A., Maynard, S. B., & Park, S. (2014). *Information security strategies: Towards an organizational multi-strategy perspective*. *Journal of Intelligent Manufacturing, 25*(2), 357–370. https://doi.org/10.1007/s10845-012-0693-8

  Utilizado en marco teórico y diseño estratégico del SOC.

- European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

  Fuente sobre amenazas como ransomware, phishing y capacidades del SOC.

- IBM Security. (2023). *Cost of a Data Breach Report 2023*. https://www.ibm.com/reports/data-breach

  Cifras de impacto económico utilizadas en análisis de pérdidas y justificación del SOC.

- Ishikawa, K. (1986). *Guide to Quality Control*. Asian Productivity Organization.

  Base teórica del diagrama de Ishikawa aplicado en pág. 25 y 38.

- ISO. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/82875.html

  Norma central en la implementación del SGSI y definición de controles A.5, A.6, A.9, A.12, A.16.

- Killmeyer, J. (2006). *Information Security Architecture: An Integrated Approach to Security in the Organization*. Auerbach Publications.

  Referencia para definición de arquitectura SOC y flujos de trabajo.

- NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. National Institute of Standards and Technology.

  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

  Base para análisis de brechas y alineación normativa del SOC.

- Rooney, J. J., & Van den Heuvel, L. N. (2004). *Root cause analysis for beginners*. *Quality Progress*, 37(7), 45–53.

  Fuente para el análisis de causa raíz citado en pág. 26.
- SANS Institute. (2020). *Incident Handler's Handbook*. https://www.sans.org/white-papers/incident-handlers-handbook/

  Utilizado para describir procedimientos de respuesta, entrenamiento y pruebas de incidentes.
- Symantec. (2019). *Internet Security Threat Report (ISTR), Volume 24*. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/istr-24

  Soporte para descripción de amenazas como phishing en entornos empresariales.
- Ubatuba. (s.f.). *¿Qué es el Diagrama de Ishikawa?* Recuperado el 20 de abril de 2025, de https://miro.com/es/diagrama/que-es-diagrama-ishikawa/

  Ilustración base para representación gráfica del análisis de causa y efecto (pág. 25).
- Gobierno de México. (s.f.). *Curso Análisis causa raíz para la investigación de incidentes y accidentes*. Recuperado el 20 de abril de 2025, de https://www.gob.mx/imp/articulos/curso-analisis-causa-raiz-para-la-investigacion-de-incidentes-y-accidentes

  Fuente secundaria para la Ilustración de análisis de causa raíz.
- DNV. (s.f.). *ISO 27001: Sistema de gestión de seguridad de la información*. Recuperado el 20 de abril de 2025, de https://www.dnv.cl/services/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-3327/

  Referencia usada para ilustración ISO27001 (pág. 28).