TRABAJO DE GRADO
Opción Seminario.

Título del trabajo
Informe Técnico de Ciberseguridad de Logired Express 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.

David Esneider Flórez Crespo
Cristian Camilo Roa Leal
Luis Fernando Sanclemente Bedoya
Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Dedicatoria

Este trabajo esta dedicado en primer lugar a Dios por brindarnos la sabiduría y la perseverancia necesaria para culminar esta importante etapa de nuestra vida profesional.

A nuestras familias, quienes nos han apoyado incondicional en todo el proceso académico dándonos todo su apoyo, motivación y amor para superar cada reto que con lleva este proceso de formación.

También dedicamos este trabajo a nuestros docentes quienes nos compartieron todos sus conocimientos y experiencia, ayudándonos a desarrollar competencias y habilidades en toda nuestra formación.

Agradecimientos

Expresamos nuestro agradecimiento a la corporación universitaria rémington y especialmente a la facultad de ingeniería de sistemas, por brindarnos una formación académica basada en principios de muy alto valor éticos los cuales forman profesionales de alto valor.

De igual manera, agradecemos al docente Jorge leonardo Ramírez restrepo por su orientación y apoyo académico durante el desarrollo del semanario de gestión de ciberseguridad en organizaciones.

Reconocemos la importancia del tema de estudio desarrollado sobre Logired Express S.A.S El cual nos permitió aplicar todas las competencias adquiridas en el seminario analizando los riesgos de seguridad de la información y gestión de incidentes basados dentro de un entorno empresarial enfocado en procesos logísticos y tecnológicos

Tabla de Contenidos

Resumen

La transformación digital ha convertido a la información en uno de los activos más importantes para las organizaciones, incrementando la necesidad de implementar estrategias que permitan garantizar su confidencialidad, integridad y disponibilidad. En este contexto, el presente informe técnico desarrolla un análisis de ciberseguridad para la empresa Logired Express S.A.S., organización colombiana dedicada a la prestación de servicios de logística, almacenamiento, transporte y distribución de mercancías a nivel nacional.

El estudio parte del diagnóstico realizado a la infraestructura tecnológica y a los procesos organizacionales, mediante el cual se identificaron diversas debilidades relacionadas con la administración de activos de información, el control de accesos, la gestión de dispositivos móviles corporativos, la ausencia de políticas de clasificación de la información, la utilización de aplicaciones personales para compartir datos corporativos y la inexistencia de procedimientos documentados para la gestión de incidentes de seguridad.

Con base en estas situaciones, se efectuó un análisis de amenazas, vulnerabilidades y riesgos, aplicando metodologías reconocidas internacionalmente para identificar los procesos críticos y establecer controles orientados a disminuir la probabilidad de materialización de incidentes de seguridad.

Como resultado, se plantean políticas organizacionales, controles técnicos y administrativos, así como recomendaciones encaminadas a fortalecer la cultura de ciberseguridad, mejorar la gestión de activos de información, optimizar los mecanismos de respaldo y recuperación de información, implementar procesos de respuesta ante incidentes y fortalecer la continuidad del negocio.

La aplicación de las medidas propuestas permitirá a Logired Express S.A.S. incrementar su nivel de madurez en ciberseguridad, reducir riesgos operacionales y proteger la información estratégica necesaria para garantizar la continuidad de sus operaciones y apoyar los planes de crecimiento nacional e internacional de la organización.

Palabras clave

1. Ciberseguridad.
2. Seguridad de la información.
3. Gestión de riesgos.
4. Activos de información.
5. Continuidad del negocio.

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

En la actualidad, la transformación digital ha permitido que las organizaciones automaticen gran parte de sus procesos mediante el uso de plataformas tecnológicas, servicios en la nube, aplicaciones móviles y sistemas de información. Sin embargo, este crecimiento tecnológico también ha incrementado la exposición a amenazas cibernéticas que pueden comprometer la operación, la reputación y la información crítica de las empresas. En este contexto, la ciberseguridad se convierte en un elemento estratégico para garantizar la continuidad del negocio y proteger los activos de información.

La ciberseguridad comprende el conjunto de políticas, procesos, tecnologías y controles destinados a proteger los sistemas informáticos, las redes, los dispositivos y la información frente a accesos no autorizados, ataques informáticos, alteraciones o pérdida de datos. Su objetivo principal consiste en reducir los riesgos derivados del uso de las tecnologías de la información y garantizar la continuidad de las operaciones empresariales (ISO/IEC 27001:2022).

Por otra parte, la seguridad de la información busca preservar tres principios fundamentales conocidos como la triada CIA:

Confidencialidad

La confidencialidad garantiza que la información únicamente pueda ser consultada por personas autorizadas. Dentro de Logired Express S.A.S. este principio resulta fundamental debido a que diariamente se administra información relacionada con clientes, rutas de transporte, inventarios, proveedores y procesos financieros.

La pérdida de confidencialidad puede ocasionar fuga de información estratégica, sanciones legales y pérdida de confianza por parte de los clientes.

Integridad

La integridad asegura que la información permanezca completa, exacta y libre de modificaciones no autorizadas.

En una empresa logística, la alteración de datos relacionados con inventarios, rutas de entrega o información financiera podría generar errores operativos, pérdidas económicas e incumplimiento de compromisos comerciales.

Disponibilidad

La disponibilidad consiste en garantizar que la información y los servicios tecnológicos puedan utilizarse cuando sean requeridos por los usuarios autorizados.

En Logired Express S.A.S. resulta indispensable mantener disponibles sistemas como:

- ERP Empresarial.
- Sistema TMS.
- Plataforma WMS.
- Plataforma GPS.
- Portal de clientes.
- Aplicación móvil para conductores.

Una indisponibilidad prolongada podría detener completamente la operación logística.

Activos de información

Los activos de información corresponden a todos aquellos recursos que poseen valor para la organización y requieren protección.

Dentro de Logired Express S.A.S. pueden identificarse los siguientes activos críticos:

- Bases de datos de clientes.
- Información financiera.
- Inventarios.
- Infraestructura tecnológica.
- Servidores.
- Equipos de cómputo.
- Dispositivos móviles.
- Plataformas ERP, TMS y WMS.
- Correos electrónicos.
- Documentación administrativa.
- Información de rutas.
- Credenciales de acceso.

La correcta identificación de estos activos constituye el primer paso para desarrollar una adecuada gestión de riesgos.

Amenazas

Una amenaza es cualquier evento, acción o circunstancia con capacidad de afectar negativamente un activo de información.

Entre las amenazas que pueden afectar a Logired Express S.A.S. se encuentran:

- Ataques de phishing.
- Malware.
- Ransomware.
- Robo de dispositivos móviles.
- Accesos no autorizados.
- Ataques internos.
- Errores humanos.
- Interrupciones del servicio de Internet.
- Fallas eléctricas.
- Desastres naturales.
- Sabotaje.
- Ingeniería social.

El caso de estudio evidencia que la organización ya ha experimentado algunos de estos eventos, como el robo de un dispositivo móvil corporativo y un ataque de phishing dirigido contra uno de sus colaboradores.

