ANALISIS DE CIBERSEGURIDAD EN UNA EMPRESA DE SERVICIOS DE INGENIERÍA

Chavez, Lautaro Nicolas – Facen, Federico Pascal – Ferrari Giuliana – Gimenez Thiago Exequiel – Sanchez Monasterio Cesar – Sbrocco Soraire Celeste Antonella

lautaronicochavez@gmail.com - fpfacen@outlook.com - giuliferrari2001@gmail.com - gimenezthiago2019@gmail.com - cesar07sm03@gmail.com - celestesbrocco@gmail.com

Resumen

M10 Ingeniería es una empresa de servicios de ingeniería ubicada en Tucumán, Argentina, con una trayectoria de 8 años. Especializada en brindar soluciones técnicas y operativas para el sector minero y otras industrias, la empresa se dedica a ofrecer servicios que abarcan desde el diseño y la planificación de proyectos hasta el monitoreo y la optimización de procesos. Con un equipo de profesionales en diversas ramas de la ingeniería, M10 Ingeniería se esfuerza en asegurar altos estándares de calidad y seguridad en cada proyecto, priorizando la eficiencia operativa y la sostenibilidad.

En el marco de su compromiso con la mejora continua, M10 Ingeniería ha emprendido un análisis exhaustivo de la seguridad de su información, guiado por los controles y requisitos de la norma ISO 27001. Este esfuerzo incluye la creación de un inventario de activos de información, donde se identifican y clasifican los activos críticos en términos de confidencialidad, integridad y disponibilidad. Esta clasificación permite comprender la criticidad de cada activo y establece una base sólida para el desarrollo de controles de seguridad más precisos.

Los resultados del análisis han señalado varios puntos críticos. En cuanto a la seguridad física, M10 Ingeniería cuenta con medidas básicas, como el uso de tarjetas de acceso y cámaras

de vigilancia en áreas restringidas. Sin embargo, es necesario implementar controles adicionales para asegurar el acceso a las instalaciones y proteger activos críticos, especialmente aquellos que se encuentran fuera del sitio. A nivel tecnológico, el análisis revela importantes desafíos, como una protección contra malware insuficiente y deficiencias en la gestión de vulnerabilidades. No existen procedimientos formales para la detección y mitigación de riesgos técnicos, y se observan debilidades en la gestión de la configuración de sistemas, lo cual expone a la empresa a incidentes de seguridad.

De manera general, las conclusiones del estudio subrayan la necesidad de implementar políticas de seguridad más rigurosas y de fortalecer la cultura de seguridad entre los empleados. Además de los controles físicos y tecnológicos, es crucial fomentar la capacitación continua para que el personal sea consciente de los riesgos y pueda responder de manera adecuada a posibles incidentes. Este análisis sirve como una hoja de ruta para que M10 Ingeniería eleve sus estándares de seguridad de la información, alineándose con las mejores prácticas de la industria y reduciendo su exposición a posibles vulnerabilidades.

Palabras Clave: Seguridad de la Información – ISO 27001 – Gestión de Riesgos – Activos de Información – Criticidad

Introducción

El presente trabajo de campo tiene como objetivo evaluar el estado de la seguridad de la información en M10 Ingeniería, una empresa con sede en Tucumán con más de ocho años de experiencia en la provisión de servicios de ingeniería para el sector minero. La empresa enfrenta desafíos significativos en la protección de sus activos de información, entre los que se incluyen datos sensibles, sistemas críticos y procesos organizacionales. A pesar de su trayectoria, M10 Ingeniería carece de un plan formal de seguridad de la información y, debido a su estructura de

TI reducida, compuesta por un solo encargado, los controles actuales, tanto físicos como tecnológicos, requieren un fortalecimiento para asegurar la protección de sus recursos.

En este análisis, se estudia el panorama actual de seguridad de la información en la empresa, basándose en los criterios de la norma ISO/IEC 27001. Dado que M10 Ingeniería no desarrolla software propio y depende de paquetes comerciales de software para sus operaciones, la gestión de estos sistemas adquiere un papel crítico en la evaluación de riesgos. La revisión se centra en aspectos clave como el manejo de derechos de acceso, la protección de equipos y el control de accesos físicos, examinando cómo se integran estas medidas en el funcionamiento diario de la empresa.

Para obtener una perspectiva más detallada, se realizó una entrevista con el encargado de TI, quien proporcionó información valiosa sobre las prácticas actuales y las posibles debilidades del sistema de seguridad. Asimismo, el inventario de activos de la empresa se consideró un elemento fundamental del análisis, ya que permitió identificar los recursos críticos y evaluar su nivel de protección. Este estudio busca no solo identificar los principales riesgos y vulnerabilidades a los que se enfrenta M10 Ingeniería, sino también proponer recomendaciones que refuercen la confidencialidad, integridad y disponibilidad de la información, asegurando un enfoque más sólido y estructurado de la seguridad de la información en la organización.

Situación Problemática

En los últimos años, M10 Ingeniería ha experimentado un crecimiento significativo en su cartera de clientes y proyectos, especialmente en el sector minero. Este incremento en la demanda de servicios ha impulsado la adopción de nuevas tecnologías y un mayor uso de sistemas de información para la gestión de proyectos, la comunicación interna y el manejo de datos técnicos y financieros de los clientes. Sin embargo, este crecimiento acelerado ha traído consigo desafíos

organizativos que han puesto en evidencia la falta de una planificación estratégica en materia de seguridad de la información.

La empresa depende en gran medida de sistemas digitales y de paquetes comerciales de software, ya que no desarrolla software propio. Sin embargo, esta dependencia ha crecido sin un acompañamiento estructurado en términos de medidas de protección y gestión de riesgos informáticos. Las conversaciones internas han revelado inquietudes sobre la capacidad de los actuales controles tecnológicos y físicos para proteger adecuadamente los datos críticos. Además, se han registrado algunos incidentes menores no documentados de pérdida de información y accesos no autorizados que han suscitado dudas sobre la solidez del manejo de la seguridad digital.

