TRABAJO DE GRADO
Opción Seminario.

Título del trabajo
Caso 6 - Industrias metalmecánicas del valle S.A.S.

Corporación Universitaria Remington.
Nombre de la facultad: Ingenierías
Nombre del programa académico: Ingeniería de Sistemas

Nombres de los estudiantes autores del trabajo de grado.

Elber Oscar Garcia Hoyos
Kevin Minota Mosquera
Franyerson Renteria Camacho

Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Tabla de Contenidos

Resumen 4
Marco conceptual y normativo 5
Conceptos fundamentales de ciberseguridad 6
Marco normativo 7
Tabla 1. Normatividad aplicable. 7
Marco contextual 9
Descripción de la organización 9
Problemática identificada 10
Identificación y análisis de activos 11
Tabla 2. Inventario de activos 12
Justificación de los activos críticos 14
Análisis de amenazas y vulnerabilidades 14
Tabla 3. Amenazas y vulnerabilidades 15
Análisis y gestión de riesgos 17
Metodología de análisis 17
Criterios de valoración 19
Tabla 4. Criterios para la valoración de riesgos 19
Matriz de riesgos 20
Políticas y controles de seguridad 24
Desarrollo de las políticas propuestas ..... **¡Error! Marcador no definido.**
Política de Control de Accesos 27
Política de Gestión de Contraseñas 28
Política de Clasificación de la Información 29
Política de Gestión de Respaldos 30
Alcance 30
Política de Respuesta a Incidentes 30
Controles propuestos 31
Justificación de las políticas y controles 33
Gestión de incidentes y continuidad del negocio 34
Análisis de la gestión de incidentes y la continuidad del negocio 38
Cultura organizacional en ciberseguridad 40
Fortalecimiento de la cultura organizacional en ciberseguridad 44
Conclusiones 45
Referencias 47

Tabla 1. Normatividad aplicable. 7
Tabla 2. Inventario de activos. 12
Tabla 3. Amenazas y vulnerabilidades. 15
Tabla 4. Criterios para la valoración de riesgos. 19
Tabla 5. Matriz de riesgos. 20
Tabla 6. Políticas de seguridad. 24

Tabla 7. Controles de seguridad..... 31
Tabla 8. Incidentes potenciales. 35
Tabla 9. Plan básico de respuesta. 37
Tabla 10. Hallazgos organizacionales..... 41
Tabla 11. Recomendaciones de mejora. 42

Resumen

Las empresas manufactureras dependen cada vez más de sistemas digitales para operar, y esa dependencia trae riesgos que antes eran ajenos al mundo industrial: accesos no autorizados, fuga de información técnica y líneas de producción detenidas por fallas en los sistemas. Cuando la tecnología crece más rápido que las políticas y los hábitos de seguridad, la brecha termina siendo un problema de negocio. Es lo que ocurre en Industrias Metalmecánicas del Valle S.A.S., empresa colombiana con más de 25 años fabricando componentes metálicos para los sectores automotriz, agrícola e industrial, que produce más de 150.000 piezas al mes apoyada en un ERP, un sistema de ejecución de manufactura, herramientas de diseño y una infraestructura híbrida.

El presente informe expone los resultados del diagnóstico de seguridad de la información realizado a esa organización, con el propósito de identificar sus activos más importantes, las amenazas y vulnerabilidades que los afectan y las situaciones de mayor riesgo para la operación, como base para una futura gestión formal de la seguridad. El estudio describió la empresa, su estructura, sus procesos principales y la infraestructura tecnológica que los soporta; analizó las situaciones encontradas durante la evaluación y los cinco incidentes registrados en los últimos tres años, entre ellos la interrupción de una línea de fabricación por una falla de configuración, la pérdida de un portátil con diseños en desarrollo y un acceso no autorizado a información técnica mediante credenciales compartidas; estableció el marco conceptual y normativo aplicable en Colombia, incluyendo la Ley 1581 de 2012, la Ley 1273 de 2009 y los estándares ISO/IEC 27001 e ISA/IEC 62443; identificó y valoró los quince activos de información más importantes, clasificados por tipo y criticidad; y determinó las amenazas y vulnerabilidades asociadas a los activos críticos, priorizando las de mayor riesgo.

De ese ejercicio se desprenden cuatro problemas de fondo: debilidades en la gestión de accesos, falta de control sobre la información corporativa, ausencia de procedimientos para la gestión de incidentes y una cultura organizacional que delega la seguridad exclusivamente en el área de tecnología. El aporte del diagnóstico es ordenar lo que estaba disperso: qué debe proteger la empresa, qué la amenaza, por dónde es vulnerable y qué atender primero. Los resultados muestran que sus principales debilidades son organizacionales antes que técnicas, y constituyen la base para formalizar la gestión de la seguridad frente a los planes de incorporar líneas automatizadas y sensores IoT durante los próximos dos años.

Palabras clave

Palabras clave: seguridad de la información, diagnóstico, activos de información, amenazas, vulnerabilidades, riesgo.

Marco conceptual y normativo

Para comprender el diagnóstico realizado a Industrias Metalmecánicas del Valle S.A.S. es necesario precisar los conceptos sobre los que se construye el análisis.

La seguridad de la información es la preservación de la confidencialidad, la integridad y la disponibilidad de la información, sin importar el medio en que esta se encuentre: sistemas, documentos, dispositivos o el conocimiento de las personas (ISO/IEC 27001:2022, s.f.). La ciberseguridad, por su parte, es un concepto relacionado, pero más específico: se ocupa de proteger los activos digitales y los sistemas conectados frente a ataques que se originan o propagan a través del ciberespacio (MinTIC, 2021). En una empresa manufacturera como la analizada, ambas dimensiones conviven: hay información que debe protegerse en papel y en el conocimiento del personal, y hay sistemas industriales conectados que pueden ser atacados por medios digitales.

Las tres propiedades que la seguridad busca preservar se conocen como la tríada CID (ISO/IEC 27001:2022, s.f.). La confidencialidad garantiza que la información solo sea conocida por quienes están autorizados; los planos de producto de la empresa son el ejemplo más claro de información que exige esta propiedad. La integridad asegura que la información sea exacta y completa, y que solo se modifique de forma autorizada; la desincronización entre el ERP y el sistema de inventarios tras una actualización incorrecta fue una pérdida de integridad. La disponibilidad garantiza que la información y los sistemas estén accesibles cuando se necesiten; la interrupción de una línea de fabricación durante varias horas mostró lo que cuesta perderla.

Un activo de información es todo elemento que tiene valor para la organización y participa en el tratamiento de sus datos (MinTIC, 2021). Los activos pueden ser físicos, como servidores, equipos y redes; digitales, como los sistemas de información y los datos que procesan; y humanos, es decir, las personas que operan los procesos. Cada tipo enfrenta riesgos diferentes y requiere protecciones distintas, razón por la cual el inventario de activos es el punto de partida de la gestión de seguridad: no se puede proteger lo que no se conoce.

Una amenaza es la causa potencial de un incidente no deseado que puede dañar un sistema o una organización, mientras que una vulnerabilidad es una debilidad de un activo o de un control que puede ser explotada por una o más amenazas (ISO/IEC 27005, 2022). La distinción importa porque sobre las amenazas, como los atacantes externos o los errores humanos, la empresa tiene poco control; las vulnerabilidades, en cambio, sí dependen de ella y son el frente donde puede actuar. El riesgo es la combinación de ambos elementos: la probabilidad de que una amenaza explote una vulnerabilidad y el impacto que eso tendría sobre

el activo afectado (ISO/IEC 27005, 2022). Valorar los riesgos permite priorizar, porque ninguna organización puede protegerlo todo al mismo tiempo; de ahí que este informe clasifique los activos por criticidad y ordene las situaciones encontradas según su gravedad.

Los controles de seguridad son las medidas que modifican el riesgo: políticas, procedimientos, mecanismos técnicos o prácticas organizacionales orientadas a reducir la probabilidad de un incidente o su impacto (ISO/IEC 27002, 2022). Los controles pueden ser preventivos, como la autenticación robusta que evita accesos indebidos; detectivos, como el monitoreo que alerta sobre actividad anormal; o correctivos, como los respaldos que permiten recuperar la información tras un incidente. El diagnóstico de la empresa muestra carencias en los tres frentes: faltan controles preventivos (credenciales compartidas, sistemas sin actualizar), detectivos (incidentes que no se reportan a tiempo) y correctivos (respaldos que nunca se han probado).

Finalmente, en una organización industrial conviene distinguir entre la tecnología de la información (IT), que comprende los sistemas administrativos como el ERP o el correo corporativo, y la tecnología de operación (OT), que agrupa los sistemas que controlan procesos físicos de producción, como el MES y las redes industriales. La seguridad OT tiene exigencias particulares, pues los equipos industriales suelen operar por años sin actualizarse y una falla compromete la operación física de la planta (ISA/IEC 62443, 2018). Esta distinción será cada vez más relevante para la empresa, que planea incorporar líneas automatizadas y sensores IoT.