Vulnerabilidades

Las vulnerabilidades representan debilidades presentes en la infraestructura tecnológica, procesos o personas que pueden ser aprovechadas por una amenaza.

Durante el diagnóstico inicial de Logired Express S.A.S. se identificaron vulnerabilidades relevantes, entre ellas:

- Ausencia de clasificación de la información.
- Contraseñas débiles.
- Dispositivos móviles sin cifrado.
- Uso de aplicaciones personales para compartir información.
- Cuentas activas de excolaboradores.
- Falta de inventario actualizado de activos.
- Ausencia de procedimientos para la respuesta a incidentes.
- Falta de campañas permanentes de sensibilización.

Estas vulnerabilidades incrementan significativamente el nivel de exposición frente a ataques cibernéticos.

Riesgo

El riesgo corresponde a la posibilidad de que una amenaza aproveche una vulnerabilidad y genere un impacto negativo sobre la organización.

La gestión del riesgo permite identificar, analizar, valorar y tratar aquellos riesgos que puedan afectar el cumplimiento de los objetivos empresariales.

En el caso de Logired Express S.A.S., algunos riesgos prioritarios son:

- Fuga de información.
- Acceso no autorizado.
- Pérdida de disponibilidad de los sistemas.
- Alteración de inventarios.
- Interrupción del servicio logístico.
- Incumplimiento normativo.
- Afectación reputacional.

Controles de seguridad

Los controles de seguridad constituyen medidas administrativas, técnicas y físicas implementadas para reducir los riesgos identificados.

Los controles pueden clasificarse como:

Controles preventivos

Buscan evitar que ocurra un incidente.

Ejemplos:

- Autenticación multifactor.
- Políticas de contraseñas.
- Capacitación.
- Segmentación de redes.
- Cifrado.

Controles de detección

Permiten identificar oportunamente incidentes de seguridad.

Ejemplos:

- Monitoreo de eventos.
- Antivirus.
- Sistemas SIEM.
- Auditorías.
- Registros de acceso.

Controles correctivos

Su objetivo consiste en restablecer la operación después de un incidente.

Ejemplos:

- Copias de seguridad.
- Planes de recuperación.
- Gestión de incidentes.
- Continuidad del negocio.

Conceptos fundamentales de ciberseguridad

La ciberseguridad es el conjunto de prácticas, políticas y tecnologías orientadas a proteger los sistemas informáticos, redes y datos frente a accesos no autorizados, ataques o daños. En el contexto de Logired Express S.A.S., la ciberseguridad resulta esencial para garantizar la continuidad de las operaciones logísticas y la confianza de los clientes, dado que la empresa depende de plataformas tecnológicas para gestionar envíos, bodegas y transporte.

Seguridad de la información
La seguridad de la información se centra en proteger los datos de la organización, sin importar el medio en que se encuentren digital o físico. Su propósito es preservar la confiabilidad de los procesos y evitar pérdidas o filtraciones de información sensible, como rutas de transporte, datos de clientes o inventarios.

Confidencialidad
La confidencialidad implica que la información solo sea accesible para las personas autorizadas. En el caso de Logired, esto significa que datos como reportes operativos o información de clientes no deben ser compartidos mediante aplicaciones personales de mensajería, ni almacenados en dispositivos no corporativos.

Integridad
La integridad asegura que la información se mantenga completa y sin alteraciones indebidas. Un ejemplo en la empresa es el evento donde un error humano generó inconsistencias en los inventarios: la falta de controles adecuados afectó la integridad de los datos, lo que repercutió en la operación logística.

Disponibilidad
La disponibilidad garantiza que los sistemas y datos estén accesibles cuando se necesiten. En Logired, la interrupción del servicio de internet en un centro de distribución evidenció la importancia de contar con planes de contingencia para mantener la operación aun en situaciones de falla tecnológica.

Aportes
Para nosotros estos conceptos se articulan directamente con los hallazgos del diagnóstico inicial, la ausencia de políticas claras de clasificación de información, el uso de dispositivos personales y la falta de procedimientos de seguridad ponen en riesgo la confidencialidad, integridad y disponibilidad de los datos.

Bibliografía

ISO/IEC 27001:2013. Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información.

Whitman, M. & Mattord, H. (2022). Principles of Information Security. Cengage Learning.

Stallings, W. (2019). Computer Security: Principles and Practice. Pearson.

Peltier, T. (2016). Information Security Policies, Procedures, and Standards. CRC Press.

ENISA (European Union Agency for Cybersecurity). (2021). Cybersecurity Basics. Disponible en: https://www.enisa.europa.eu

Marco normativo

Para fortalecer la gestión de la ciberseguridad en Logired Express S.A.S. se consideran las siguientes normas y estándares internacionales.

Tabla 1. Normatividad aplicable.

Norma o estándar	*Propósito*	*Aplicabilidad en Logired Express S.A.S.*
ISO/IEC 27001:2022	Implementar un Sistema de Gestión de Seguridad de la Información (SGSI).	Permite establecer políticas, controles y gestión de riesgos.
ISO/IEC 27002:2022	Buenas prácticas para controles de seguridad.	Sirve como guía para implementar controles técnicos y administrativos.
NIST Cybersecurity Framework 2.0	Gestión integral de riesgos de ciberseguridad.	Facilita identificar, proteger, detectar, responder y recuperar ante incidentes.
ISO 22301	Gestión de Continuidad del Negocio.	Garantiza la continuidad de las operaciones frente a interrupciones.
Ley 1581 de 2012	Protección de datos personales.	Regula el tratamiento de la información de clientes y colaboradores.
Ley 1273 de 2009	Delitos informáticos.	Establece sanciones frente a ataques contra la información y sistemas informáticos.
Decreto 1377 de 2013	Reglamenta la protección de datos personales.	Complementa la gestión de información personal dentro de la organización.

Importancia del marco normativo

La adopción de estas normas permitirá a Logired Express S.A.S. fortalecer su modelo de seguridad de la información mediante la implementación de procesos de gestión de riesgos, políticas corporativas, controles de acceso, protección de datos personales y planes de continuidad del negocio. Además, facilitará el cumplimiento de la legislación colombiana y el desarrollo de una cultura organizacional orientada a la ciberseguridad, aspecto fundamental considerando el crecimiento proyectado de la empresa y su futura expansión internacional.

Referencias (APA 7)

- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.
- National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0.
- Congreso de Colombia. (2012). Ley 1581 de 2012.
- Congreso de Colombia. (2009). Ley 1273 de 2009.
- Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013.

Marco contextual

El marco contextual constituye un componente fundamental del presente informe técnico, ya que permite describir el entorno organizacional en el cual se desarrolla el análisis de ciberseguridad. Conocer las características de la empresa, su estructura organizacional, los procesos estratégicos y la infraestructura tecnológica facilita la comprensión de los riesgos que pueden afectar la seguridad de la información y la continuidad de las operaciones.