En un entorno tan competitivo como el de la ingeniería para el sector minero, donde se manejan datos de alto valor y proyectos que requieren un alto grado de confidencialidad, la infraestructura tecnológica de M10 Ingeniería ha comenzado a ser objeto de cuestionamientos. La empresa, con una estructura de TI que cuenta con un solo encargado, enfrenta dificultades para asegurar que sus recursos estén suficientemente protegidos contra posibles riesgos cibernéticos y garantizar la confidencialidad, integridad y disponibilidad de la información. Este panorama ha llevado a los directivos de M10 Ingeniería a considerar la necesidad de realizar una revisión exhaustiva del estado actual de la seguridad de la información y de implementar mejoras que permitan una gestión más robusta y eficiente de sus activos de información.

Preguntas de Investigación

- ¿Cuáles son las políticas y controles actuales que tiene implementados M10 Ingeniería para proteger la confidencialidad, integridad y disponibilidad de la información crítica de la empresa?

- ¿De qué manera están gestionados los riesgos asociados a la seguridad de la información en M10 Ingeniería, y qué tan efectiva es la evaluación de esos riesgos en términos de prevención de incidentes?
- ¿Qué nivel de conocimiento y conciencia tienen los empleados de M10 Ingeniería sobre las mejores prácticas de seguridad de la información y cómo contribuyen a mantener un entorno seguro?

Objetivo General

Realizar un diagnóstico integral sobre el estado de la seguridad de la información en M10 Ingeniería, analizando las políticas y controles existentes, evaluando la efectividad de la gestión de riesgos, y determinando el nivel de concienciación y preparación del personal, con el fin de identificar áreas de mejora y proponer acciones que fortalezcan la protección de la información crítica de la empresa.

Objetivos Específicos

- Analizar las políticas y controles de seguridad de la información implementados en M10 Ingeniería, evaluando su adecuación para garantizar la confidencialidad, integridad y disponibilidad de los datos críticos.
- Evaluar el proceso de gestión de riesgos relacionados con la seguridad de la información en M10 Ingeniería, determinando su efectividad en la identificación y mitigación de amenazas potenciales.
- Determinar el nivel de conocimiento y conciencia del personal de M10 Ingeniería respecto a las mejores prácticas de seguridad de la información, proponiendo medidas para mejorar su capacitación si es necesario.

Marco Metodológico

La investigación adoptará un **enfoque cualitativo y cuantitativo** (mixto), ya que combinará el análisis descriptivo de políticas, procedimientos y percepción del personal, junto con la recolección de datos medibles relacionados con incidentes, controles y riesgos. El enfoque cualitativo permitirá explorar la profundidad del conocimiento y las percepciones del personal, mientras que el cuantitativo evaluará la existencia de medidas concretas y su efectividad.

Tipo de Investigación

Se realizará una **investigación descriptiva y exploratoria**:

- **Descriptiva**: Permitirá identificar y describir las políticas y controles actuales de seguridad de la información, así como la gestión de riesgos en la empresa.
- **Exploratoria**: Ayudará a descubrir posibles vulnerabilidades y áreas de mejora que no están formalmente documentadas o percibidas por la empresa.

Técnicas de Recolección de Datos

Se utilizarán diversas técnicas para garantizar un análisis completo de la seguridad de la información:

- **Revisión Documental**: Se realizará una revisión de las políticas, procedimientos, protocolos y normativas existentes en M10 Ingeniería relacionados con la seguridad de la información y la gestión de riesgos.
- **Entrevistas Semi-estructuradas**: Se entrevistará a los responsables de TI, directivos y personal clave para obtener información detallada sobre la implementación y efectividad de las políticas de seguridad, así como sus percepciones sobre los riesgos.
- **Observación Directa**: Se observarán los procesos operativos relacionados con el manejo de la información, la implementación de controles y la respuesta ante incidentes menores de seguridad.

Marco Teórico

En el contexto actual, donde la información se ha convertido en un activo fundamental para las organizaciones, la protección de datos y la seguridad de la información son temas prioritarios. La creciente digitalización y la interconexión de sistemas han incrementado la vulnerabilidad de las organizaciones frente a amenazas cibernéticas, lo que pone en riesgo no solo su integridad operativa, sino también la confianza de sus clientes y socios comerciales. En este sentido, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es esencial para salvaguardar la información crítica.

Este marco teórico explora diversos aspectos relacionados con la seguridad de la información, centrándose especialmente en la ISO 27001. Se abordarán conceptos clave que son esenciales para comprender la relevancia y la aplicación de esta norma en la gestión de la seguridad de la información dentro de las organizaciones.

Concepto de Seguridad de la Información

La seguridad de la información se define como el conjunto de prácticas y herramientas que se utilizan para proteger la información de una organización. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de los datos (Sánchez, 2011). Esto implica la implementación de controles técnicos y administrativos que aseguren la protección contra accesos no autorizados, pérdida o corrupción de datos.

ISO 27001: Sistema de Gestión de Seguridad de la Información

La ISO/IEC 27001 es la norma internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma proporciona un marco para gestionar la seguridad de la información en un enfoque sistemático y basado en riesgos (ISO, 2013). Según García (2018), la adopción de esta norma

permite a las organizaciones proteger su información de manera efectiva, adaptándose a un entorno cambiante y cumpliendo con los requisitos legales y normativos.

La norma se compone de varios elementos clave:

- **Contexto de la organización**: Comprende la identificación de las partes interesadas y sus requisitos.
- **Liderazgo**: Resalta la importancia del compromiso de la alta dirección en la implementación del SGSI.
- **Planificación**: Incluye la evaluación de riesgos y el tratamiento de los mismos.
- **Soporte**: Se refiere a la asignación de recursos y formación del personal.
- **Operación**: Se centra en la implementación de los controles necesarios.
- **Evaluación del desempeño**: Implica la medición y evaluación del SGSI.
- **Mejora continua**: Busca la mejora constante de los procesos (ISO, 2013).