Conceptos fundamentales de ciberseguridad

Un concepto que conviene precisar desde ya es el de Sistema de Gestión de Seguridad de la Información (SGSI): el marco de políticas, procesos y recursos que una organización adopta para gestionar la seguridad de forma sistemática y no reactiva (ISO/IEC 27001:2022, s.f.). El SGSI se apoya en un ciclo de mejora continua, conocido como Planificar-Hacer-Verificar-Actuar, que obliga a revisar periódicamente los riesgos y ajustar los controles según los resultados obtenidos. Este es, en últimas, el marco que propone este informe para Industrias Metalmecánicas del Valle S.A.S., que hoy gestiona la seguridad de forma dispersa, sin un responsable claro ni una revisión periódica de sus controles.

En el diseño de los controles suelen aplicarse dos principios complementarios. El de defensa en profundidad plantea que ningún control es infalible por sí solo, por lo que conviene disponer varias capas de protección, red, sistema, aplicación y usuario, de modo que la falla de una no deje expuesto el activo por completo (NIST, 2024). El de mínimo privilegio establece que cada usuario o proceso debe contar solo con los permisos estrictamente necesarios para su función, ni uno más (ISO/IEC 27005, 2022). Ambos principios están ausentes en la situación actual de la empresa: las credenciales compartidas identificadas en el diagnóstico contradicen directamente el mínimo privilegio, y la dependencia de un único control de acceso perimetral, sin capas adicionales, contradice la defensa en profundidad.

También es necesario diferenciar entre evento e incidente de seguridad. Un evento es cualquier ocurrencia identificada en un sistema que indica una posible violación de la seguridad, mientras que un incidente es un evento, o una serie de ellos, que efectivamente compromete la confidencialidad, la integridad o la disponibilidad de un activo (ISO/IEC 27035-1, 2023). La empresa ha tenido varios incidentes en los últimos tres años que no se reportaron a tiempo, en parte porque no distingue con claridad ambas categorías ni cuenta con un procedimiento para escalarlos. Ligado a esto está el concepto de continuidad del negocio, entendida como la capacidad de la organización para seguir operando, o para recuperarse en un tiempo aceptable, ante un incidente que interrumpa sus procesos críticos (ISO 22301, 2019). La interrupción de la línea de fabricación registrada en el diagnóstico es un ejemplo directo de lo que este concepto busca prevenir.

Por último, la seguridad no depende solo de la tecnología. La cultura de seguridad se refiere al conjunto de conocimientos, actitudes y comportamientos que las personas de una organización tienen frente al manejo de la información (MinTIC, 2021). Las personas pueden ser tanto la vulnerabilidad más explotada, cuando desconocen los riesgos o no siguen los procedimientos, como el control más efectivo, cuando identifican y reportan a tiempo una situación anómala. El diagnóstico de Industrias Metalmecánicas del Valle S.A.S. confirma esta doble condición: la mayoría de los problemas de fondo encontrados, desde las credenciales compartidas hasta los incidentes no reportados, tienen origen en prácticas del personal más que en fallas puramente técnicas.

Marco normativo

El fortalecimiento de la seguridad en una organización requiere apoyarse en estándares y normas que definan lineamientos para proteger la información y gestionar los riesgos. En el caso de Industrias Metalmecánicas del Valle S.A.S. esto es especialmente necesario por la naturaleza industrial de sus procesos y por la alta dependencia tecnológica identificada durante el diagnóstico. Las normas que se relacionan a continuación constituyen el referente frente al cual se evaluaron las prácticas de la organización.

Tabla 1. Normatividad aplicable.

Norma o estándar	Propósito	Aplicabilidad en la organización
ISO/IEC 27001:2022	Define los requisitos para implementar y mejorar un sistema de gestión de seguridad de la información (SGSI).	Marco para formalizar la gestión de seguridad que la empresa no tiene: políticas, inventario de activos, responsabilidades y gestión de incidentes.
ISO/IEC 27002:2022	Proporciona un catálogo de buenas prácticas y	Orienta la implementación de controles para las debilidades detectadas: gestión de accesos,

	controles de seguridad de la información.	respaldos, incidentes y protección de activos.
ISO/IEC 27005:2022	Orienta la gestión de riesgos de seguridad de la información.	Metodología para identificar, valorar y tratar los riesgos del diagnóstico, como los derivados de credenciales compartidas.
NIST Cybersecurity Framework 2.0	Marco para identificar, proteger, detectar, responder y recuperarse frente a incidentes de ciberseguridad.	Guía práctica para fortalecer la capacidad de respuesta, hoy inexistente: la empresa carece de procedimiento documentado de incidentes.
Ley 1581 de 2012	Régimen colombiano de protección de datos personales.	La empresa trata datos de 420 colaboradores, clientes y proveedores, y el sistema biométrico capta datos sensibles de especial protección.
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 en materia de tratamiento de datos.	Define las condiciones de autorización, políticas de tratamiento y manejo de los datos personales que la organización recolecta.
Ley 1273 de 2009	Tipifica los delitos informáticos en Colombia.	Da soporte legal frente a incidentes ya sufridos, como el acceso no autorizado a información técnica y los intentos de intrusión tras el phishing.
Modelo de Seguridad y Privacidad de la Información (MSPI), MinTIC	Orienta la implementación de la seguridad de la información en organizaciones colombianas.	Ofrece un ciclo de operación e instrumentos aplicables al contexto nacional para estructurar la gestión de seguridad de la empresa.
ISA/IEC 62443	Serie de estándares de ciberseguridad para sistemas	Aplica a los entornos OT de la planta: MES, redes industriales y

	de automatización y control industrial.	los sensores IoT que se proyecta implementar.

La selección responde a las necesidades concretas del caso. La ISO/IEC 27001 es la más importante para la organización porque ataca la raíz de su problemática: el diagnóstico no reveló fallas tecnológicas aisladas sino la ausencia de una gestión formal de la seguridad, que es lo que un SGSI estructura (ISO/IEC 27001:2022, s.f.). La ISO/IEC 27002 la complementa en la práctica, pues ofrece el catálogo de controles con el que se pueden cerrar las debilidades encontradas, desde la gestión de accesos hasta los respaldos (ISO/IEC 27005, 2022). La ISO/IEC 27005 aporta el método para gestionar los riesgos, dando continuidad al ejercicio de identificación de activos, amenazas y vulnerabilidades de este informe, y el marco NIST CSF 2.0 suma una guía operativa para desarrollar las capacidades de detección y respuesta que la empresa hoy no tiene (NIST, 2024).

En el plano legal colombiano, la Ley 1581 de 2012 expone a la empresa a sanciones de la Superintendencia de Industria y Comercio si no protege adecuadamente los datos personales que trata, y su decreto reglamentario 1377 de 2013 precisa las obligaciones prácticas: autorizaciones, políticas de tratamiento y atención de consultas y reclamos. La Ley 1273 de 2009 le permite denunciar penalmente los accesos no autorizados que ya sufrió, a la vez que la obliga a demostrar diligencia en la protección de su información. Como referente nacional, el Modelo de Seguridad y Privacidad de la Información del MinTIC ofrece un ciclo de operación e instrumentos alineados con el contexto colombiano, útiles como hoja de ruta de implementación (MinTIC, 2021). Por último, la serie ISA/IEC 62443 cobra relevancia por el carácter industrial del negocio: las normas de gestión tradicionales se quedan cortas frente a redes de planta y equipos que no pueden actualizarse con la frecuencia de un computador de oficina, un frente que crecerá con las líneas automatizadas y los sensores IoT proyectados.

Marco contextual

Descripción de la organización

Industrias Metalmecánicas del Valle S.A.S. es una empresa colombiana con más de 25 años de trayectoria, dedicada al diseño, la fabricación y la comercialización de componentes metálicos para los sectores automotriz, agrícola e industrial, con clientes tanto nacionales como internacionales. Opera desde una planta principal de producción y dos centros de distribución regionales, y produce mensualmente más de 150.000 piezas industriales. La planta emplea a cerca de 420 personas entre operarios, supervisores, ingenieros, personal administrativo, logística y directivos, distribuidas en doce áreas, entre ellas Producción, Ingeniería y Diseño, Planeación Industrial, Tecnología y Sistemas, Calidad, Compras, Logística, Talento Humano, Finanzas, Seguridad y Salud en el Trabajo, y Mantenimiento Industrial.

La operación se sostiene sobre seis procesos que dependen entre sí de forma directa: planeación de producción, producción industrial, gestión de inventarios, diseño e ingeniería, logística y distribución, y gestión financiera. Un retraso en la planeación repercute de inmediato en inventarios, y un cambio de última hora en un diseño se traslada directamente a la línea de fabricación.

Esa dependencia se apoya en una infraestructura considerable: 180 computadores de escritorio, 75 portátiles y 15 servidores virtualizados, sobre los que corren el ERP, el sistema MES, el sistema de gestión de inventarios, el sistema de diseño asistido por computador (CAD), un sistema de gestión documental y el correo corporativo. A esto se suman una plataforma de respaldo, un sistema biométrico de acceso, redes WiFi-corporativas y redes industriales dedicadas a producción, equipos de monitoreo industrial, y una infraestructura híbrida que combina servidores locales con servicios en la nube. Toda esa plataforma la administra un equipo de diez personas: un director de TI, tres administradores de infraestructura, dos desarrolladores y cuatro analistas de soporte, un equipo reducido si se compara con el tamaño de la infraestructura que debe sostener.