En este capítulo se presenta una caracterización de Logired Express S.A.S., empresa dedicada a la prestación de servicios de logística y distribución de mercancías a nivel nacional. Asimismo, se describen los principales procesos de negocio, los recursos tecnológicos utilizados y las situaciones identificadas durante el diagnóstico inicial, las cuales evidencian la necesidad de fortalecer la gestión de la seguridad de la información mediante la implementación de políticas, controles y buenas prácticas alineadas con estándares internacionales.

El análisis del contexto organizacional permite comprender cómo la creciente dependencia de las tecnologías de la información ha convertido la ciberseguridad en un elemento estratégico para garantizar la disponibilidad, integridad y confidencialidad de los activos de información. Del mismo modo, proporciona las bases para identificar las amenazas, vulnerabilidades y riesgos que serán evaluados en los capítulos posteriores del informe.

Descripción de la organización

Logired Express S.A.S. es una empresa colombiana con más de quince años de experiencia en el sector logístico, dedicada a la prestación de servicios de almacenamiento, transporte, distribución y seguimiento de mercancías a nivel nacional. A lo largo de su trayectoria, la organización ha consolidado una importante participación en el mercado mediante la prestación de servicios a empresas pertenecientes a sectores como comercio, manufactura, salud y tecnología, caracterizados por requerir altos niveles de disponibilidad, confiabilidad y trazabilidad en sus procesos logísticos.

La empresa desarrolla sus operaciones desde una sede administrativa principal y cinco centros regionales de distribución estratégicamente ubicados en diferentes ciudades del país, lo que le permite gestionar diariamente más de 12.000 envíos. Para garantizar la eficiencia operativa, cuenta con aproximadamente 320 colaboradores distribuidos entre personal administrativo, coordinadores logísticos, supervisores de operaciones, conductores, auxiliares de bodega y profesionales del área tecnológica.

La operación de Logired Express S.A.S. depende en gran medida de la infraestructura tecnológica, la cual soporta procesos críticos relacionados con la planificación de rutas, administración de inventarios, monitoreo de vehículos, atención al cliente y gestión financiera. Entre los recursos tecnológicos más importantes se encuentran un sistema ERP empresarial, una plataforma de gestión de transporte (TMS), un sistema de administración de bodegas (WMS), plataformas de monitoreo GPS, aplicaciones móviles para conductores, un portal web para clientes, sistemas de videovigilancia, plataformas de respaldo de información y una infraestructura basada en nube híbrida.

El área de Tecnología y Sistemas está conformada por un gerente de TI, dos administradores de infraestructura, tres analistas de soporte y dos desarrolladores, quienes son responsables de garantizar la disponibilidad, mantenimiento y seguridad de los servicios tecnológicos que soportan la operación diaria.

El crecimiento constante de la organización ha generado una mayor dependencia de las tecnologías de la información, convirtiendo a la ciberseguridad en un componente estratégico para garantizar la continuidad de las operaciones, proteger los activos de información y mantener la confianza de clientes, proveedores y demás partes interesadas.

Problemática identificada

Como parte del proceso de evaluación inicial, una firma consultora especializada realizó un diagnóstico sobre el estado de la seguridad de la información dentro de la organización, identificando diversas situaciones que representan riesgos significativos para la operación y la continuidad del negocio. Uno de los principales hallazgos corresponde a la ausencia de una política formal para la clasificación de la información, situación que dificulta establecer niveles adecuados de protección según la sensibilidad de los datos administrados por la empresa. Esta debilidad incrementa la probabilidad de divulgación no autorizada de información relacionada con clientes, rutas logísticas, inventarios y procesos administrativos. También se evidenció que algunos conductores comparten dispositivos móviles corporativos durante los cambios de turno y que varios supervisores almacenan información operativa en dispositivos personales, prácticas que incrementan el riesgo de pérdida, alteración o acceso no autorizado a información corporativa.

Durante el diagnóstico también fueron identificadas cuentas de usuario pertenecientes a excolaboradores que permanecían activas dentro de algunos sistemas empresariales, lo cual representa una vulnerabilidad crítica debido a la posibilidad de accesos no autorizados a plataformas corporativas. Otro aspecto preocupante corresponde a la inexistencia de mecanismos de cifrado en parte de los dispositivos móviles corporativos. En caso de pérdida o robo de estos equipos, la información almacenada podría ser consultada por terceros sin mayores restricciones.

Adicionalmente, se observó que algunas contraseñas utilizadas por los colaboradores no cumplen con criterios mínimos de complejidad y que diferentes centros regionales administran la información utilizando procedimientos distintos, dificultando la implementación de controles homogéneos de seguridad.

El análisis también permitió identificar la inexistencia de un procedimiento documentado para la gestión de incidentes de ciberseguridad. Aunque la organización realiza copias de seguridad periódicamente, no existen evidencias recientes sobre pruebas de restauración, aspecto que limita la capacidad de recuperación ante eventos que afecten la disponibilidad de la información. Otro hallazgo importante corresponde al uso frecuente de aplicaciones personales de mensajería instantánea para compartir información relacionada con operaciones logísticas. Esta práctica incrementa considerablemente el riesgo de fuga de información, incumplimiento de políticas corporativas y exposición de datos sensibles. Finalmente, el diagnóstico evidenció la ausencia de campañas permanentes de sensibilización en ciberseguridad y la inexistencia de un inventario actualizado de activos de información, limitando la capacidad de la organización para gestionar adecuadamente sus riesgos tecnológicos.

Identificación y analisis de activos

Uno de los procesos más importantes dentro de la gestión de la ciberseguridad consiste en identificar los activos de información que soportan los procesos críticos de la organización. Un activo de información es cualquier recurso que posee valor para la empresa y cuya pérdida, alteración o indisponibilidad puede afectar el cumplimiento de los objetivos estratégicos.

En Logired Express S.A.S., la operación logística depende directamente de diversos activos tecnológicos y de información que permiten administrar el transporte, el almacenamiento, el seguimiento de mercancías, la atención al cliente y los procesos administrativos. Debido a esta alta dependencia tecnológica, resulta indispensable mantener un inventario actualizado que permita conocer el nivel de criticidad de cada activo y establecer controles adecuados para su protección.

La identificación de activos constituye el punto de partida para el análisis de riesgos, ya que permite determinar cuáles recursos requieren mayor nivel de protección y cuáles podrían generar un mayor impacto sobre la operación en caso de materializarse un incidente de seguridad.