3. Gestión de Riesgos

La gestión de riesgos es fundamental en la ISO 27001, ya que permite identificar, evaluar y tratar los riesgos asociados con la seguridad de la información (Cano, 2016). Esta gestión implica un proceso sistemático que incluye la identificación de amenazas, vulnerabilidades y el análisis del impacto que estos pueden tener en la organización.

Importancia de la Conciencia y Formación del Personal

La capacitación y la concienciación del personal son elementos esenciales para el éxito del SGSI. Según Alcaraz (2017), el personal debe estar debidamente formado en las políticas de seguridad y en la identificación de incidentes de seguridad. La falta de conciencia sobre la seguridad de la información puede llevar a errores humanos que comprometan la seguridad de los datos.

Controles de Seguridad de la Información

La implementación de controles de seguridad es un componente esencial de la ISO 27001. Estos controles pueden ser técnicos (como firewalls y cifrado), administrativos (políticas y procedimientos) y físicos (seguridad en el acceso a las instalaciones) (Ruiz, 2019). La elección de los controles adecuados depende de la evaluación de riesgos realizada y de las necesidades específicas de la organización.

Activos de Información

Los activos de información son todos los datos, documentos, sistemas y procesos que tienen valor para una organización. Esto incluye, pero no se limita a, bases de datos, informes, registros, software, hardware, y cualquier información que pueda influir en la capacidad de la organización para operar efectivamente y cumplir con sus objetivos. La gestión de activos de información implica no solo la identificación y clasificación de estos elementos, sino también la implementación de medidas de seguridad adecuadas para protegerlos contra accesos no autorizados, alteraciones, pérdidas o destrucciones. La identificación de activos de información es fundamental, ya que permite a la organización aplicar controles de seguridad efectivos y garantizar la confidencialidad, integridad y disponibilidad de la información (Gómez & López, 2019)

Criticidad

La criticidad se refiere a la importancia y el impacto que tiene un activo de información en las operaciones y objetivos de una organización. Los activos críticos son aquellos cuya pérdida, daño o indisponibilidad pueden causar un impacto significativo, ya sea financiero, operativo o reputacional. Evaluar la criticidad implica considerar factores como la función del activo dentro de la organización, su valor para los procesos de negocio, y las consecuencias potenciales de su compromisión. Esta evaluación es esencial para priorizar esfuerzos de

seguridad, ya que permite asignar recursos y controles de protección adecuados a los activos que son más vitales para el funcionamiento continuo y el éxito estratégico de la organización (Sánchez & Martínez, 2020).

Madurez en la Seguridad de la Información

El concepto de madurez en la seguridad de la información se refiere al nivel de desarrollo y eficacia de las prácticas de seguridad dentro de una organización. Según Espinosa (2020), un modelo de madurez permite a las organizaciones evaluar su estado actual de seguridad y planificar mejoras continuas. Un enfoque de madurez implica establecer indicadores de rendimiento, evaluar el cumplimiento de políticas de seguridad y realizar auditorías periódicas para identificar áreas de mejora.

Tendencias Emergentes en Seguridad de la Información

La seguridad de la información está en constante evolución. Las nuevas tecnologías, como la inteligencia artificial y la computación en la nube, presentan tanto oportunidades como desafíos en la gestión de la seguridad (Pérez, 2021). La ISO 27001 también se adapta a estas tendencias, permitiendo a las organizaciones incorporar nuevos controles y prácticas de seguridad en su SGSI.

Aplicación

La investigación sobre el estado de la seguridad de la información en M10 Ingeniería se llevó a cabo mediante un enfoque estructurado que abarcó varios pasos clave, cada uno diseñado para proporcionar un diagnóstico exhaustivo y fundamentado.

Entrevista con el Encargado de TI

En primer lugar, se realizó una entrevista con el encargado de TI de la organización. Durante esta fase, se formuló un conjunto de preguntas dirigidas a comprender las prácticas actuales de seguridad de la información implementadas en M10 Ingeniería. La entrevista abordó

temas como las políticas de seguridad existentes, los procedimientos de gestión de incidentes y la capacitación del personal en temas de seguridad. Se alentó al encargado a compartir su percepción sobre los riesgos más significativos que enfrenta la empresa y los desafíos operativos que podrían comprometer la seguridad de los datos. La información recolectada a partir de esta entrevista fue fundamental para establecer un contexto claro y una base sólida para las siguientes etapas del diagnóstico. Tanto la entrevista como las respuestas brindadas por el encargado de TI se encuentran en el **APENDICE A** del presente documento.

La entrevista con el encargado de TI reveló que, aunque posee una amplia experiencia en sistemas de información, carece de conocimientos específicos en seguridad de la información, lo que representa una debilidad importante en el contexto actual de ciberseguridad. La falta de capacitación formal y de un enfoque actualizado en las mejores prácticas de seguridad reduce la capacidad de la organización para anticipar y gestionar riesgos tecnológicos. Además, la dependencia de soluciones básicas y obsoletas refleja una necesidad urgente de modernización en las herramientas y procedimientos de TI. Esto también resalta la importancia de que la alta dirección considere la implementación de programas de formación y desarrollo continuo en ciberseguridad para el personal clave.

Revisión Documental

Posteriormente a la entrevista, se tenía previsto llevar a cabo una revisión documental de las políticas y procedimientos relacionados con la seguridad de la información en M10 Ingeniería. El objetivo de esta revisión era verificar la existencia y la efectividad de los controles documentados, así como su alineación con los requisitos establecidos por la norma ISO 27001. Dada la ausencia de políticas documentadas con respecto a la seguridad de la información resultó imposible realizar la revisión documental.