La empresa además atraviesa un momento de expansión: en los próximos dos años planea incorporar líneas de producción automatizadas y sensores IoT para el monitoreo de maquinaria, y ya manifiesta interés en fortalecer su analítica de datos. Ese crecimiento va a sumar más dispositivos conectados a la red industrial, justo en un momento en que, como se describe a continuación, la gestión de la seguridad todavía no está a la altura de la dependencia tecnológica que ya tiene la organización.

Problemática identificada

Una firma consultora realizó una evaluación inicial de la organización y encontró doce situaciones que, agrupadas, señalan hacia los mismos puntos débiles. En la gestión de accesos, halló que varios supervisores comparten credenciales para ingresar a los sistemas de producción, que existen usuarios con privilegios elevados que ya no cumplen funciones relacionadas con producción, y que no todos los dispositivos de planta cuentan con mecanismos de autenticación robusta; a esto se suma que algunos equipos industriales siguen operando con sistemas sin actualizaciones recientes, una condición habitual en entornos OT pero que aquí no está compensada con ningún control adicional. En el control de la información corporativa, la evaluación no encontró una política formal de clasificación, detectó archivos de diseño industrial guardados en dispositivos externos personales, y confirmó que varios colaboradores usan aplicaciones de mensajería personal para compartir documentos técnicos. En la gestión de incidentes, no existe un procedimiento documentado, los respaldos se hacen con regularidad pero nunca se ha probado si realmente permiten restaurar la información, y las prácticas de seguridad varían de un área a otra sin que haya un criterio común. Tampoco existe un inventario actualizado de activos de información, lo que explica por qué la primera tarea de este informe fue precisamente reconstruirlo.

Estas debilidades ya se han traducido en incidentes concretos. En los últimos tres años la empresa registró cinco: una falla de configuración interrumpió una línea de fabricación durante varias horas y generó retrasos y sobrecostos; un colaborador recibió un correo fraudulento que simulaba venir de un proveedor estratégico de materias primas, seguido de intentos de acceso no autorizado a los sistemas internos; un portátil de ingeniería con planos y diseños de productos en desarrollo se extravió durante una visita técnica a un cliente; una actualización de software mal aplicada desincronizó temporalmente el ERP con el sistema de inventarios; y se detectó un acceso no autorizado a información técnica mediante credenciales compartidas entre colaboradores, el mismo problema que ya se había señalado como debilidad estructural.

Las entrevistas con colaboradores y directivos muestran por qué estas situaciones se repiten. Buena parte del personal considera que la seguridad informática es un asunto exclusivo del área de tecnología, y varias áreas priorizan el cumplimiento de metas de producción por encima de los controles de seguridad. Hay resistencia a modificar procedimientos que llevan años en uso, desconocimiento de los riesgos asociados a la información técnica e industrial, capacitaciones esporádicas que no llegan a todo el personal, y una confianza excesiva en prácticas informales para compartir información, lo que explica que no todos los incidentes se reporten a tiempo. La alta dirección, por su parte, reconoce que el crecimiento tecnológico de la empresa ha sido más rápido que la actualización de sus políticas y procedimientos de seguridad, y que no existe todavía una estrategia formal de gobierno de datos, un vacío que se va a sentir más conforme avancen los planes de automatización y de sensores IoT.

En conjunto, estas situaciones apuntan a cuatro problemas de fondo que atraviesan el resto del informe: debilidades en la gestión de accesos, falta de control sobre la información corporativa, ausencia de procedimientos formales para la gestión de incidentes, y una cultura organizacional que delega la seguridad por completo en el área de tecnología. Sobre esa base se construyen el inventario de activos, el análisis de amenazas y vulnerabilidades, y las políticas y controles que se proponen más adelante.

Identificación y análisis de activos

Identificar los activos es el punto de partida de la gestión de riesgos: antes de proteger algo hay que saber qué se tiene y cuánto vale para la operación. La ISO/IEC 27005 entiende por activo de información todo elemento que soporta los procesos de la organización y cuya afectación puede traducirse en pérdidas operativas, económicas, legales o de reputación (ISA/IEC 62443, 2018).

En Industrias Metalmecánicas del Valle S.A.S. esta tarea pesa más que en otras empresas por su nivel de dependencia tecnológica. El diagnóstico mostró que la protección no puede limitarse a la infraestructura informática de oficina; también están en juego los sistemas industriales, la información técnica y las plataformas que sostienen la producción. Buena parte de la operación descansa sobre el ERP, el MES, las redes industriales y las herramientas de diseño asistido, que coordinan desde la fabricación y los inventarios hasta la logística y la administración corporativa.

Por eso la identificación abarcó elementos tecnológicos, de información y operativos ligados al funcionamiento de la empresa. Para asignar la criticidad de cada activo se evaluó su impacto en la operación, qué tanto depende de él la organización, la sensibilidad de la información que maneja, su papel en la continuidad de los procesos y las consecuencias que tendría un incidente sobre él.

Para la identificación se revisó la infraestructura tecnológica de la compañía y los procesos principales que soporta: planeación de producción, producción industrial, gestión de inventarios, diseño e ingeniería, logística y gestión financiera. A partir de esa revisión se seleccionaron los activos más importantes para la operación, es decir, aquellos cuya afectación

tendría un impacto directo sobre la producción, las finanzas o la información sensible de la empresa.

Los activos se clasificaron en tres categorías. Los activos físicos corresponden a la infraestructura y los elementos tangibles, como servidores, equipos de cómputo y redes. Los activos digitales agrupan la información, los sistemas y los servicios tecnológicos, como el ERP, el MES o los planos de producto. Los activos humanos son las personas que participan en esos procesos de la organización. Esta clasificación facilita el análisis, porque cada tipo de activo enfrenta riesgos diferentes y requiere de medidas de protección distintas: un servidor puede fallar o ser dañado físicamente, un sistema puede ser atacado o quedar indisponible, y una persona puede ser víctima de engaño o cometer errores.

Inventario de activos

El resultado de la identificación se presenta en la siguiente tabla.

Tabla 2. Inventario de activos.

Activo	Tipo	Descripción	Criticidad
Sistema ERP empresarial	Digital	Integra los procesos administrativos, financieros y de abastecimiento.	Alta
Sistema MES	Digital	Controla la ejecución de la manufactura en las líneas de producción.	Alta
Planos y diseños de producto	Digital	Información técnica de Ingeniería; propiedad intelectual de la empresa.	Alta
Servidores virtualizados (15)	Físico	Soportan los sistemas centrales y los servicios de red.	Alta
Sistema de gestión de inventarios	Digital	Controla materias primas, producto en proceso y terminado.	Alta

Redes industriales de producción	Físico	Comunican la maquinaria y los equipos de monitoreo de planta.	Alta
Plataforma de respaldo de información	Digital	Almacena las copias de seguridad; único mecanismo de recuperación.	Alta
Personal de la organización	Humano	Los 420 colaboradores que operan los sistemas y manejan la información.	Alta
Equipos de cómputo (180 de escritorio y 75 portátiles)	Físico	Herramienta de trabajo del personal; los portátiles salen de las sedes con información técnica.	Media
Correo electrónico corporativo	Digital	Canal oficial de comunicación interna y externa.	Media
Sistema de gestión documental	Digital	Almacena la documentación administrativa y técnica.	Media
Sistema CAD	Digital	Aplicación con la que Ingeniería desarrolla los planos.	Media
Sistema biométrico de acceso	Físico	Controla el ingreso físico a instalaciones y áreas restringidas.	Media
Redes WiFi corporativas	Físico	Conectividad inalámbrica en las sedes.	Media
Infraestructura en la nube	Digital	Aloja parte de los servicios dentro del esquema híbrido.	Media

Justificación de los activos críticos

La criticidad se asignó según el impacto que tendría sobre la operación la pérdida de confidencialidad, integridad o disponibilidad de cada activo. Se valoraron con criticidad alta los sistemas de los que depende directamente la producción y la administración del negocio, como el ERP, el MES, el sistema de inventarios y las redes industriales: una interrupción en cualquiera de ellos detendría o distorsionaría la fabricación, tal como ocurrió con la falla de configuración que paralizó una línea de producción durante varias horas generando retrasos en la entrega de pedidos y costos operativos adicionales. Los planos y diseños de producto se valoraron como críticos por tratarse de la propiedad intelectual de la compañía, cuya filtración sería irreversible; la pérdida del portátil de ingeniera con diseños en desarrollo demostró que este activo ya estuvo expuesto. La plataforma de respaldos recibió la misma valoración por ser el único mecanismo de recuperación de información, agravado por el hecho de que no se realizan pruebas de restauración. El personal se consideró un activo crítico porque los incidentes registrados, en particular el correo fraudulento que derivó en intentos de acceso no autorizado, muestran que el factor humano es el punto de entrada más explotado por los atacantes.