Inventario de activos

Tabla 2. Inventario de activos

Activo	*Tipo*	*Descripción*	*Criticidad*
Base de datos de clientes	Información	Contiene información personal, contratos e historial de clientes.	Muy Alta
Sistema ERP	Software	Gestiona procesos administrativos, financieros y operativos.	Muy Alta
Plataforma TMS	Software	Administra rutas, vehículos y entregas.	Muy Alta
Plataforma WMS	Software	Controla inventarios y almacenamiento.	Muy Alta
Sistema GPS	Software/Hardware	Monitorea la ubicación de los vehículos en tiempo real.	Alta
Portal web corporativo	Software	Permite a los clientes consultar el estado de sus envíos.	Alta
Aplicación móvil para conductores	Software	Gestiona entregas, novedades y rutas asignadas.	Alta
Correo electrónico corporativo	Información	Medio oficial de comunicación empresarial.	Alta
Infraestructura en nube híbrida	Infraestructura	Almacena aplicaciones, respaldos y servicios críticos.	Muy Alta
Plataforma de respaldo (Backup)	Infraestructura	Garantiza la recuperación de la información.	Muy Alta
Servidores corporativos	Hardware	Ejecutan aplicaciones críticas de la organización.	Muy Alta
Equipos de escritorio	Hardware	Utilizados por personal administrativo.	Media
Computadores portátiles	Hardware	Utilizados por personal directivo y operativo.	Alta

CLASIFICACIÓN DE LOS ACTIVOS

Los activos identificados pueden clasificarse en cuatro grandes categorías:

Activos de información

Corresponden a los datos utilizados por la organización para desarrollar sus procesos de negocio.

Ejemplos:

- Base de datos de clientes.
- Información financiera.
- Información logística.
- Información de talento humano.
- Documentación corporativa.
- Credenciales de acceso.

Estos activos representan el mayor valor para la organización debido a que contienen información estratégica cuya pérdida podría afectar la continuidad del negocio y generar sanciones legales.

Activos de software

Comprenden las aplicaciones que soportan la operación logística.

Entre ellos se encuentran:

- ERP.
- WMS.
- TMS.
- Portal Web.
- Aplicación móvil.
- Sistema GPS.

La indisponibilidad de cualquiera de estos sistemas tendría un impacto directo sobre la operación diaria.

Activos de hardware

Incluyen todos los equipos físicos utilizados por la empresa.

Entre ellos:

- Servidores.
- Computadores.
- Portátiles.
- Dispositivos móviles.
- Equipos de red.
- Sistema de videovigilancia.

Su protección es fundamental para garantizar la disponibilidad de los servicios tecnológicos.

Activos de infraestructura

Corresponden a los recursos tecnológicos que permiten el funcionamiento de toda la plataforma informática.

Ejemplos:

- Red LAN.
- Redes Wifi.
- Infraestructura en nube híbrida.
- Plataforma de respaldo.
- Equipos de comunicaciones.

Activos críticos

Después del análisis realizado, se identifican como activos críticos los siguientes:

Base de datos de clientes

Constituye uno de los activos más importantes debido a que almacena información confidencial relacionada con clientes, contratos, entregas y facturación. Una pérdida o fuga de esta información podría generar afectaciones legales, económicas y reputacionales.

Sistema ERP

El ERP integra los procesos administrativos, financieros y operativos de la empresa. Su indisponibilidad impediría la ejecución de actividades esenciales como facturación, compras y control presupuestal.

Plataforma TMS

Es el sistema encargado de administrar toda la operación de transporte. Una falla en esta plataforma impediría la programación de rutas y el seguimiento de vehículos.

Plataforma WMS

Controla el almacenamiento, recepción y despacho de mercancías. Una alteración de la información podría ocasionar pérdidas económicas significativas.

Infraestructura en nube híbrida

La organización depende cada vez más de servicios en la nube para soportar aplicaciones críticas y respaldos de información. Este activo requiere elevados niveles de disponibilidad y protección.

Credenciales de acceso

Las cuentas de usuario y contraseñas representan uno de los activos más sensibles debido a que permiten el acceso a los sistemas corporativos. La permanencia de cuentas activas pertenecientes a excolaboradores constituye una vulnerabilidad crítica identificada durante el diagnóstico.

Plataforma de respaldo

Los respaldos garantizan la recuperación de la información ante incidentes como ataques de ransomware, fallas tecnológicas o errores humanos. Aunque la empresa realiza copias de seguridad periódicas, se identificó la necesidad de ejecutar pruebas regulares de restauración para asegurar su efectividad.

Justificación de la criticidad

La valoración de criticidad realizada evidencia que los activos relacionados con la información, los sistemas de gestión empresarial y la infraestructura tecnológica poseen el nivel más alto de importancia para la organización. Estos recursos soportan los procesos misionales de Logired Express S.A.S., incluyendo la planificación logística, el seguimiento de envíos, la administración de inventarios, la atención al cliente y la gestión financiera.

La afectación de cualquiera de estos activos podría ocasionar interrupciones en la operación, pérdida de información confidencial, incumplimiento de obligaciones contractuales, sanciones legales y un deterioro significativo en la imagen corporativa. Por esta razón, dichos activos serán considerados prioritarios en las siguientes etapas del análisis de amenazas, vulnerabilidades y gestión de riesgos.

Analisis de amenazas y vulnerabilidades

La identificación de amenazas y vulnerabilidades constituye una de las etapas fundamentales dentro de la gestión de riesgos en ciberseguridad. Este proceso permite reconocer los eventos que pueden comprometer la confidencialidad, integridad y disponibilidad de la información, así como las debilidades que podrían ser explotadas por actores maliciosos o por errores internos.

En Logired Express S.A.S., el análisis realizado evidencia que la organización enfrenta un entorno tecnológico complejo, debido a la integración de múltiples plataformas, dispositivos móviles, sistemas de información y servicios en la nube que soportan la operación logística a nivel nacional. Esta dependencia tecnológica incrementa la superficie de ataque y exige la implementación de controles de seguridad más robustos. Durante el diagnóstico inicial se identificaron diversas vulnerabilidades relacionadas con la gestión de accesos, protección de dispositivos, administración de la información y cultura organizacional. Estas condiciones aumentan la probabilidad de incidentes que podrían afectar la continuidad del negocio y la confianza de los clientes.
Las amenazas identificadas incluyen tanto factores externos, como ataques informáticos y campañas de phishing, como factores internos relacionados con errores humanos, incumplimiento de políticas y deficiencias en los procesos de seguridad.

Tabla 3. Amenazas y vulnerabilidades

Activo	*Amenaza*	*Vulnerabilidad*
Base de datos de clientes	Robo de información	No existe clasificación de la información
ERP	Acceso no autorizado	Contraseñas débiles
ERP	Malware	Equipos sin controles actualizados
Plataforma TMS	Ransomware	Falta de segmentación de red
Plataforma WMS	Alteración de inventarios	Errores humanos
Sistema GPS	Caída del servicio	Dependencia del proveedor
Portal Web	Ataques DDoS	Falta de monitoreo permanente
Aplicación móvil	Robo del dispositivo	Equipos sin cifrado
Dispositivos móviles	Pérdida del equipo	Compartición entre conductores
Correo corporativo	Phishing	Falta de capacitación
Infraestructura Cloud	Acceso indebido	Gestión inadecuada de permisos
Red Wifi corporativa	Intrusión	Configuración insegura
Red Wifi visitantes	Acceso a red interna	Segmentación insuficiente
Sistema documental	Eliminación accidental	Permisos excesivos
Backup	Imposibilidad de recuperación	No existen pruebas de restauración
Credenciales	Robo de contraseñas	Políticas de contraseñas débiles
Información financiera	Manipulación	Control insuficiente de accesos
Información logística	Fuga de información	Uso de aplicaciones personales
Servidores	Fallo de hardware	Mantenimiento preventivo limitado
Equipos de usuarios	Malware	Navegación insegura
Equipos de red	Ataques externos	Firmware desactualizado

Analisis y gestión de riesgos

Para evaluar el riesgo de manera estructurada, se adoptará un enfoque semicuantitativo simplificado inspirado en los principios metodológicos de la norma (ISO/IEC 27005 y Magerit.) La valoración del riesgo se calcula multiplicando el factor de Probabilidad (P) por el factor de Impacto (I), asignando escalas numéricas del 1 al 5.