Cruce de Información con los Controles del Anexo de la Norma ISO 27001

Posteriormente, se llevó a cabo un cruce de la información obtenida mediante la entrevista y la observación directa realizada en la organización con los controles establecidos en el anexo de la norma ISO 27001. En esta etapa, se revisaron los anexos A.5, A.6, A.7 y A.8 de la norma, evaluando su implementación en M10 Ingeniería. Se analizó si los controles se seguían de manera efectiva y si existían evidencias de su aplicación y se asignó un puntaje de 0 a 3 para medir su cumplimiento. Este análisis no solo permitió identificar los controles que se estaban cumpliendo, sino también resaltar las áreas críticas donde había deficiencias o carencias en la protección de los activos de información. Este proceso de comparación fue esencial para comprender la alineación de la organización con las mejores prácticas internacionales en seguridad de la información. Emana de este análisis la madurez de la empresa en cuanto a seguridad de la información. Este análisis se encuentra en el **APENDICE B** del presente documento.

La evaluación de los controles bajo el marco de la norma ISO reveló que si bien algunos mecanismos de seguridad están presentes, en general, la implementación es inconsistente y carece de una gestión sistemática. Las principales áreas de debilidad incluyen la falta de un control riguroso sobre el acceso privilegiado y la gestión inadecuada de vulnerabilidades técnicas. Los controles físicos están en una condición aceptable, pero los controles tecnológicos muestran deficiencias significativas, como la falta de autenticación robusta y la gestión de configuraciones desactualizadas. Es evidente que la organización necesita reforzar sus políticas y procesos de seguridad para cumplir con los estándares internacionales y minimizar riesgos.

Elaboración de un Inventario de Activos de Información

A continuación, se procedió a la elaboración de un inventario de activos de información. Este inventario incluyó todos los activos relevantes, tales como bases de datos, servidores, software, documentos críticos, así como otros recursos tangibles e intangibles que son

esenciales para las operaciones de la empresa. Se documentaron características como la ubicación, el propietario y la clasificación de la información para cada activo, permitiendo una comprensión clara de qué información se debía proteger. Esta actividad fue crucial, ya que sentó las bases para identificar las vulnerabilidades asociadas con cada activo y estableció un marco para la posterior evaluación de riesgos.

Evaluación de la Criticidad de los Activos

La siguiente fase consistió en la evaluación de la criticidad de los activos. En esta etapa, se analizó la importancia de cada activo en función de su impacto potencial en la organización, considerando tres dimensiones fundamentales: la confidencialidad (protección de datos sensibles), la integridad (precisión y completitud de la información) y la disponibilidad (acceso oportuno a la información). Se utilizó una metodología de análisis de riesgos que permitió clasificar los activos en niveles de criticidad (alto, medio y bajo), lo que facilitó la identificación de aquellos activos que requerían una protección prioritaria. Esta evaluación se realizó mediante talleres de trabajo colaborativos, donde se involucró al personal clave, asegurando que se tuviera en cuenta la experiencia práctica en la gestión de cada activo. Este análisis, en conjunto con el inventario de activos de información, se encuentra en el **APENDICE C** del presente documento.

El análisis del inventario de activos de información ha evidenciado varias áreas de mejora en cuanto a la documentación, clasificación y gestión de los activos críticos. Si bien se han identificado activos clave, no existe una clasificación clara ni políticas de protección adecuadas en función de su criticidad. Además, los procedimientos actuales no detallan suficientemente la custodia y manejo de los activos, lo que expone a la organización a posibles fugas o pérdidas de información. El inventario también carece de una categorización adecuada

de los riesgos asociados a cada activo, lo que impide una correcta priorización de las medidas de seguridad.

Planteamiento de Mejoras Basadas en Activos y la Norma ISO 27001

Finalmente, se plantearon mejoras en base a los activos identificados y a los requerimientos de la norma ISO 27001. En esta fase, se elaboró un conjunto de recomendaciones, detalladas en el título siguiente, diseñadas para fortalecer la seguridad de la información en M10 Ingeniería. Las mejoras incluyeron propuestas para la implementación de controles adicionales donde se identificaron brechas, así como sugerencias para mejorar la documentación de políticas y procedimientos existentes. También se hicieron recomendaciones sobre la capacitación del personal en temas de seguridad de la información, fomentando una cultura organizacional orientada a la protección de datos. El objetivo final fue proporcionar un conjunto de acciones concretas y medibles que permitan a M10 Ingeniería optimizar su sistema de gestión de seguridad de la información, alineándose con los estándares internacionales y mitigando de manera efectiva los riesgos asociados con la gestión de la información.

Recomendaciones

La evaluación de la organización ha revelado múltiples áreas críticas que requieren una intervención urgente para asegurar tanto la protección de la información como la integridad de los sistemas. Durante el análisis, se detectaron debilidades en la gestión de accesos, en la seguridad de los sistemas, en la protección contra malware y en la gestión de vulnerabilidades, entre otros aspectos. Estas fallas representan riesgos significativos que podrían comprometer la operatividad de la organización, exponer información sensible o afectar su reputación.

Para abordar estos problemas, se han propuesto recomendaciones que cubren la implementación de nuevas políticas y tecnologías, así como la capacitación y concienciación del personal. Estas medidas buscan no solo mitigar los riesgos actuales, sino también sentar una

base sólida para la futura gestión de la seguridad tecnológica. A continuación, se detallan los principales aspectos abordados:

Fortalecer la gestión de accesos privilegiados y de usuarios finales:

Se recomienda un control riguroso sobre los derechos de acceso, especialmente para cuentas con privilegios elevados. La creación de un procedimiento estandarizado para asignar y revisar estos accesos reducirá los riesgos de abuso. Esto incluye implementar autenticación multifactor (MFA) para usuarios con acceso privilegiado, políticas de contraseñas robustas y auditorías trimestrales para asegurar que los accesos sean mínimos y necesarios.