Los activos de criticidad media apoyan la operación diaria y el flujo de información, pero su afectación no detiene los procesos productivos de manera inmediata.

Análisis de amenazas y vulnerabilidades

La identificación de amenazas y vulnerabilidades constituye una etapa fundamental dentro del proceso de gestión de riesgos de seguridad de la información, ya que permite comprender cómo determinados eventos pueden afectar los activos críticos de una organización. Una amenaza representa cualquier circunstancia con capacidad de causar un incidente que comprometa la confidencialidad, integridad o disponibilidad de la información, mientras que una vulnerabilidad corresponde a una debilidad que puede ser explotada por dicha amenaza (ISA/IEC 62443, 2018).

En Industrias Metalmecánicas del Valle S.A.S. se evidencian múltiples vulnerabilidades que incrementan la exposición de la organización frente a incidentes de ciberseguridad. El diagnóstico inicial revela deficiencias relacionadas con la gestión de identidades, el control de accesos, la protección de la información técnica, la actualización de sistemas industriales y la ausencia de procedimientos formales para responder a incidentes de seguridad. Estas condiciones, sumadas al crecimiento tecnológico de la empresa y a la futura incorporación de

soluciones IoT para la automatización de procesos industriales, incrementan considerablemente la superficie de ataque de la organización.

Con el propósito de identificar los principales escenarios de riesgo, se relacionan los activos críticos previamente identificados con las amenazas más probables y las vulnerabilidades observadas durante el estudio del caso.

-

Tabla 3. Amenazas y vulnerabilidades.

Activo	Amenaza	Vulnerabilidad
Sistema MES	Acceso no autorizado	Credenciales compartidas entre supervisores.
Planos y diseños de producto	Fuga de propiedad intelectual	Información en portátiles y dispositivos personales sin control.
Personal de la organización	Ingeniería social (phishing)	Capacitación esporádica y baja conciencia en seguridad.
Sistema ERP	Pérdida de integridad de la información	Actualizaciones sin gestión de cambios ni pruebas previas.
Líneas de producción	Interrupción de la operación	Configuraciones sin procedimientos de control.
Equipos y sistemas industriales	Explotación de fallas conocidas y malware	Sistemas sin actualizaciones recientes.

Sistemas internos	Abuso de privilegios	Usuarios con permisos elevados que ya no los requieren.
Plataforma de respaldos	Imposibilidad de recuperar información	Copias sin pruebas periódicas de restauración.
Información técnica y documental	Fuga de información	Uso de mensajería personal y dispositivos externos.
Redes industriales	Acceso no autorizado a la red de planta	Autenticación débil en dispositivos de producción.
Correo electrónico corporativo	Phishing e ingeniería social	Escasa capacitación y concienciación del personal.
Servidores virtualizados	Ataques de ransomware	Actualizaciones insuficientes y concentración de servicios críticos.
Equipos portátiles de ingeniería	Robo o pérdida de equipos	Uso fuera de las sedes sin controles adicionales de seguridad.
Infraestructura híbrida (local y nube)	Acceso indebido o configuraciones inseguras	Crecimiento tecnológico sin actualización de políticas y controles.
Sistema de gestión de inventarios	Alteración o indisponibilidad de la información	Dependencia de la sincronización con el ERP.
Sistema de gestión documental	Alteración o pérdida de documentos	Ausencia de política de clasificación de la información.

A partir de la tabla, el análisis permite establecer cuáles son las situaciones que representan mayor riesgo para la organización.

La situación más grave es la combinación de credenciales compartidas con acceso a los sistemas de producción. No se trata de una debilidad teórica: la empresa ya registró un acceso no autorizado a información técnica usando cuentas compartidas. Mientras varias personas usen la misma credencial, es imposible saber quién hizo qué en los sistemas, y ningún otro control funciona bien sobre esa base. Además, afecta al activo del que depende directamente la fabricación.

El segundo riesgo en importancia es la exposición de los planos y diseños de producto. Son la propiedad intelectual de la compañía y hoy circulan en portátiles que salen de las sedes, en dispositivos externos personales y por aplicaciones de mensajería. El extravío del portátil de ingeniería con diseños en desarrollo demostró que la fuga no es una posibilidad remota sino algo que ya ocurrió. A diferencia de una interrupción operativa, que se supera con horas o días de trabajo, la filtración de un diseño a un competidor es irreversible.

El tercer riesgo crítico es el factor humano frente a la ingeniería social. El correo fraudulento que simulaba a un proveedor estratégico, seguido de intentos de acceso a los sistemas internos, muestra que los atacantes ya identificaron a la empresa como objetivo y que apuestan por engañar a las personas antes que por vulnerar la tecnología. Con capacitaciones esporádicas que no llegan a todo el personal, la probabilidad de que un intento futuro tenga éxito es alta.

Un cuarto riesgo suele pasar desapercibido porque no ha generado incidentes visibles: los respaldos sin pruebas de restauración. Si un evento grave, como un ransomware o una falla mayor, comprometiera la información, la empresa descubriría en el peor momento si sus copias sirven o no. Un respaldo que nunca se ha probado es una promesa, no una garantía.

Las demás situaciones de la tabla también requieren atención, pero estas cuatro concentran la mayor combinación de probabilidad e impacto: afectan los activos más críticos, tres de ellas ya se materializaron y la restante compromete la capacidad de recuperación de todo lo demás. A esto se suma que los planes de incorporar líneas automatizadas y sensores IoT conectarán más equipos a redes que hoy operan con autenticación débil, ampliando la superficie de ataque antes de corregir las debilidades existentes.

Análisis y gestión de riesgos

Metodología de análisis

El análisis de riesgos desarrollado para Industrias Metalmecánicas del Valle S.A.S. se realizó mediante una metodología de análisis cualitativo, tomando como referencia la norma ISO/IEC 27005 sobre gestión de riesgos de seguridad de la información (ISO/IEC 27005, 2022). El procedimiento consistió en tomar cada activo, establecer qué amenazas podrían afectarlo y a través de qué debilidades, y calificar después la gravedad y la posibilidad de cada escenario.

El punto de partida fueron los activos ya levantados en el inventario: sistemas de información, infraestructura tecnológica, redes, información crítica y los servicios que sostienen la administración y la producción. A cada activo se le asociaron las amenazas con mayor posibilidad de ocurrencia y las vulnerabilidades que podrían facilitarlas. De ese cruce resultaron

escenarios de riesgo concretos, sustentados en lo que muestra el caso y no en situaciones genéricas.

La calificación empleó dos criterios. El primero es el impacto: las consecuencias que tendría la materialización del riesgo, evaluadas según la afectación de la operación de planta, la disponibilidad de los servicios, la integridad y confidencialidad de la información, y los costos económicos, legales o de reputación derivados. El segundo es la probabilidad: la posibilidad de que la amenaza aproveche la vulnerabilidad, estimada a partir del estado actual de la infraestructura, las prácticas de trabajo observadas y los antecedentes de la organización. Este último criterio tuvo un peso particular en el análisis, pues varios de los riesgos valorados ya se materializaron en los últimos tres años; su probabilidad no se estimó por suposición sino con hechos registrados.

Ambos criterios se midieron en tres niveles: alto, medio y bajo. El nivel de riesgo resulta de cruzarlos. Cuando el impacto es alto y la probabilidad alta o media, el riesgo queda en nivel alto y exige atención prioritaria. Las combinaciones intermedias producen nivel medio y requieren mejoras. Las combinaciones bajas solo demandan seguimiento. Esta forma de priorizar corresponde al propósito de un sistema de gestión de seguridad, que no busca eliminar todos los riesgos sino tratarlos según su importancia para el negocio (ISO/IEC 27001:2022, s.f.).

La elección del método cualitativo obedece al alcance del estudio. La empresa no dispone de estadísticas históricas suficientes para calcular frecuencias, pero el diagnóstico y los incidentes registrados permiten estimar la exposición con criterio técnico. Esta manera de valorar, apoyada en el contexto y los antecedentes de cada organización, es la misma que orienta el modelo colombiano de gestión de seguridad (MinTIC, 2021).

El método conserva además la trazabilidad del informe. Cada riesgo de la matriz proviene de un activo del inventario, de una amenaza y de una vulnerabilidad documentadas en las tablas anteriores, de manera que toda valoración puede rastrearse de principio a fin. Con la matriz construida, la organización cuenta con una guía para decidir qué controles implementar primero, reducir la posibilidad de los incidentes y disminuir su impacto sobre los activos críticos.

Criterios de valoración

Tabla 4. Criterios para la valoración de riesgos.

Criterio	***Alto***	***Medio***	***Bajo***
Impacto	La materialización del riesgo puede generar interrupción de procesos críticos, pérdida significativa de información, afectaciones económicas importantes o incumplimiento legal.	El riesgo ocasiona afectaciones moderadas en la operación, con posibilidad de recuperación en un tiempo razonable.	El riesgo produce consecuencias menores, con impacto limitado sobre la operación y fácil recuperación.
Probabilidad	Existen antecedentes o condiciones que hacen muy probable la ocurrencia del riesgo.	El riesgo puede presentarse bajo determinadas condiciones, aunque no ocurre con frecuencia.	Es poco probable que el riesgo se materialice debido a la existencia de controles o a la baja exposición.