- Escala de Probabilidad: 1: Muy Baja (Raro), 2: Baja (Poco probable), 3: Media (Posible), 4: Alta (Probable), 5: Muy Alta (Casi seguro — eventos ya experimentados de forma recurrente).
- Escala de Impacto: 1: Insignificante, 2: Menor, 3: Moderado, 4: Mayor (Afecta operaciones regionales substancialmente), 5: Catastrófico (Parálisis total del negocio logístico o sanciones legales graves).

El Nivel de Riesgo (R) resultante se clasifica en cuatro cuadrantes:

- Bajo (1 a 4): Riesgo aceptable, requiere monitoreo.
- Medio (5 a 9): Requiere controles preventivos programados.
- Alto (10 a 14): Requiere mitigación prioritaria y asignación presupuestal.
- Crítico (15 a 25): Requiere intervención e implementación inmediata de salvaguardas técnicas.

Metodología de análisis

La gestión de riesgo en la ciberseguridad es un proceso el cual permite identificar, analizar, evaluar y administrar todas aquellas situaciones que puedan afectar todos los activos de la información de una organización. Teniendo en cuenta el caso de Logired Express S.A.S, la verificación de los riesgos se realizó tomando como referencia las prácticas establecidas en la ISO/IEC 27005:2022, la ISO/IEC 27001:2022 y el NIST Cybersecurity Framework 2.0, estas metodologías son las más reconocidas en la administración de riesgos enfocados con seguridad de la información.

Este proceso inicia con la identificación de los activos más críticos dentro de la organización, teniendo como referencia aquellos recursos indispensables para el desarrollo de las actividades principales dentro de la organización. Se analizaron con anterioridad y de forma muy de tallada las a amenazas que pueden afectar los activos, así como las vulnerabilidades identificadas durante el diagnóstico inicial.

Con la información recolectada se inicia con la valoración del riesgo teniendo como consideración dos vulnerabilidades principales.

Con la información obtenida se realizó una valoración del riesgo considerando dos variables principales:

- **Probabilidad:** posibilidad de que una amenaza explote una vulnerabilidad.
- **Impacto:** consecuencias que tendría la materialización del riesgo sobre la organización.

El nivel de riesgo se determinó mediante la combinación de estas variables, clasificándolos en **Bajo**, **Medio**, **Alto** y **Muy Alto**, con el propósito de priorizar su tratamiento.

Criterios de valoración
Probabilidad

Nivel	Descripción
Baja	Es poco probable que el riesgo ocurra.
Media	Puede presentarse ocasionalmente.
Alta	Es probable que ocurra durante la operación.
Muy Alta	Se espera que ocurra si no se implementan controles.

Impacto

Nivel	Descripción
Bajo	Afectación mínima, fácilmente recuperable.
Medio	Interrupción parcial de procesos.
Alto	Afectación significativa de la operación.
Muy Alto	Paralización de procesos críticos, pérdidas económicas y daño reputacional.

Matriz de riesgos

Tabla 4. Matriz de riesgo

Riesgo	*Impacto (I)*	*Probabilidad (P)*	*Nivel (I x P)*	*Clasificación*
R1: Acceso no autorizado a datos de clientes por extravío de dispositivos móviles desprotegidos.	4	5	20	Crítico
R2: Interrupción de la operación de despacho por fallas de conectividad de red o caída del sistema GPS.	4	4	16	Crítico
R3: Intrusión a sistemas internos y secuestro de datos corporativos a través de correos maliciosos (Phishing).	5	3	15	Crítico
R4: Fuga o alteración indebida de inventarios por uso de canales de comunicación personal y equipos propios.	3	4	12	Alto
R5: Imposibilidad de restaurar la operación central por fallas en la integridad de las copias de respaldo.	5	2	10	Alto

Análisis de riesgos

De acuerdo con la matriz de riesgos, se identificó que los riesgos R1, R2 y R3 son los más importantes, ya que fueron clasificados como críticos. Estos riesgos pueden afectar

la información de los clientes, interrumpir la operación logística y comprometer los sistemas de la empresa mediante ataques de phishing.

Los riesgos R4 y R5 fueron clasificados como altos. Aunque su nivel es menor, pueden generar pérdida de información, errores en la operación y dificultades para recuperar los sistemas en caso de un incidente.

En general, el análisis muestra que LogiRed Express S.A.S. depende de sus sistemas de información para desarrollar sus actividades. Por esta razón, es importante implementar controles de seguridad que permitan reducir los riesgos identificados y garantizar la continuidad de la operación.

Politicas y controles de seguridad

La construcción del modelo de seguridad de la información para Logired Express S.A.S. no se plantea como un esquema de imposición restrictiva o puramente teórico, sino como un habilitador estratégico diseñado a partir del diagnóstico empírico de las vulnerabilidades del negocio logístico. La interdependencia de los flujos de información en la cadena de suministro exige que las directrices de seguridad se integren de manera orgánica en el día a día operativo de la empresa, protegiendo la confidencialidad, la integridad y la disponibilidad de los datos de despacho, almacenamiento e inventarios de los clientes.

Este marco estructural de políticas y controles toma como referencia las mejores prácticas del estándar internacional ISO/IEC 27001:2022 y las directrices de implementación de la norma ISO/IEC 27002:2022, adaptando su nivel de exigencia a las capacidades y necesidades de expansión de una organización en crecimiento como Logired, la cual cuenta con centros de distribución regionales interconectados a través de una red híbrida.

Políticas Propuestas

A partir de los resultados obtenidos en el diagnóstico y del análisis de riesgos realizado a LogiRed Express S.A.S., se plantean cinco políticas de seguridad de la información que buscan responder a las principales necesidades identificadas durante la evaluación.

Estas políticas surgen como una medida para corregir las debilidades encontradas en la organización, entre ellas el manejo inadecuado de dispositivos móviles, las fallas en el control de accesos, la falta de un procedimiento para atender incidentes de seguridad y la ausencia de lineamientos para el manejo de la información.

Tabla 5. Políticas de seguridad propuestas para Logired Express S.A.S.