Implementar un proceso formal de gestión de vulnerabilidades técnicas:

La organización debe adoptar herramientas automatizadas para el escaneo continuo de vulnerabilidades en redes y sistemas, junto con un calendario de actualizaciones y parches para abordar rápidamente las amenazas. La política debe priorizar vulnerabilidades según su criticidad, y realizar pruebas de penetración periódicas para detectar puntos vulnerables.

Fortalecer las medidas de protección contra malware y realizar formación continua:

Aunque existen controles básicos contra malware, se requiere una estrategia de protección de múltiples capas, combinando antivirus avanzados, detección de amenazas y firewalls, junto con una política de control de acceso a dispositivos externos. Igualmente, se necesita formación continua para el personal en temas como ransomware y phishing, con simulacros regulares para mejorar su capacidad de respuesta.

Mejorar la gestión y frecuencia de respaldos:

Se recomienda implementar un sistema automatizado de respaldos que defina intervalos regulares y realice pruebas de restauración trimestrales. Estos respaldos deben almacenarse en ubicaciones externas y locales para asegurar la recuperación de datos críticos en caso de desastre.

Desarrollar e implementar un sistema robusto de gestión de la configuración:

La gestión de configuración es clave para mantener la seguridad y estabilidad de los sistemas. Se propone crear un inventario detallado de sistemas y dispositivos, con auditorías regulares para garantizar configuraciones seguras. El control de cambios formal permitirá que todas las modificaciones en configuraciones o software sean aprobadas y documentadas.

Adoptar un enfoque integral de seguridad en redes:

La seguridad de las redes debe reforzarse con una estrategia de protección y segmentación. Esto incluye la implementación de sistemas de detección y prevención de intrusiones (IDS/IPS) y controles de segmentación de redes para reducir el impacto de ataques. También es importante revisar periódicamente las configuraciones de seguridad en dispositivos como routers y firewalls.

La implementación de estas medidas permitirá a la organización fortalecer sus defensas, reducir vulnerabilidades y mejorar su capacidad para responder a incidentes, logrando una protección integral de sus activos digitales y una mejor gestión de los riesgos tecnológicos.

Conclusiones

En términos generales, la evaluación de la seguridad de la información dentro de la organización revela un panorama preocupante, donde las debilidades en los controles tecnológicos y la falta de conocimientos especializados sobre seguridad son predominantes. Las entrevistas y auditorías de control destacan una necesidad crítica de mejorar la infraestructura de seguridad, desde la gestión de accesos hasta la protección contra vulnerabilidades y amenazas emergentes. La organización no cuenta con procedimientos robustos ni con un enfoque sistemático para abordar la seguridad de la información, lo que la deja expuesta a riesgos innecesarios.

Por otro lado, el inventario de activos es insuficiente para proporcionar una visión clara de los puntos vulnerables y los recursos críticos que necesitan ser protegidos. Esto subraya la necesidad de implementar una estrategia integral que no solo aborde las deficiencias tecnológicas, sino que también considere la formación del personal, la mejora de los procedimientos y la actualización continua de herramientas de seguridad.

En definitiva, la organización debe adoptar un enfoque más proactivo y holístico en la gestión de la seguridad de la información, invirtiendo en nuevas tecnologías, formalizando procesos, y asegurando que el personal clave tenga la formación necesaria para enfrentar los desafíos actuales. Esto no solo mejorará la resiliencia tecnológica, sino que también fortalecerá la capacidad de la organización para proteger sus activos más valiosos en un entorno cada vez más complejo y vulnerable.

Apéndice

APENDICE A

A.1- Entrevista al encargado de TI de M10 Ingeniería.

Sección 1: Información General

1. ***¿Cuál es su rol en la gestión de la seguridad de la información dentro de M10 Ingeniería?***
    - **Objetivo**: Comprender el nivel de responsabilidad y la posición del entrevistado en relación con la seguridad de la información en la organización.
    - **Respuesta**: "Soy el encargado de TI. Mi responsabilidad principal es asegurar que nuestros sistemas funcionen de manera eficiente y, aunque tengo en cuenta la seguridad de la información, no tenemos un enfoque formalizado en este aspecto."
2. ***¿Cuánto tiempo ha trabajado en esta posición?***

- **Objetivo**: Evaluar la experiencia del entrevistado en su rol, lo que puede influir en su comprensión de los procedimientos y desafíos de seguridad de la información.
- **Respuesta**: "He estado en este cargo desde la fundación de la empresa. Mi formación es en ingeniería de sistemas, por lo que estoy más orientado al ámbito técnico."

Sección 2: Políticas y Procedimientos

3. ***¿Existen políticas formales de seguridad de la información en la empresa?***
   - **Objetivo**: Determinar si la organización cuenta con un marco normativo para guiar la gestión de la seguridad de la información.
   - **Respuesta**: "No contamos con políticas formales de seguridad de la información. Hasta ahora, hemos manejado este tema de manera más práctica que teórica."
4. ***Si la respuesta es afirmativa, ¿podría describir brevemente estas políticas?***
   - **Objetivo**: Obtener detalles sobre el contenido y el enfoque de las políticas existentes, lo que permite identificar su alineación con las mejores prácticas.
   - **Respuesta**: "Como mencioné, no hay políticas definidas. En general, trato de seguir algunas buenas prácticas que considero relevantes."
5. ***¿Cómo se comunican estas políticas a los empleados?***
   - **Objetivo**: Evaluar la efectividad de la comunicación interna sobre las políticas, lo que afecta la concientización y el cumplimiento por parte del personal.
   - **Respuesta**: "Dado que no hay políticas documentadas, lo que hago es tocar el tema de seguridad en reuniones informales. Sin embargo, no hay un proceso estructurado para ello."