Nivel de riesgo	Requiere atención prioritaria e implementación inmediata de controles.	Requiere seguimiento y aplicación de medidas de mitigación.	Puede aceptarse temporalmente, manteniendo monitoreo y controles existentes.

Matriz de riesgos

Tabla 5. Matriz de riesgos.

Activo	*Amenaza*	*Vulnerabilidad*	*Impacto*	*Probabilidad*	*Nivel*
Sistema MES	Acceso no autorizado	Uso compartido de credenciales entre supervisores.	Alto	Alto	Alto
Diseños industriales CAD	Robo o fuga de información	Almacenamiento de archivos en dispositivos personales y pérdida de equipos portátiles.	Alto	Alto	Alto
Correo electrónico corporativo	Phishing e ingeniería social	Escasa capacitación y concienciación del personal.	Alto	Alto	Alto
Líneas de producción	Interrupción del	Sistemas industriales desactualizados	Alto	Medio	Alto

	proceso productivo	y configuraciones sin procedimientos de control.			
Redes industriales de producción	Ataques de malware o acceso no autorizado	Autenticación débil en dispositivos de planta y equipos sin actualizaciones recientes.	Alto	Medio	Alto
Servidores virtualizados	Ataques de ransomware	Actualizaciones insuficientes y concentración de servicios críticos.	Alto	Medio	Alto
Sistema de gestión de inventarios	Alteración o indisponibilidad de la información	Dependencia de la sincronización con el ERP.	Alto	Medio	Alto
Plataforma de respaldo de información	Pérdida permanente de información	No se realizan pruebas periódicas de restauración de respaldos.	Alto	Medio	Alto
Equipos portátiles de ingeniería	Robo o pérdida de información	Uso de equipos fuera de las instalaciones sin controles adicionales de seguridad.	Alto	Medio	Alto
Infraestructura híbrida (local y nube)	Acceso indebido o configuraciones inseguras	Crecimiento tecnológico sin actualización de políticas y controles de seguridad.	Alto	Medio	Alto

Sistema ERP empresarial	Pérdida de integridad de la información	Actualizaciones sin gestión de cambios ni pruebas previas.	Medio	Medio	Medio
Sistemas internos	Abuso de privilegios	Usuarios con permisos elevados que ya no los requieren.	Medio	Medio	Medio
Sistema de gestión documental	Alteración o pérdida de documentos	Ausencia de política de clasificación de la información.	Medio	Medio	Medio

La calificación alta de varios escenarios no responde a una apreciación general sobre el estado de la empresa, sino a dos condiciones que el diagnóstico permitió verificar. El impacto se calificó como alto cuando la afectación del activo detiene o compromete de forma directa un proceso productivo o administrativo esencial, según los criterios definidos en la Tabla 4. La probabilidad se calificó como alta cuando la vulnerabilidad asociada permanece sin ningún control que la mitigue y, además, cuando el escenario ya se materializó al menos una vez en los últimos tres años. Tres de los cuatro riesgos con mayor valoración cumplen las dos condiciones. El acceso indebido al sistema MES mediante credenciales compartidas, la fuga de diseños almacenados en dispositivos personales y el phishing dirigido al correo corporativo cuentan con antecedente documentado entre los incidentes que la empresa registró, de modo que su probabilidad no proviene de una estimación técnica sino de un hecho que puede repetirse mientras la causa siga vigente.

La valoración muestra una exposición considerable: la mayoría de los riesgos quedó en nivel alto. Dos factores explican ese resultado. La operación administrativa y productiva depende casi por completo de los sistemas tecnológicos, y buena parte de las vulnerabilidades encontradas todavía no tiene controles que reduzcan su probabilidad de ocurrencia.

Los riesgos que exigen prioridad recaen sobre el sistema MES, los diseños industriales elaborados en CAD, el correo corporativo, las redes industriales, los servidores virtualizados, la infraestructura híbrida y la plataforma de respaldos. Son los activos que sostienen los procesos esenciales de la empresa, de modo que un incidente contra su disponibilidad, su integridad o su confidencialidad se traduce en afectación directa de la operación.

El acceso no autorizado al sistema MES encabeza la matriz. Los supervisores comparten credenciales para ingresar a los sistemas de producción, y con esas cuentas ya se registró un acceso indebido a información técnica. Mientras varias personas usen la misma credencial es imposible rastrear quién hizo qué, y el activo comprometido es justamente el que controla la fabricación: una manipulación o una interrupción del MES detiene las líneas y compromete el cumplimiento de los pedidos. La probabilidad se calificó como alta porque la práctica sigue

vigente y el antecedente ya existe; el impacto, porque ningún otro control de la matriz funciona sobre una base sin trazabilidad.

Los diseños industriales son quizá el activo más sensible. Contienen la información técnica y la propiedad intelectual de los productos que la empresa fabrica. Hoy esos archivos se guardan también en dispositivos personales, y ya hubo un portátil extraviado con diseños en desarrollo, antecedente que eleva la probabilidad de fuga. El riesgo quedó en nivel alto por lo que una filtración significaría para la competitividad y la confidencialidad de la información estratégica. A diferencia de otros activos, aquí el daño no se revierte: una vez el diseño sale de la organización no hay control que lo recupere.

El correo corporativo también quedó entre las prioridades. Es el principal medio de comunicación de la organización y, a la vez, la puerta de entrada más usada por la ingeniería social y el phishing. Sin programas permanentes de sensibilización, la probabilidad de que un colaborador caiga en un engaño es alta, y un solo engaño exitoso puede comprometer credenciales, información confidencial y otros sistemas conectados. El intento de suplantación de un proveedor estratégico, seguido de accesos no autorizados, demostró que la empresa ya está en la mira.

Las redes industriales, los servidores virtualizados y la infraestructura híbrida comparten el nivel alto por su papel de soporte de toda la operación. El diagnóstico registró dispositivos de planta con autenticación débil, equipos sin actualizaciones recientes y un crecimiento tecnológico que no vino acompañado de políticas ni controles equivalentes. En esas condiciones la superficie de ataque crece, y una amenaza como el ransomware encontraría servicios críticos concentrados y puertas mal cerradas, con la continuidad de la producción en juego.

La plataforma de respaldos merece un párrafo aparte. Es el activo del que depende la recuperación de la información después de un incidente. La empresa realiza copias con regularidad, pero nunca las ha puesto a prueba, así que no hay forma de saber si funcionarían. Frente a un ransomware, una falla tecnológica o un error humano, esa incertidumbre puede convertirse en pérdida definitiva de información crítica.

Este es el único riesgo de nivel alto sin incidente previo, y su valoración se sostiene por razones distintas. La probabilidad se calificó como alta porque las copias nunca se han sometido a pruebas de restauración, de manera que una falla en el procedimiento no se detectaría antes del evento sino durante él, cuando ya no hay margen de corrección. El impacto se calificó como alto porque este activo opera como última medida de recuperación de la organización: si el respaldo falla, el daño ocasionado por cualquier otro incidente deja de ser reversible. Esa condición explica que un riesgo sin antecedentes quede en el mismo nivel que los anteriores.

En contraste, la pérdida de integridad del ERP por actualizaciones sin control de cambios, el abuso de privilegios en los sistemas internos y el sistema de gestión documental quedaron en nivel medio. Su afectación no detendría de inmediato los procesos productivos, aunque tampoco son riesgos menores: la desincronización entre el ERP y el sistema de inventarios ya ocurrió una vez, y los usuarios con permisos que no corresponden a sus funciones siguen activos. Su tratamiento puede darse de forma progresiva, una vez estén cubiertos los riesgos prioritarios.

En conjunto, la matriz señala hacia dónde dirigir los esfuerzos: control de accesos y gestión de identidades y privilegios, protección de la propiedad intelectual, actualización de la infraestructura, aseguramiento de los dispositivos de planta y una cultura de ciberseguridad más sólida. Avanzar en esos frentes reduce a la vez la probabilidad de los incidentes y su impacto, y mejora la capacidad de la empresa para proteger sus activos críticos y sostener la operación.

Políticas y controles de seguridad

La gestión de riesgos realizada para Industrias Metalmecánicas del Valle S.A.S. dejó a la vista debilidades que afectan la seguridad de la información y la continuidad de las operaciones: credenciales compartidas entre supervisores, ausencia de una política de clasificación de la información, documentación técnica almacenada en dispositivos personales, sistemas industriales sin actualizar y falta de un procedimiento formal para atender incidentes.

Frente a ese panorama, el paso siguiente del informe es proponer políticas y controles. Las políticas de seguridad son el fundamento de un sistema de gestión de seguridad de la información, pues definen los lineamientos que orientan el comportamiento del personal y la protección de los activos frente a amenazas internas y externas (ISO/IEC 27001:2022, s.f.). Los controles, por su parte, son las medidas concretas de tipo administrativo, físico y tecnológico con las que esos lineamientos se llevan a la práctica y se reducen los riesgos ya valorados (ISO/IEC 27005, 2022).