Identificador y Nombre	*Declaración del Objetivo de la Política*	*Riesgos de Ciberseguridad Asociados*
POL-SEC-01: Control de Acceso y Gestión de Identidades	Regular y documentar el acceso a todos los sistemas operativos centrales (ERP, TMS, WMS, nube híbrida), basándose estrictamente en el principio del menor privilegio. Obliga al uso de autenticación multifactor (MFA) y determina que los procesos de baja o desvinculación de personal deben inhabilitar el acceso en un plazo menor a 24 horas.	R1: Acceso no autorizado. R3: Intrusión a sistemas internos (Phishing / Robo de credenciales).
POL-SEC-02: Clasificación y Manejo Seguro de la Información	Clasificar los datos de la organización en cuatro categorías oficiales (Pública, Interna, Confidencial y Restringida), fijando directrices técnicas claras para el almacenamiento, cifrado y transmisión segura de las bases de datos de clientes e inventarios.	R4: Fuga o alteración indebida de inventarios por uso de canales no autorizados.
POL-SEC-03: Seguridad para Dispositivos Móviles y Terminales Portátiles	Definir las condiciones de uso de terminales, teléfonos inteligentes y escáneres asignados a los supervisores de bodega y conductores. Exige el cifrado de almacenamiento completo (Full Disk Encryption) y prohíbe explícitamente el uso compartido de dispositivos sin el registro de relevo correspondiente.	R1: Acceso no autorizado por extravío de dispositivos móviles desprotegidos.
POL-SEC-04: Canales de Comunicación Corporativa y Shadow IT	Prohibir de manera categórica la transmisión de información relacionada con la operación logística, guías de despacho, rutas activas, manifiestos de carga o datos personales.	R4: Fuga o alteración indebida de inventarios.
POL-SEC-05: Gestión y Verificación de	Adoptar e institucionalizar el modelo técnico de respaldo 3-2-1. Exige el uso de almacenamiento de copias inmutables y aisladas de la red principal (air-gapped) y	R5: Imposibilidad de restaurar la operación central por

Copias de Respaldo	obliga a la ejecución trimestral de pruebas prácticas de restauración total de bases de datos.	fallas en integridad de copias.

Controles Propuestos

El siguiente nivel estratégico consiste en traducir las intenciones políticas en controles técnicos y de procedimiento concretos, cuya ejecución reduce cuantitativamente los indicadores de probabilidad e impacto de la matriz de riesgos de Logired.

Controles de seguridad sugeridos para mitigación del riesgo
tabla 6 controles de seguridad

Riesgo Asociado	*Medida de Control Propuesta (ISO 27002 / NIST CSF 2.0)*	*Justificación Técnica y Operativa del Control*
R1: Acceso no autorizado por pérdida de dispositivos móviles.	Despliegue de una solución de Gestión de Dispositivos Móviles (MDM) con cifrado AES-256 forzado.	Centraliza la monitorización de todos los terminales asignados a conductores y supervisores. Facilita el borrado remoto inmediato ante incidentes de pérdida, bloquea la descarga de aplicaciones no oficiales y exige credenciales de acceso robustas obligatorias.
R2: Interrupción de la operación por caída de red o GPS.	Implementación de un esquema SD-WAN con enlaces redundantes LTE/5G y activación del modo "Store and Forward" en aplicativos locales.	Evita que la pérdida de un proveedor principal de fibra en un centro de distribución regional paralice la facturación y el despacho. El modo de almacenamiento local permite a la aplicación móvil de conductores guardar datos del trayecto de forma desconectada y sincronizarlos automáticamente al recuperar señal.
R3: Intrusión a sistemas corporativos mediante Phishing.	Configuración obligatoria de Autenticación de Doble Factor (MFA) para inicios de sesión externos y endurecimiento de políticas de correo (DKIM/SPF/DMARC).	Neutraliza el impacto del Phishing. Aunque un atacante capture de manera exitosa la contraseña de un colaborador usando técnicas de ingeniería social, no podrá acceder a la infraestructura híbrida sin el

		código dinámico generado en el dispositivo físico autorizado.
R4: Fuga de información por uso de herramientas personales.	Habilitación de una plataforma corporativa unificada (ej. Teams/Slack empresarial) bajo directivas DLP (Prevención de Pérdida de Datos).	Reemplaza el uso de herramientas comerciales personales ofreciendo un canal de igual dinamismo, pero auditable y seguro, donde el motor DLP restringe activamente la posibilidad de exportar archivos identificados como confidenciales.
R5: Fallas de restauración de copias de seguridad.	Automatización de rutinas de simulación de restauración en entornos virtuales aislados (Sandbox Recovery Testing).	Elimina la incertidumbre técnica del estado del respaldo. El sistema no solo informa si la copia se completó con éxito, sino que mensualmente monta las bases de datos de clientes e inventarios en un servidor de prueba para certificar que la información es legible y recuperable dentro de las métricas de RTO y RPO exigidas por Logired.

Justificación de las Políticas y Controles en la Reducción del Riesgo

La interconexión estratégica de estas directrices y medidas persigue la maduración del ecosistema tecnológico de Logired Express S.A.S. En primer lugar, la implementación conjunta de la POL-SEC-01 y la POL-SEC-03, complementadas con el control técnico MDM, soluciona de raíz el factor de exposición crítica de la operación en ruta. El conductor ya no representa un punto débil no supervisado, sino un nodo de información seguro cuyo dispositivo móvil está protegido de manera robusta contra el acceso físico de terceros no autorizados, mitigando cualquier vulneración a la Ley 1581 de 2012 por tratamiento indebido de datos personales de remitentes y destinatarios.

En segundo lugar, la adopción de canales de comunicación internos (POL-SEC-04) y herramientas DLP mitiga el riesgo de pérdida de propiedad intelectual u operativa. Al concentrar las comunicaciones de inventarios y rutas logísticas en entornos corporativos, la organización recupera el control sobre su activo de información más valioso, evitando el espionaje corporativo y la fuga no intencionada de datos operativos.

Finalmente, la cultura de verificación de las copias de seguridad (POL-SEC-05 y controles asociados de restauración automatizada) actúa como el último mecanismo de

defensa de la organización. Ante una eventual caída de los servidores o frente a un ataque sofisticado de ransomware que logre superar el resto de las defensas, Logired tendrá la certeza operativa de poder restaurar de manera íntegra e inmediata la base de datos de envíos, garantizando la continuidad de su servicio de transporte y distribución sin incurrir en pérdidas financieras o daños irreparables a la reputación empresarial.

Gestión de incidentes y continuidad del negocio

La creciente dependencia de las tecnologías de la información ha convertido la gestión de incidentes de ciberseguridad en un proceso fundamental para garantizar la continuidad operativa de las organizaciones. En empresas del sector logístico como Logired Express S.A.S., donde la disponibilidad de los sistemas tecnológicos es indispensable para coordinar el transporte, el almacenamiento y la distribución de mercancías, un incidente de seguridad puede generar importantes afectaciones operativas, económicas y reputacionales.

La gestión de incidentes comprende el conjunto de procedimientos destinados a identificar, analizar, contener, erradicar y recuperar los servicios afectados por un evento de seguridad. Su finalidad es reducir el impacto sobre la organización y restablecer las operaciones en el menor tiempo posible.