6. ***¿Existen procedimientos específicos para la gestión de incidentes de seguridad?***
    - **Objetivo**: Identificar si hay protocolos establecidos para responder a incidentes de seguridad, lo cual es crucial para mitigar riesgos.
    - **Respuesta**: "No, no tenemos procedimientos específicos. Cuando ocurre un incidente, trato de solucionarlo en el momento, pero no hay un protocolo claro."

Sección 3: Formación y Conciencia

7. ***¿Qué tipo de capacitación se ofrece al personal sobre seguridad de la información?***
    - **Objetivo**: Conocer las iniciativas de formación que se implementan para mejorar la conciencia sobre la seguridad de la información entre los empleados.
    - **Respuesta**: "No ofrecemos capacitación específica sobre seguridad de la información. La formación que brindamos es más sobre el uso de las herramientas tecnológicas que sobre prácticas de seguridad."
8. ***¿Con qué frecuencia se realiza esta capacitación?***
    - **Objetivo**: Evaluar la regularidad de las capacitaciones, lo que puede indicar el compromiso de la organización con la seguridad de la información.
    - **Respuesta**: "Dado que no hay un enfoque formal, no hay una frecuencia establecida para la capacitación."
9. ***¿Cómo evalúa la efectividad de estas capacitaciones en la concientización del personal?***
    - **Objetivo**: Comprender cómo la organización mide el impacto de la capacitación y si hay mecanismos para evaluar su efectividad.

- **Respuesta**: "Al no ofrecer capacitación en seguridad de la información, no tengo una forma de evaluar la efectividad. Siento que hay una falta de conciencia entre los empleados sobre este tema."

Sección 4: Evaluación de Riesgos

10. ***¿Se realiza alguna evaluación de riesgos en la organización?***
    - **Objetivo**: Determinar si hay un enfoque proactivo hacia la identificación y gestión de riesgos relacionados con la seguridad de la información.
    - **Respuesta**: "No hacemos evaluaciones de riesgos de forma sistemática. Hasta ahora, la seguridad de la información no ha sido una prioridad en nuestra gestión."
11. ***Si es así, ¿con qué frecuencia se llevan a cabo estas evaluaciones?***
    - **Objetivo**: Evaluar la periodicidad de las evaluaciones de riesgos, lo que puede influir en la capacidad de la organización para adaptarse a nuevas amenazas.
    - **Respuesta**: "Como no realizamos evaluaciones de riesgos, no hay una frecuencia definida."
12. ***¿Qué metodología se utiliza para la identificación y evaluación de riesgos?***
    - **Objetivo**: Conocer el enfoque utilizado para evaluar riesgos, lo que puede revelar la robustez del proceso de gestión de riesgos.
    - **Respuesta**: "No aplicamos ninguna metodología específica. En general, manejo los problemas según van surgiendo, más por experiencia que por un marco teórico."

Sección 5: Controles y Herramientas

13. ***¿Qué controles de seguridad se han implementado para proteger los activos de información?***

- **Objetivo**: Identificar los controles existentes que protegen los activos críticos de información y evaluar su adecuación.
- **Respuesta**: "He implementado controles técnicos básicos, como antivirus y firewalls. También trato de realizar copias de seguridad, aunque no siempre son tan regulares como me gustaría."

14. ***¿Utilizan alguna herramienta específica para la gestión de la seguridad de la información?***
    - **Objetivo**: Conocer las herramientas tecnológicas que la organización emplea para gestionar la seguridad, lo que puede proporcionar información sobre su nivel de sofisticación.
    - **Respuesta**: "No, no utilizamos herramientas específicas para la gestión de la seguridad de la información. Me manejo con lo que está a nuestra disposición, que suele ser bastante básico."
15. ***¿Qué mecanismos de monitoreo y respuesta se han establecido para detectar y responder a incidentes de seguridad?***
    - **Objetivo**: Evaluar la capacidad de la organización para monitorear y reaccionar ante incidentes de seguridad, lo que es crucial para minimizar daños.
    - **Respuesta**: "No contamos con un sistema de monitoreo formal. Si detecto un problema, intento abordarlo de inmediato, pero no tengo un seguimiento constante."

Sección 6: Críticas y Mejoras

16. ***Desde su perspectiva, ¿cuáles son los principales desafíos que enfrenta M10 Ingeniería en términos de seguridad de la información?***

- **Objetivo**: Recoger la opinión del entrevistado sobre los obstáculos que enfrenta la organización, lo que puede informar sobre áreas críticas a abordar.
- **Respuesta**: "Los principales desafíos son la falta de presupuesto para inversiones en seguridad y la obsolescencia de ciertos sistemas. Recientemente perdimos información debido a un fallo en un servidor."

17. ***¿Hay áreas donde considera que se podrían implementar mejoras significativas?***
    - **Objetivo**: Identificar oportunidades de mejora desde la perspectiva del encargado de TI, lo que puede guiar el desarrollo de recomendaciones.
    - **Respuesta**: "Definitivamente. Necesitamos modernizar nuestra infraestructura y establecer políticas de seguridad claras. La capacitación del personal también es un aspecto que no se puede pasar por alto."
18. ***¿Existen preocupaciones específicas sobre la seguridad de datos sensibles o críticos para la organización?***
    - **Objetivo**: Conocer las inquietudes sobre la protección de información sensible, lo que puede influir en las prioridades de mejora.
    - **Respuesta**: "Sí, la reciente pérdida de información sensible me preocupa mucho. Deberíamos tener un plan más robusto para proteger nuestros datos críticos."

APENDICE B

Análisis de controles ISO 27001

Anexo A.5 – Controles Organizacionales

A.5.1 Política de seguridad de la información: No existe una política formal, indicando falta de dirección en seguridad de la información.

A.5.2 Roles y responsabilidades de seguridad de la información: Algunos roles asignados, pero no documentados ni comunicados.

A.5.3 Segregación de funciones: Presente en algunas áreas, aunque no de manera consistente.