Las políticas y controles que se presentan a continuación responden directamente a los riesgos de la matriz: cada propuesta ataca una debilidad documentada en el diagnóstico.

Tabla 6. Políticas de seguridad.

Política	***Objetivo***	***Riesgo asociado***
Política de Control de Accesos	Garantizar que únicamente los usuarios autorizados puedan acceder a los sistemas corporativos según sus funciones.	Accesos no autorizados y uso indebido de privilegios.

Política de Gestión de Contraseñas	Establecer criterios para la creación, uso y actualización segura de credenciales.	Robo o compromiso de cuentas de usuario.
Política de Clasificación de la Información	Definir niveles de clasificación y tratamiento de la información institucional.	Fuga o divulgación de información confidencial.
Política de Uso Aceptable de Recursos Tecnológicos	Regular el uso adecuado de equipos, redes, correo electrónico y dispositivos corporativos.	Uso indebido de recursos tecnológicos y propagación de amenazas.
Política de Gestión de Respaldos	Garantizar la disponibilidad y recuperación de la información institucional.	Pérdida permanente de información crítica.

Política de Gestión de Vulnerabilidades	Establecer procedimientos para mantener actualizados los activos tecnológicos.	Explotación de vulnerabilidades conocidas.
Política de Respuesta a Incidentes	Definir el procedimiento institucional para gestionar incidentes de seguridad.	Respuesta tardía o inadecuada frente a incidentes.
Política de Capacitación en Ciberseguridad	Fortalecer la cultura organizacional mediante programas permanentes de formación.	Errores humanos, phishing e ingeniería social.
Política de Seguridad para Dispositivos Móviles	Regular el uso de portátiles y dispositivos utilizados fuera de la organización.	Robo o pérdida de información corporativa.

Política de Continuidad del Negocio	Garantizar la continuidad de los procesos críticos ante eventos que afecten la operación.	Interrupción prolongada de los servicios organizacionales.

Políticas propuestas

Política de Control de Accesos

Objetivo

Garantizar que únicamente los usuarios autorizados puedan acceder a los recursos tecnológicos de la organización, de acuerdo con las funciones y responsabilidades asignadas a cada cargo.

Alcance

Aplica a todos los colaboradores, contratistas, proveedores y terceros que tengan acceso a los sistemas de información, redes corporativas, plataformas industriales y servicios tecnológicos de Industrias Metalmecánicas del Valle S.A.S.

Lineamientos principales:

- Cada usuario deberá disponer de una cuenta individual e intransferible.
- Se prohíbe compartir usuarios y contraseñas.
- Los permisos se asignarán bajo el principio de mínimo privilegio.
- Todo acceso deberá ser aprobado por el responsable del proceso.
- Los privilegios serán revisados periódicamente y eliminados cuando ya no sean necesarios.
- Los sistemas críticos deberán utilizar autenticación multifactor (MFA).

Responsables:

- Dirección de Tecnología.
- Responsable de Seguridad de la Información.
- Líderes de proceso.
- Todos los usuarios autorizados.

Riesgo que busca reducir:

Accesos no autorizados, alteración de la información y uso indebido de privilegios administrativos.

Política de Gestión de Contraseñas

Objetivo

Establecer requisitos para la creación, almacenamiento, renovación y protección de las credenciales de acceso utilizadas en los sistemas corporativos.

Alcance

Aplica a todos los usuarios con acceso a recursos tecnológicos de la organización.

Lineamientos principales:

- Las contraseñas deberán contener una longitud mínima de doce caracteres.
- Se utilizarán combinaciones de letras, números y caracteres especiales.
- Las contraseñas deberán renovarse periódicamente.
- Está prohibido reutilizar contraseñas anteriores.
- No podrán almacenarse en papel ni compartirse con otros usuarios.
- Responsables
- Dirección de Tecnología.
- Todos los colaboradores.

Riesgo que busca reducir

Compromiso de cuentas mediante ataques de fuerza bruta, robo de credenciales o ingeniería social.

Política de Clasificación de la Información

Objetivo

Establecer criterios para clasificar la información institucional según su nivel de sensibilidad y definir las medidas de protección correspondientes.

Alcance

Aplica a toda la información física y digital generada por la organización.

Lineamientos principales:

- La información será clasificada como Pública, Uso Interno, Confidencial o Restringida.
- Los documentos confidenciales deberán almacenarse únicamente en repositorios autorizados.
- Se restringirá el uso de dispositivos personales para almacenar información institucional.
- Toda información deberá eliminarse mediante procedimientos seguros cuando finalice su periodo de conservación.
- Responsables
- Todos los colaboradores.
- Líderes de proceso.
- Área de Tecnología.

Riesgo que busca reducir

Pérdida de propiedad intelectual, fuga de información y divulgación de datos confidenciales.

Política de Gestión de Respaldos

Objetivo

Garantizar la disponibilidad y recuperación de la información institucional mediante procedimientos seguros de respaldo.

Alcance

Aplica a todos los sistemas de información y bases de datos críticas.

Lineamientos principales:

- Se realizarán copias de seguridad automáticas.
- Los respaldos deberán almacenarse en ubicaciones diferentes.
- Se efectuarán pruebas periódicas de restauración.
- Los respaldos deberán protegerse mediante mecanismos de cifrado.
- Responsables
- Dirección de Tecnología.
- Administradores de infraestructura.

Riesgo que busca reducir

Pérdida permanente de información y prolongadas interrupciones operativas.

Política de Respuesta a Incidentes

Objetivo

Definir el procedimiento institucional para detectar, contener, analizar y recuperar los servicios afectados por incidentes de seguridad.

Alcance

Aplica a todos los incidentes que afecten activos tecnológicos o información institucional.

Lineamientos principales:

- Todo incidente deberá ser reportado inmediatamente.
- Se establecerá un equipo responsable de la atención de incidentes.
- Cada incidente deberá documentarse y analizarse.

- Finalizado el incidente se implementarán acciones correctivas para evitar su recurrencia.
- Responsables
- Equipo de Tecnología.
- Responsable de Seguridad de la Información.
- Alta Dirección.

Riesgo que busca reducir

Incremento del impacto causado por una respuesta tardía o desorganizada.

Controles propuestos

Tabla 7. Controles de seguridad.

Riesgo	***Control***	***Justificación***
Acceso no autorizado al ERP	Implementación de autenticación multifactor (MFA).	Reduce significativamente el riesgo de compromiso de credenciales.
Uso compartido de usuarios	Gestión de identidades y revisión periódica de privilegios.	Garantiza que cada usuario tenga únicamente los permisos necesarios.
Robo de información técnica	Cifrado de equipos portátiles y restricción de dispositivos personales.	Protege la información sensible frente a pérdida o robo de equipos.

Ataques de phishing	Capacitaciones periódicas y campañas de concienciación.	Disminuye el riesgo asociado al error humano.
Sistemas desactualizados	Gestión de parches y actualización continua.	Reduce la explotación de vulnerabilidades conocidas.
Propagación de malware	Segmentación de redes industriales.	Limita la propagación de amenazas entre diferentes segmentos de la infraestructura.
Pérdida de información	Copias de seguridad automáticas con pruebas de restauración.	Garantiza la recuperación de la información ante incidentes.
Configuraciones inseguras	Auditorías periódicas de infraestructura tecnológica.	Permite identificar y corregir configuraciones vulnerables.
Actividades maliciosas	Monitoreo continuo de eventos y registros de auditoría.	Facilita la detección temprana de incidentes de seguridad.

Interrupción de procesos críticos	Implementación del Plan de Continuidad del Negocio.	Reduce el tiempo de recuperación y asegura la continuidad operativa.

Justificación de las políticas y controles

Las políticas y controles propuestos responden a los riesgos valorados en la matriz: cada medida ataca una debilidad concreta que el análisis documentó en Industrias Metalmecánicas del Valle S.A.S. Su implementación fortalece la protección de los activos críticos, mejora la capacidad de prevención frente a las amenazas y establece procedimientos que hoy la empresa no tiene.

Las políticas de control de accesos y de clasificación de la información atienden los dos hallazgos más repetidos del diagnóstico. Con credenciales individuales y privilegios revisados se reduce la probabilidad de accesos no autorizados y se recupera la trazabilidad que las cuentas compartidas anularon. Con reglas claras de clasificación y manejo, la información estratégica deja de circular por dispositivos personales y canales informales. La política de respaldos, junto con las pruebas de restauración, apunta al otro frente: que la organización pueda recuperarse cuando un incidente comprometa la disponibilidad de sus servicios, certeza que hoy no existe porque las copias nunca se han probado.

Los controles técnicos refuerzan la infraestructura por su lado. La autenticación multifactor dificulta el uso de credenciales robadas, la gestión de actualizaciones cierra las fallas conocidas de los equipos industriales y el control de cambios evita interrupciones como la que ya detuvo una línea de producción. A la par, la capacitación permanente y el procedimiento de gestión de incidentes trabajan el componente humano: buscan que los colaboradores dejen de ver la seguridad como un asunto exclusivo del área de tecnología, sepan reconocer un intento de engaño y tengan claro qué hacer y a quién reportar cuando algo ocurra.