Actualmente, el diagnóstico realizado evidenció que Logired Express S.A.S. no cuenta con un procedimiento formal documentado para la gestión de incidentes de seguridad, situación que incrementa los tiempos de respuesta y dificulta la coordinación entre las diferentes áreas involucradas.

Por esta razón, se propone la implementación de un proceso estructurado que permita responder de manera eficiente frente a incidentes relacionados con ataques cibernéticos, pérdida de información, fallas tecnológicas o interrupciones de los servicios críticos.

Tabla 7 Gestión de incidentes y continuidad del negocio

Incidente	*Descripción*	*Impacto*
Ataque de phishing	Recepción de correos fraudulentos dirigidos a colaboradores.	Robo de credenciales y acceso no autorizado.
Ataque de ransomware	Cifrado malicioso de servidores y estaciones de trabajo.	Interrupción total de la operación logística.
Robo de dispositivo móvil	Pérdida o hurto de equipos utilizados por conductores o supervisores.	Exposición de información corporativa.
Caída del ERP	Indisponibilidad del sistema administrativo y financiero.	Suspensión de procesos críticos.
Falla del sistema GPS	Imposibilidad de monitorear la ubicación de los vehículos.	Retrasos operativos y reclamaciones de clientes.
Pérdida de conectividad	Interrupción del servicio de Internet.	Afectación de la comunicación entre sedes.
Eliminación accidental de información	Borrado involuntario de archivos críticos.	Pérdida de datos operativos.
Fuga de información	Divulgación no autorizada de información corporativa.	Daño reputacional y sanciones legales.
Malware	Infección de equipos por software malicioso.	Disminución del rendimiento y riesgo de propagación.
Ataque al portal web	Intento de afectar la disponibilidad o integridad del portal para clientes.	Interrupción del servicio y pérdida de confianza.

Plan de respuesta a incidentes

Se propone la adopción de un proceso basado en el ciclo de respuesta a incidentes recomendado por el **NIST**, compuesto por las siguientes fases:

Tabla 8. Plan de respuesta

Fase	*Acción*
Preparación	Definir roles, responsabilidades, herramientas y procedimientos para la atención de incidentes.
Identificación	Detectar el incidente mediante herramientas de monitoreo y reportes de usuarios.
Contención	Limitar la propagación del incidente aislando sistemas comprometidos.
Erradicación	Eliminar la causa del incidente, como malware, accesos no autorizados o configuraciones inseguras.
Recuperación	Restaurar los servicios afectados utilizando respaldos verificados y monitorear el correcto funcionamiento.
Lecciones aprendidas	Documentar el incidente, identificar oportunidades de mejora y actualizar procedimientos.

Equipo de respuesta a incidentes

Se recomienda conformar un **Equipo de Respuesta a Incidentes de Seguridad (CSIRT interno)** integrado por representantes de las principales áreas de la organización:

Cargo	*Responsabilidad*
Gerente de TI	Coordinar la respuesta técnica al incidente.
Administradores de infraestructura	Contener y recuperar los sistemas afectados.
Analistas de soporte	Atender incidentes reportados por los usuarios.
Dirección de Operaciones	Garantizar la continuidad de los procesos logísticos.

Talento Humano	Gestionar la comunicación con los colaboradores cuando sea necesario.
Gerencia General	Aprobar decisiones estratégicas durante incidentes críticos.

Continuidad del negocio

La continuidad del negocio tiene como objetivo garantizar que la organización pueda mantener sus procesos esenciales durante una interrupción y recuperarse en el menor tiempo posible. Considerando la naturaleza de Logired Express S.A.S., los procesos que requieren mayor prioridad de recuperación son:

1. Plataforma ERP.
2. Plataforma TMS.
3. Plataforma WMS.
4. Sistema GPS.
5. Portal web para clientes.
6. Plataforma de respaldo.
7. Correo electrónico corporativo.

La recuperación de estos servicios permitirá restablecer rápidamente la capacidad operativa de la empresa.

Estrategias de continuidad

Con el propósito de fortalecer la resiliencia organizacional, se proponen las siguientes acciones:

- Implementar un **Plan de Continuidad del Negocio (BCP)** documentado y aprobado por la alta dirección.
- Diseñar un **Plan de Recuperación ante Desastres (DRP)** para los sistemas críticos.
- Realizar pruebas semestrales de recuperación de respaldos.

- Mantener copias de seguridad cifradas y almacenadas fuera del sitio principal.
- Implementar redundancia en los enlaces de Internet de los centros de distribución.
- Establecer acuerdos de nivel de servicio (SLA) con proveedores tecnológicos.
- Definir tiempos objetivos de recuperación (RTO) y puntos objetivos de recuperación (RPO) para los sistemas críticos.
- Ejecutar simulacros periódicos de atención a incidentes y continuidad del negocio.

Recomendaciones para fortalecer la continuidad

Para mejorar la capacidad de respuesta y recuperación, se recomienda que Logired Express S.A.S.:

- Formalice un procedimiento de gestión de incidentes alineado con estándares internacionales.
- Designe responsables específicos para cada fase del proceso.
- Establezca canales de comunicación para incidentes críticos.
- Documente y analice cada incidente ocurrido.
- Monitoree continuamente la infraestructura tecnológica mediante herramientas de seguridad.
- Integre la gestión de incidentes con los procesos de gestión de riesgos y continuidad del negocio.

Estas acciones contribuirán a minimizar los tiempos de inactividad y reducir el impacto de futuros incidentes sobre la operación logística.

Cultura organizacional en ciberseguridad

Podemos decir que la ciberseguridad no depende exclusivamente de la implementación de herramientas tecnológicas, depende de los compromisos de los colaboradores quienes son los que interactúan diariamente con la información y los sistemas de la organización La cultura organizacional es un elemento de prioridad a fortalecer para ayudar a la protección de los activos de la información y ayudar a reducir los riesgos asociados al factor humano

Es claro que una cultura de ciberseguridad se considera solida cuando se promueve el conocimiento colectivo dentro de la organización. Generar sentido de pertenecía y participación dentro de los colaboradores en la protección de la información de la organización ayuda a detectar posibles fallas. Esto nos dará como resultado que cada colaborados va a comprender de manera más eficaz todos los riesgos asociados al utilizar tecnologías de la información, generando que los colaboradores conozcan políticas de seguridad y adopten buenas prácticas en desarrollo de sus labores diarias.

Durante el diagnóstico realizado a Logired Express S.A.S se evidencio que, aunque la organización dispone de unas herramientas de la información bien estructurada y robusta, se dejó en evidencia que existe debilidades de concientización de los colaboradores y la adopción de prácticas seguras. esta novedad incrementa las probabilidades de incidente asociados a los errores humanos. El uso inadecuado constante de las herramientas de la información y a la resistencia a la implementación de nuevos controles.

Por esta razón se debe de implementar una estrategia integral que fortalezca la cultura organizacional dentro de los colaboradores, esto mediante un programa de capacitación acompañado de campañas de sensibilización y un mecanismo que incentive la participación activa de todos los colaboradores en gestión de la ciberseguridad organizacional.