A.5.4 Responsabilidades de gestión: Las responsabilidades de seguridad no están formalizadas en todos los niveles.

A.5.5 Contacto con autoridades: Contactos esporádicos sin sistematización.

A.5.6 Contacto con grupos de interés especial: Participación esporádica, sin planificación estructurada.

A.5.7 Inteligencia de amenazas: No se realizan análisis formales de amenazas.

A.5.8 Seguridad de la información en la gestión de proyectos: Considerada en los proyectos, pero sin formalización.

A.5.9 Inventario de información y otros activos asociados: Falta de un inventario de activos críticos.

A.5.10 Uso aceptable de información y otros activos: Sin documentación formal de reglas

A.5.11 Devolución de activos: Procedimiento informal para devolución, sin formalización.

A.5.12 Clasificación de la información: No se clasifica formalmente la información.

A.5.13 Etiquetado de información: Sin procedimientos para etiquetar la información.

A.5.14 Transferencia de información: La información se transfiere sin controles adecuados.

A.5.15 Control de acceso: Se implementan, pero no están documentados y son débiles.

A.5.16 Gestión de identidad: Proceso de gestión de identidades básico y sin documentación.

A.5.17 Información de autenticación: Gestión informal, sin controles estrictos.

A.5.18 Derechos de acceso: Asignados, pero sin revisiones periódicas.

A.5.19 Seguridad en relaciones con proveedores: Considerada, pero sin procedimientos específicos.

A.5.20 Seguridad en contratos con proveedores: Falta de requisitos de seguridad en contratos.

A.5.21 Gestión de seguridad en cadena de suministro: No se evalúan riesgos en la cadena de suministro TIC.

A.5.22 Seguimiento de seguridad en proveedores: No se monitorea regularmente la seguridad de proveedores.

A.5.23 Seguridad en uso de servicios en la nube: Falta de procedimientos para el uso seguro de la nube.

A.5.24 Planificación de gestión de incidentes: No hay un plan para la gestión de incidentes.

A.5.25 Evaluación de eventos de seguridad: No existe proceso para categorizar eventos de seguridad.

A.5.26 Respuesta a incidentes: Respuesta no estructurada y sin procedimientos.

A.5.27 Aprendizaje de incidentes: No se documentan lecciones aprendidas de incidentes.

A.5.28 Seguridad en sistemas de comunicación: Limitada, sin controles adecuados en transmisión de información.

A.5.29 Seguridad durante la interrupción: No se cuenta con un plan para mantener seguridad en interrupciones.

A.5.30 Preparación TIC para continuidad empresarial: No hay un plan de continuidad empresarial.

A.5.31 Requisitos legales y contractuales: No se identifican ni documentan los requisitos legales de seguridad.

A.5.32 Derechos de propiedad intelectual: Falta de procedimientos para proteger la propiedad intelectual.

A.5.33 Protección de registros: Sin medidas adecuadas para proteger los registros.

A.5.34 Privacidad y protección de PII: No se cumplen los requisitos de privacidad y protección de datos personales.

A.5.35 Revisión independiente de seguridad de información: No se realizan auditorías de seguridad.

A.5.36 Cumplimiento de políticas de seguridad: Sin revisiones periódicas del cumplimiento de políticas.

A.5.37 Procedimientos operativos documentados: No se documentan procedimientos operativos de seguridad.

Anexo A.6 – Controles de Personas

A.6.1 Revisión de antecedentes: No se verifica antecedentes de candidatos, generando riesgos.

A.6.2 Términos y condiciones de empleo: No se establecen condiciones de seguridad en contratos laborales.

A.6.3 Sensibilización y formación en seguridad: No se proporciona formación en seguridad al personal.

A.6.4 Proceso disciplinario: Sin proceso formal para gestionar violaciones de seguridad.

A.6.5 Responsabilidades post-terminación de empleo: No se define seguridad después de la salida de empleados.

A.6.6 Acuerdos de confidencialidad: No hay acuerdos ni revisiones de confidencialidad periódicos.

A.6.7 Trabajo remoto: Implementado con VPN para protección en acceso remoto.

A.6.8 Informes de eventos de seguridad: No existe un mecanismo para informar incidentes de seguridad.

Anexo A.7 – Controles Físicos

A.7.1 Perímetros de seguridad física: Se han establecido perímetros de seguridad básicos que delimitan las áreas donde se almacenan activos de valor significativo.

A.7.2 Entrada física: Las áreas seguras están protegidas por controles de entrada, como tarjetas magnéticas y acceso restringido.

A.7.3 Asegurar oficinas, salas e instalaciones: Las oficinas y salas tienen medidas de seguridad implementadas, como cerraduras y controles de acceso.

A.7.4 Monitoreo de seguridad física: La instalación cuenta con un sistema básico de monitoreo, como cámaras de seguridad, para detectar accesos no autorizados.

A.7.5 Protección contra amenazas físicas y ambientales: Se han implementado medidas para proteger contra amenazas físicas, como sistemas de detección de incendios y protocolos básicos de evacuación.

A.7.6 Trabajando en áreas seguras: Las áreas seguras están equipadas con medidas de seguridad adecuadas, como control de acceso y monitoreo.

A.7.7 Escritorios limpios y pantallas despejadas: No se han implementado políticas de "escritorios limpios".

A.7.8 Ubicación y protección de equipos: El equipo se ubica en áreas seguras y se han tomado medidas para protegerlo.

A.7.9 Seguridad de los activos fuera de las instalaciones: Los activos de información se proporcionan a los empleados y estos pueden retirarlos de la empresa.

A.7.10 Medios de almacenamiento: Se cuenta con un proceso básico para gestionar los medios de almacenamiento, aunque no se cuenta con protocolos de destrucción segura.

A.7.11 Utilidades de apoyo: Las instalaciones están equipadas con sistemas de respaldo para protegerse contra cortes de energía.