El efecto conjunto se da sobre las dos variables de la matriz. Las medidas preventivas reducen la probabilidad de que los riesgos se materialicen; las de recuperación y respuesta disminuyen el impacto cuando algo falla. Con ello la organización protege su continuidad operativa y alinea su gestión de seguridad con las buenas prácticas establecidas por la ISO/IEC 27001:2022 y la ISO/IEC 27002:2022.

Gestión de incidentes y continuidad del negocio

La dependencia tecnológica que hoy tienen las organizaciones industriales cambió el peso de los incidentes de seguridad: una falla o un ataque ya no afecta solo a la información, afecta la operación completa. Por eso la gestión de incidentes y la continuidad del negocio son piezas centrales de cualquier estrategia de seguridad: de ellas depende que los servicios sigan disponibles, que las pérdidas se contengan y que los procesos críticos se recuperen en un tiempo razonable. La norma ISO/IEC 27035-1:2023 plantea que la gestión de incidentes debe estructurarse en procesos de preparación, detección, evaluación, respuesta y aprendizaje, de manera que el impacto de cada evento se reduzca y la capacidad de respuesta de la organización mejore con la experiencia (ISO, 2023).

Para Industrias Metalmecánicas del Valle S.A.S., el análisis permitió identificar varios escenarios capaces de comprometer la continuidad: accesos no autorizados a los sistemas corporativos, ataques de ransomware, pérdida de información técnica, fallas en la infraestructura, campañas de phishing y explotación de vulnerabilidades en los sistemas industriales. Cada uno amenaza la confidencialidad, la integridad o la disponibilidad de la información, y varios de ellos golpean directamente la producción: líneas detenidas, pedidos retrasados, sobrecostos y daño a la reputación de la empresa. No son escenarios teóricos; la interrupción de una línea de fabricación y la pérdida del portátil con diseños ya mostraron ese encadenamiento.

La continuidad del negocio busca justamente que los procesos esenciales se mantengan o se restablezcan en un tiempo aceptable después de un incidente. Eso exige un trabajo previo: identificar los eventos con mayor probabilidad de ocurrir, asignar responsabilidades claras, definir procedimientos de respuesta y contar con mecanismos de recuperación de los servicios críticos. De acuerdo con ISO 22301:2019, un sistema de gestión de continuidad del negocio fortalece la resiliencia de la organización y mejora su capacidad de recuperación frente a situaciones que alteren su funcionamiento normal (ISO 22301, 2019).

A partir de los riesgos valorados en el diagnóstico, se proponen a continuación los incidentes potenciales y un plan básico de respuesta, como punto de partida para que la organización formalice su proceso de gestión de incidentes, hoy inexistente.

Tabla 8. Incidentes potenciales.

Incidente	***Descripción***	***Impacto***
Acceso no autorizado al sistema ERP	Uso indebido de credenciales o explotación de privilegios para acceder a información corporativa.	Alto
Ataque de ransomware	Cifrado de servidores o estaciones de trabajo que impida el acceso a la información.	Alto
Campaña de phishing	Correos electrónicos fraudulentos dirigidos a obtener credenciales o instalar software malicioso.	Alto
Pérdida o robo de equipos portátiles	Extravío de dispositivos con información técnica o confidencial de la organización.	Alto
Fallo del sistema MES	Interrupción del sistema que controla los procesos de producción industrial.	Alto
Indisponibilidad de la infraestructura de red	Fallas en la conectividad que afecten la operación de los sistemas corporativos.	Alto

Corrupción o pérdida de bases de datos	Eliminación accidental, daño lógico o alteración de información crítica.	Alto
Falla en la recuperación de respaldos	Imposibilidad de restaurar la información después de un incidente.	Alto
Infección por malware	Propagación de software malicioso en estaciones de trabajo y servidores.	Medio
Error humano en procesos críticos	Eliminación accidental de información o configuraciones incorrectas por parte de usuarios.	Medio

Tabla 9. Plan básico de respuesta.

Fase	***Acción***
Preparación	Definir roles y responsabilidades, establecer procedimientos, realizar capacitaciones y mantener actualizados los controles de seguridad.
Identificación	Detectar oportunamente el incidente mediante monitoreo, registros de auditoría y reportes de los usuarios.
Contención	Aislar los sistemas afectados para evitar la propagación del incidente y proteger los activos críticos.
Erradicación	Eliminar la causa del incidente mediante la remoción de malware, cierre de vulnerabilidades o revocación de accesos comprometidos.
Recuperación	Restaurar los sistemas y la información utilizando respaldos verificados y validar el funcionamiento normal de los servicios.

Comunicación	Informar oportunamente a la alta dirección, responsables del proceso y demás partes interesadas sobre la evolución del incidente.
Lecciones aprendidas	Documentar el incidente, identificar oportunidades de mejora y actualizar políticas, procedimientos y controles para prevenir eventos similares.

Análisis de la gestión de incidentes y la continuidad del negocio

La implementación de un proceso formal de gestión de incidentes permitirá a Industrias Metalmecánicas del Valle S.A.S. responder de manera organizada y reducir el impacto que un evento de seguridad pueda generar sobre sus operaciones. Actualmente, el caso de estudio evidencia la ausencia de procedimientos documentados para atender incidentes, lo que puede ocasionar respuestas tardías, falta de coordinación entre las áreas involucradas y mayores tiempos de recuperación.

La fase de preparación representa el elemento más importante del proceso, ya que permite establecer previamente los recursos, responsabilidades y mecanismos necesarios para actuar frente a un incidente. En esta etapa resulta indispensable conformar un equipo responsable de la gestión de incidentes, definir canales de comunicación, mantener inventarios actualizados de los activos y realizar capacitaciones periódicas a los colaboradores. Estas acciones facilitan una respuesta más rápida y disminuyen la probabilidad de errores durante situaciones de emergencia.

Una vez identificado un incidente, la organización debe priorizar las actividades de contención, especialmente cuando se trate de ataques de ransomware, accesos no autorizados o propagación de malware dentro de la infraestructura tecnológica. El aislamiento oportuno de los equipos afectados, la deshabilitación de cuentas comprometidas y la segmentación temporal de las redes permiten evitar que el incidente se extienda hacia otros sistemas críticos, reduciendo así el impacto sobre la producción y los servicios corporativos.

Posteriormente, la fase de erradicación busca eliminar completamente la causa del incidente. Para ello es necesario aplicar actualizaciones de seguridad, eliminar software malicioso, corregir configuraciones vulnerables y fortalecer los controles que permitieron la materialización del evento. No basta con restablecer el funcionamiento de los sistemas; también es necesario eliminar las condiciones que facilitaron el incidente para evitar su repetición.

La recuperación constituye uno de los aspectos más relevantes para garantizar la continuidad del negocio. En el caso analizado, la existencia de copias de seguridad representa una fortaleza; sin embargo, el diagnóstico evidencia que estas no son sometidas a pruebas periódicas de restauración. Por esta razón, se recomienda establecer procedimientos que permitan verificar regularmente la integridad de los respaldos y asegurar que puedan utilizarse eficazmente cuando ocurra un incidente real.

Finalmente, el proceso debe concluir con una etapa de lecciones aprendidas, en la que se documenten las causas del incidente, la efectividad de la respuesta implementada y las oportunidades de mejora identificadas. Esta información permitirá actualizar las políticas de seguridad, fortalecer los controles existentes y mejorar continuamente la capacidad de respuesta de la organización.

En conjunto, las medidas propuestas contribuyen a incrementar la resiliencia organizacional y permiten que Industrias Metalmecánicas del Valle S.A.S. mantenga la continuidad de sus procesos críticos aun cuando se presenten incidentes de seguridad que afecten sus activos tecnológicos. La combinación de procedimientos documentados, personal capacitado, controles preventivos y mecanismos de recuperación fortalecerá la capacidad de la empresa para proteger la información, minimizar tiempos de inactividad y garantizar el cumplimiento de sus compromisos operativos y comerciales.

Cultura organizacional en ciberseguridad

Ningún control técnico protege a una empresa cuyos empleados no saben protegerla. La tecnología detiene una parte de los ataques; la otra parte entra por las personas, por sus hábitos y por lo que ignoran. De ahí que la cultura organizacional en ciberseguridad sea un asunto estratégico y no un complemento: es la que reduce los incidentes que nacen de un error humano, de un procedimiento ignorado o del desconocimiento de los riesgos del manejo de la información.

Las referencias del sector apuntan en esa dirección. La norma ISO/IEC 27002:2022 pide procesos permanentes de concienciación, educación y capacitación, para que cada colaborador entienda su responsabilidad frente a la información y trabaje con prácticas seguras (ISO, 2022). El NIST Cybersecurity Framework 2.0 agrega el ingrediente que suele faltar: formación continua sí, pero acompañada de comunicación efectiva y de liderazgo, porque sin respaldo de la dirección la cultura no se sostiene (NIST, 2024).