Tabla 9. Hallazgos organizacionales

Situación observada	*Riesgo asociado*
Los empleados consideran que la seguridad es responsabilidad exclusiva del área de TI.	Bajo compromiso organizacional con la ciberseguridad.
Se prioriza la rapidez en las operaciones sobre el cumplimiento de controles de seguridad.	Incremento de errores operativos y vulnerabilidades.
Uso frecuente de aplicaciones personales de mensajería para compartir información laboral.	Fuga de información y pérdida de confidencialidad.
Desconocimiento de los riesgos asociados al uso de dispositivos móviles corporativos.	Pérdida o exposición de información sensible.
Capacitaciones esporádicas en seguridad de la información.	Mayor probabilidad de ataques de ingeniería social y phishing.
Los incidentes de seguridad no siempre son reportados oportunamente.	Retrasos en la respuesta y aumento del impacto de los incidentes.
Resistencia al cambio frente a nuevos controles tecnológicos.	Dificultad para implementar políticas y medidas de seguridad.
Diferencias en los procedimientos entre sedes.	Inconsistencias en la aplicación de controles de seguridad.

Tabla 10. Recomendaciones de mejora

Hallazgo	*Recomendación*
Baja participación del personal	Desarrollar una cultura de corresponsabilidad en ciberseguridad.
Falta de capacitación	Implementar un programa anual de formación y actualización.
Uso de aplicaciones personales	Adoptar plataformas corporativas autorizadas para la comunicación.
Desconocimiento de amenazas	Realizar simulaciones periódicas de ataques de phishing e ingeniería social.
Ausencia de campañas permanentes	Diseñar campañas mensuales de sensibilización sobre buenas prácticas de seguridad.
Procesos diferentes entre sedes	Estandarizar procedimientos y políticas en toda la organización.
Resistencia al cambio	Involucrar a los colaboradores en la implementación de nuevas medidas de seguridad.
Falta de reporte de incidentes	Establecer canales simples y confidenciales para el reporte de incidentes.

Estrategias para fortalecer la cultura organizacional

Con el fin de fortalecer la cultura de ciberseguridad en Logired Express S.A.S se debe de implementar la siguiente estrategia que ayudar de forma efectiva a esta organización.

Capacitaciones constantes
Implementar un plan anual o semestral de formación enfocado a todos los colaboradores de la organización, enfocados en los siguientes contenidos:

- Protección de datos personales.
- Gestión de contraseñas.
- Seguridad de la información.
- Uso seguro del correo electrónico corporativo.
- Ingeniería social.

- Phishing.
- Protección de dispositivos móviles corporativos.
- Manejo seguro de la información.

las capacitaciones deben de estar estandarizadas a las áreas de los colaboradores y adicional deben de hacerse de forma periódica y dinámica para cada a rea de la compañía.

Campañas de sensibilización

Se complementas las capacitaciones con campañas internas para los colaboradores en general:

- Carteleras informativas.
- Videos educativos.
- Simulacros de phishing.
- Jornadas de concientización.

Estas actividades mantienen enfocados a los colaboradores en la importancia de la ciberseguridad en el desarrollo de las actividades diarias dentro de la organización.

Fortalecimiento de liderazgo organizacional

La organización en cabezada por la alta gerencia promoverá activamente la cultura Logired seguro mediante el apoyo y ejemplo de las buenas prácticas en ciberseguridad también implementará recursos para la implementación de nuevas a actualizaciones dentro del programa de ciberseguridad.

Indicadores de seguimiento

Para evaluar la efectividad de las estrategias implementadas se debe de establecer indicadores como:

- Indicador de colaboradores capacitados.
- Tiempo de respuesta a incidentes.
- Número de incidentes reportados.
- Resultado se simulación de phishing.
- Cumplimento de políticas de seguridad.
- Calidad de la actualización de los activos.

Estos indicadores nos permitirán verificar el nivel de madures de los colaboradores y de la organización en las acciones de mejora continua establecidos para la ciberseguridad de Logired Express S.A.S.

Logros esperados

La implementación de cada una de las recomendaciones nos dará como resultado:

- Reducir los errores humanos.
- Disminuir de forma acertada la probabilidad de ataques exitosos hacia la organización.
- Aumentar los conocimientos de los colaboradores.
- Fortalecer el cumplimento de las políticas de ciberseguridad dentro de la organización.
- Aumento de la capacidad de respuesta ante incidentes.
- Fortalecer el cumplimento de los estándares internacionales en ciberseguridad.
- Aumentar la confianza de nuestro clientes y aliados estratégicos.

Una cultura organizacional solida pude facilitar la implementación de nuevas tecnologías de analítica de datos que se pueden tener en los planes de expansión de la organización.

Conclusiones

El análisis realizado a **LogiRed Express S.A.S.** evidenció que la organización cuenta con una infraestructura tecnológica moderna y una alta dependencia de los sistemas de información, lo que convierte la ciberseguridad en un factor estratégico para la continuidad del negocio y la protección de los activos críticos.

El diagnóstico permitió identificar vulnerabilidades en la gestión de accesos, dispositivos móviles, respaldos y ausencia de procedimientos formales para incidentes, lo que incrementa la probabilidad de riesgos que afectan la disponibilidad de los servicios, la integridad de la información y la confianza de los clientes.

La aplicación de metodologías de análisis de riesgos basadas en estándares internacionales (ISO/IEC 27001, ISO/IEC 27002 y NIST Cybersecurity Framework) permitió establecer prioridades claras y evidenciar que amenazas como phishing, ransomware, robo de credenciales, fuga de información y errores humanos representan los escenarios de mayor impacto. La adopción de controles preventivos, correctivos y de diagnóstico fortalecerá la seguridad de la información y la resiliencia organizacional.

Finalmente, se identificó la necesidad de consolidar una cultura organizacional enfocada en la ciberseguridad. Dado que gran parte de los riesgos tienen origen en el factor humano, resulta indispensable establecer programas permanentes de capacitación, campañas de sensibilización y estrategias de comunicación que promuevan el compromiso de los colaboradores. La implementación de estas recomendaciones permitirá mejorar los estándares de seguridad, optimizar la gestión de riesgos tecnológicos y reforzar la confianza de los clientes en la organización
.

Referencias

Normativa internacional

- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
- International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. ISO.
- International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. ISO.
- International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems*. ISO.

Marco de referencia

- National Institute of Standards and Technology. (2024). *Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce.
- National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*. NIST.

Legislación colombiana

- Congreso de Colombia. (2009). *Ley 1273 de 2009*. Por medio de la cual se modifica el Código Penal y se crea el bien jurídico de la protección de la información y de los datos.
- Congreso de Colombia. (2012). *Ley 1581 de 2012*. Régimen General de Protección de Datos Personales.
- Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013*. Reglamentación parcial de la Ley 1581 de 2012.

Bibliografía

- Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Cengage Learning.
- Stallings, W. (2020). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley.
- ISACA. (2020). *COBIT 2019 Framework: Governance and Management Objectives*. ISACA.
- ENISA. (2023). *Threat Landscape Report*. European Union Agency for Cybersecurity.