A.7.12 Seguridad del cableado: Los cables de energía y datos están organizados y protegidos adecuadamente, lo que reduce el riesgo de intercepción o daño.

A.7.13 Mantenimiento de equipamiento: El equipamiento se mantiene regularmente y se han implementado políticas de mantenimiento preventivo, lo que contribuye a la disponibilidad y seguridad de la información.

A.7.14 Eliminación o reutilización segura de equipos: No existen protocolos sobre eliminación segura.

APENDICE C

ID DEL ACTIVO	NOMBRE DEL ACTIVO DE INFORMACIÓN	DESCRIPCIÓN	UBICACIÓN	ÁREA	TIPO	CLASIFICACIÓN DE LA INFORMACIÓN	CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD		CRITICIDAD		PROPIETARIO DEL ACTIVO	CUSTODIO DEL ACTIVO	PROCESO	SUBPROCESO
M8-TI-001	Servidor de base de datos	Base de datos que contiene información financiera	Sala de servidores	TI	Hardware	Interna	3	Confidencial	3	Irremplazable	3	Delicada	**27**	**Alta**	Gerente de TI	Admin. de Servidores	Gestión Financiera	Administración de bases de datos
M8-TI-002	Aplicación ERP	Sistema de gestión que centraliza las operaciones comerciales	Oficina central	Operaciones	Software	Interna	3	Confidencial	3	Irremplazable	2	Relevante	**18**	**Alta**	Gerente de Operaciones	Desarrollador del ERP	Producción	Gestión de operaciones
M8-TI-003	Correo Electrónico Corporativo	Sistema de mensajería utilizado para comunicaciones internas y externas	Nube	TI	Software	Externa	2	Uso interno	2	Recuperable	2	Relevante	**8**	**Media**	Gerente de TI	Admin. de Servidores	Comunicación	Mensajería
M8-TI-004	Manual de Procesos	Documento con procedimientos operativos estándar	Oficina de documentación	Administración	Procedimiento	Interna	2	Uso interno	1	Reemplazable	1	Estándar	**2**	**Baja**	Gerente de Administración	Responsable de Documentación	Documentación	Gestión de calidad
M8-TI-005	Respaldo de Datos Financieros	Copias de seguridad de la información financiera crítica	Almacenamiento externo	TI	Hardware	Interna	3	Confidencial	3	Irremplazable	3	Delicada	**27**	**Alta**	Gerente de TI	Admin. de Servidores	Gestión Financiera	Respaldo de datos
M8-TI-006	Base de Datos de Clientes	Información personal y de contacto de los clientes de la empresa	Servidor en la nube	Comercial	Base de Datos	Externa	3	Confidencial	3	Irremplazable	2	Relevante	**18**	**Alta**	Gerente Comercial	Responsable de TI	Gestión de clientes	Atención al cliente
M8-TI-007	Planillas de Sueldos	Documentos electrónicos que contienen la información salarial de empleados	Servidor Central	Recursos Humanos	Procedimiento	Interna	3	Confidencial	2	Recuperable	3	Delicada	**18**	**Alta**	Gerente de Recursos Humanos	Responsable de TI	Gestión de recursos humanos	Administración de personal
M8-TI-008	Sistema de Control de Inventarios	Sistema para gestionar el inventario de materias primas y productos	Servidor Central	Logística	Software	Interna	2	Uso interno	2	Recuperable	2	Relevante	**8**	**Media**	Gerente de Logística	Responsable de TI	Gestión de inventarios	Control de stock
M8-TI-009	Contratos con Proveedores	Documentación legal y acuerdos con proveedores de servicios y productos	Servidor Central	Compras	Documento	Externa	3	Confidencial	2	Recuperable	2	Relevante	**12**	**Media**	Gerente de Logística	Responsable de Compras	Gestión de compras	Proveedores
M8-TI-010	Sistema de Control de Acceso	Software y hardware que gestiona el control de acceso físico a las instalaciones	Servidor Local	Tecnología	Hardware	Interna	3	Confidencial	2	Recuperable	3	Delicada	**18**	**Alta**	Gerente de TI	Responsable de Seguridad	Gestión de seguridad física	Control de accesos

Referencias

- Alcaraz, M. (2017). *La importancia de la capacitación en seguridad de la información*. Revista de Seguridad Informática, 5(1), 35-42. Editorial Universidad Nacional de La Plata.
- Cano, A. (2016). *Gestión de riesgos en la seguridad de la información*. *Gestión y Estrategia*, 22(3), 67-78. Editorial Universidad de Buenos Aires.
- Espinosa, R. (2020). *Modelos de madurez en seguridad de la información: Un enfoque práctico*. *Revista Iberoamericana de Seguridad de la Información*, 12(1), 45-58. Editorial Universidad de Salamanca.
- García, J. (2018). *Implementación de la norma ISO 27001 en empresas: Un enfoque práctico*. *Revista Iberoamericana de Seguridad de la Información*, 11(2), 29-37. Editorial Universidad de Alicante.
- Gómez, J. A., & López, M. J. (2019). *Gestión de la seguridad de la información: un enfoque práctico*. Editorial Universitaria.
- ISO. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization.
- Pérez, S. (2021). *Tendencias en seguridad de la información: Desafíos y oportunidades*. *Revista de Tecnología y Seguridad*, 14(2), 12-19. Editorial Universidad de Zaragoza.
- Ruiz, F. (2019). *Protección de activos críticos a través de la ISO 27001*. *Revista Internacional de Seguridad y Protección*, 7(3), 100-115. Editorial Universidad de Barcelona.
- Sánchez, J. (2011). *Seguridad de la información: Conceptos y prácticas*. *Gestión de Riesgos*, 2(1), 21-32. Editorial Universidad de Valencia.
- Sánchez, R., & Martínez, A. (2020). *Análisis de riesgos en la seguridad de la información: un enfoque metodológico*. Ediciones de la U.