¿Y cómo está la empresa en ese frente? El contraste es notorio. Industrias Metalmecánicas del Valle S.A.S. ha invertido en infraestructura tecnológica, pero el componente humano se quedó atrás. Los supervisores comparten credenciales. La información técnica termina en dispositivos personales. Las capacitaciones existen, aunque esporádicas y sin cubrir a todo el personal. No hay un procedimiento para reportar incidentes, y en las entrevistas apareció el hallazgo que explica todos los anteriores: buena parte del personal cree que la seguridad es un asunto del área de tecnología, mientras algunas áreas anteponen sus metas de producción a cualquier control.

El diagnóstico deja entonces una lectura incómoda pero útil: varios de los riesgos valorados no vienen de fallas en los sistemas sino de la forma en que la gente trabaja. Y eso no se corrige comprando equipos. Se corrige con una cultura que involucre a todos los colaboradores en la protección de la información, desde la gerencia hasta la planta, y no solamente al equipo de TI.

Tabla 10. Hallazgos organizacionales.

Situación observada	***Riesgo asociado***
Uso compartido de credenciales entre algunos colaboradores.	Accesos no autorizados, pérdida de trazabilidad y uso indebido de privilegios.
Almacenamiento de información técnica en dispositivos personales.	Fuga de información, pérdida de propiedad intelectual y exposición de datos sensibles.
Ausencia de programas permanentes de capacitación en ciberseguridad.	Mayor probabilidad de ataques de phishing, ingeniería social y errores humanos.
Procedimientos poco definidos para el reporte de incidentes.	Respuesta tardía y aumento del impacto de los incidentes de seguridad.
Falta de actualización periódica de algunos sistemas tecnológicos.	Explotación de vulnerabilidades conocidas y afectación de los servicios críticos.
Escasa sensibilización sobre la clasificación y manejo de la información.	Divulgación accidental de información confidencial e incumplimiento de políticas internas.

Dependencia del conocimiento individual para algunos procesos tecnológicos.	Riesgo operativo ante ausencia de personal clave o rotación de colaboradores.

Tabla 11. Recomendaciones de mejora.

Hallazgo	***Recomendación***
Uso compartido de credenciales.	Implementar campañas de sensibilización sobre gestión de identidades y aplicar controles que impidan compartir cuentas de usuario.
Uso de dispositivos personales para almacenar información corporativa.	Restringir el almacenamiento de información institucional en equipos personales e implementar soluciones de cifrado y administración de dispositivos.
Falta de capacitación en ciberseguridad.	Diseñar un programa anual de formación que incluya phishing, gestión de contraseñas, protección de datos y respuesta a incidentes.

Ausencia de procedimientos para reportar incidentes.	Establecer un protocolo institucional que permita reportar incidentes de forma rápida y documentada.
Sistemas tecnológicos desactualizados.	Implementar un programa periódico de actualización y gestión de vulnerabilidades para todos los activos tecnológicos.
Desconocimiento sobre clasificación de la información.	Capacitar al personal en los niveles de clasificación de la información y en los procedimientos para su adecuado tratamiento.
Dependencia de conocimientos individuales.	Documentar procedimientos críticos y fortalecer la transferencia de conocimiento entre las diferentes áreas de la organización.

Fortalecimiento de la cultura organizacional en ciberseguridad

Las recomendaciones apuntan a la prevención: que la protección de la información deje de recaer en unos pocos y se vuelva tarea de todos los colaboradores. Un programa permanente de capacitación es la base. Con él, el personal entiende a qué amenazas está expuesta la empresa, aprende a reconocer comportamientos sospechosos, cuida sus credenciales y aplica las políticas de seguridad porque las comprende, no porque se las impusieron.

El reporte de incidentes necesita el mismo tratamiento. Hoy nadie sabe a quién avisar ni cómo. Cuando existan canales definidos y acciones claras, los tiempos de detección, contención y recuperación se acortan, y con ellos el impacto sobre los procesos críticos. Un incidente reportado a tiempo es un problema manejable; el mismo incidente callado durante días puede ser una crisis.

La información también pide orden. Sensibilizar al personal sobre el valor de lo que maneja reduce las fugas y facilita el cumplimiento de las políticas. Restringir el almacenamiento de información de la empresa en dispositivos personales cierra una exposición que ya cobró un portátil con diseños en desarrollo.

Nada de lo anterior se sostiene sin la alta dirección. Se necesitan recursos para capacitar, políticas actualizadas y seguimiento periódico a los indicadores de seguridad. Ese respaldo visible es lo que convierte la ciberseguridad en una responsabilidad compartida y no en una función más del área de tecnología, que es justamente la creencia que el diagnóstico encontró instalada.

Con colaboradores formados, procedimientos documentados, liderazgo comprometido y controles técnicos funcionando, la empresa puede elevar de forma progresiva su madurez en seguridad de la información. Esa combinación fortalece su resiliencia frente a las amenazas, protege sus activos críticos y asegura la continuidad de una operación que depende cada día más de lo digital.

Conclusiones

El diagnóstico arrojó un resultado que conviene señalar de entrada. De los quince activos inventariados, los que concentraron riesgo alto no son aquellos donde la empresa carece de tecnología, sino aquellos donde invirtió en tecnología sin acompañarla de gestión. El sistema MES, los diseños elaborados en CAD, el correo corporativo, las redes industriales y la plataforma de respaldos operan sobre infraestructura suficiente; lo que falta en cada caso es una credencial individual, una clasificación de la información, una capacitación permanente o una prueba de restauración. La seguridad de esta organización no depende de adquirir más soluciones técnicas.

El cruce entre la matriz de riesgos y los cinco incidentes registrados confirma esa lectura. De los cuatro escenarios con mayor valoración, tres ya se materializaron: el acceso indebido con cuentas compartidas, el extravío del portátil con diseños en desarrollo y el correo fraudulento que suplantó a un proveedor estratégico. Ninguno explotó una falla de software. Los tres aprovecharon una práctica organizacional que sigue vigente, razón por la cual su probabilidad se calificó como alta. El cuarto escenario, la ausencia de pruebas de restauración, no ha producido incidentes visibles todavía, y por eso mismo resulta el más comprometedor: de él depende que los demás sean recuperables.

La valoración también mostró que las cuatro problemáticas de fondo identificadas al inicio del estudio funcionan como causas encadenadas y no como hallazgos independientes. Las credenciales compartidas anulan la trazabilidad, y sin trazabilidad ningún procedimiento de gestión de incidentes puede establecer qué ocurrió ni quién intervino. La ausencia de una política de clasificación permite que los planos circulen por dispositivos personales y aplicaciones de mensajería, y esa circulación convierte un extravío en una fuga de propiedad intelectual. La creencia de que la seguridad corresponde únicamente al área de tecnología sostiene las tres anteriores, porque ninguna se corrige desde la dirección de TI sin participación de las áreas que las originan. Por ese motivo las políticas propuestas se ordenaron en ese sentido: control de accesos y clasificación de la información primero, dado que del avance en esas dos frentes depende la efectividad de las restantes.

Un cuarto resultado se refiere a la capacidad de respuesta. Los incidentes de los últimos tres años se atendieron sin procedimientos documentados, sin responsables definidos y sin certeza sobre el estado de los respaldos. Esa improvisación no aumentó el número de eventos, pero sí su costo: la interrupción de la línea de fabricación generó retrasos y sobrecostos que un procedimiento formal de contención habría acotado. Las políticas, el plan de respuesta y las pruebas periódicas de restauración propuestas en este informe atienden precisamente esa distancia entre lo que la empresa detecta y lo que puede hacer al respecto.

El diagnóstico entrega, en consecuencia, un punto de partida antes que un cierre. La organización proyecta incorporar líneas automatizadas y sensores IoT durante los próximos dos años, lo que ampliará la superficie de ataque sobre una red que hoy ya presenta dispositivos de planta con autenticación débil y equipos sin actualizaciones recientes. Cada nuevo elemento conectado heredará las condiciones actuales de gestión,

no las de la tecnología que se adquiera. Formalizar la seguridad de la información antes de esa expansión, y no después, constituye la conclusión práctica que se desprende del ejercicio.

Referencias

ISA/IEC 62443. (2018). Obtenido de https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

ISO 22301. (2019). Obtenido de https://www.iso.org/standard/75106.html

ISO/IEC 27001:2022. (s.f.). Obtenido de https://www.iso.org/standard/82875.html

ISO/IEC 27002. (2022). Obtenido de https://www.iso.org/standard/75652.html

ISO/IEC 27005. (2022). Obtenido de https://www.iso.org/standard/80585.html

ISO/IEC 27035-1. (2023). Obtenido de https://www.iso.org/standard/60803.html

MinTIC. (2021). Obtenido de https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7288.html

NIST. (2024). Obtenido de https://www.nist.gov/cyberframework

Centro Criptológico Nacional. (2021). CCN-STIC 817. Gestión de ciberincidentes. https://www.ccn-cert.cni.es

Instituto Nacional de Ciberseguridad. (2022). Guía de gestión de riesgos de seguridad de la información. https://www.incibe.es

Instituto Nacional de Ciberseguridad. (2023). Protege tu empresa. https://www.incibe.es/protege-tu-empresa