



TRABAJO DE GRADO
Opción Seminario.

INFORME TÉCNICO
CASO DE LA EMPRESA TRANSMOVIL NACIONAL S.A.S.

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

Nombre de la estudiante autora del trabajo de grado.

Lina Marcela Otalvaro Garcia

Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Tabla de Contenidos

Resumen.....	3
Marco conceptual y normativo	4
Conceptos fundamentales de ciberseguridad	4
Marco normativo.....	6
Marco contextual	8
Descripción de la organización.....	8
Problemática identificada.....	9
Identificación y análisis de activos	10
Inventario de activos	10
Análisis de amenazas y vulnerabilidades.....	13
Análisis y gestión de riesgos.....	16
Metodología de análisis	16
Matriz de riesgos.....	16
Análisis de riesgos prioritarios.....	17
Políticas y controles de seguridad.....	18
Políticas propuestas.....	18
Controles propuestos.....	19
Justificación de la estrategia de controles	20
Gestión de incidentes y continuidad del negocio.....	20
Incidentes potenciales	20
Plan básico de respuesta.....	21
Estrategia para la continuidad del negocio	22
Cultura organizacional en ciberseguridad.....	23
Hallazgos organizacionales.....	23
Recomendaciones de mejora.....	24
Fortalecimiento de la cultura organizacional.....	25
Conclusiones	27
Referencias.....	29

Resumen

El presente informe técnico se desarrolla en el marco del seminario de grado del programa de Ingeniería de Sistemas de la Corporación Universitaria Remington, y tiene como finalidad analizar la situación actual de seguridad de la información en la empresa TransMovil Nacional S.A.S., organización dedicada al transporte intermunicipal de pasajeros en Colombia.

TransMovil Nacional S.A.S. es una compañía con más de treinta años de trayectoria en el sector transporte, que opera a nivel nacional conectando ciudades principales, municipios intermedios y zonas rurales. La empresa cuenta con una flota de 180 vehículos, atiende aproximadamente 1.200.000 pasajeros al año y emplea cerca de 480 colaboradores en diversas áreas operativas, administrativas y tecnológicas.

Durante los últimos años, la organización ha venido fortaleciendo sus canales digitales mediante plataformas de venta de tiquetes en línea, aplicaciones móviles y sistemas de seguimiento de flota en tiempo real. Sin embargo, este crecimiento tecnológico no ha ido acompañado de una actualización proporcional en las políticas y procedimientos de seguridad, lo que ha generado una serie de vulnerabilidades que merecen ser analizadas con profundidad.

El propósito de este informe es identificar los principales riesgos de ciberseguridad que enfrenta la organización, evaluar sus activos de información más críticos, analizar las amenazas y vulnerabilidades presentes, y proponer medidas de control que contribuyan a fortalecer la postura de seguridad de la empresa. Para ello, se aplicaron conceptos fundamentales de ciberseguridad, se revisó el marco normativo colombiano aplicable y se realizó un análisis sistemático de la información recopilada durante el diagnóstico inicial.

Los resultados más relevantes evidencian problemas significativos en áreas como la gestión de credenciales, la clasificación de información, la concientización del personal y la gestión de incidentes. Asimismo, se identificaron activos críticos que requieren protección prioritaria, así como amenazas que podrían materializarse con impactos considerables para la continuidad operativa de la organización.

Palabras clave

Ciberseguridad; gestión de riesgos; activos de información; seguridad de la información; políticas de seguridad.

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

Para abordar de manera adecuada el análisis de seguridad en TransMovil Nacional S.A.S., es necesario comprender una serie de conceptos teóricos que sirven como base para la evaluación de riesgos y la implementación de controles. En primer lugar, es importante distinguir entre ciberseguridad y seguridad de la información ya que, aunque están estrechamente relacionados, no son términos idénticos.

La ciberseguridad puede entenderse como el conjunto de medidas, prácticas tecnológicas diseñadas para proteger sistemas, redes, dispositivos y datos contra ataques, daños o accesos no autorizados en el entorno digital. Según el CONPES 3995 de Colombia, la seguridad digital busca desarrollar la confianza digital mediante el fortalecimiento de la seguridad y la reducción de vulnerabilidades en el ciberespacio (*Acevedo, 2024*). Por su parte, la seguridad de la información es un concepto más amplio que abarca la protección de la información en cualquiera de sus formas, ya sea digital, física o verbal.

De acuerdo con la ISO 27001, la Seguridad de la Información se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los sistemas que la procesan (*CIBERSEGURIDAD, 2015*). Estos tres pilares, conocidos como la tríada CIA (por sus siglas en inglés: Confidentiality, Integrity, Availability), constituye cualquier estrategia de seguridad.

La confidencialidad se refiere a la garantía de que la información solo sea accesible por aquellas personas, sistemas o procesos que estén debidamente autorizados (*finales, s.f.*). en el contexto de TransMovil, esto aplica directamente a la información personal de los pasajeros, como datos de identificación, historiales de viaje y métodos de pago, que no deben estar disponibles para personas no autorizadas.

La integridad implica asegurar que la información sea exacta, completa y no haya sido alterada de manera no autorizada (*Fortinet, s.f.*). cuando se habla de integridad en el transporte de pasajeros, esto se traduce en garantizar que los itinerarios, reservas programación de servicios y los registros operacionales no sean modificados indebidamente, ya que cualquier alteración podría generar graves problemas operativos.

Finalmente, la disponibilidad hace referencia a que la información y los sistemas estén accesibles y utilizables cuando sean requeridos por los usuarios autorizados (*Tecnología, 2021*). En el caso de TransMovil, esto resulta especialmente crítico dado que la empresa depende cada vez más de plataformas tecnológicas para operar, incluyendo la venta de tiquetes en línea, el sistema GPS de monitoreo vehicular y la plataforma de recaudo electrónico.

Los activos de información son todos aquellos elementos que tienen valor para la organización y que contribuyen al cumplimiento de sus objetivos (*Amaya, 2020*). Estos activos pueden ser tangibles, como servidores, computadores y dispositivos móviles, o intangibles, como la información de pasajeros, las bases de datos operacionales, el conocimiento del personal y la reputación corporativa.

Una amenaza se define como cualquier evento o circunstancia que puede causar daño a un activo de información, ya sea de origen natural, humano o técnico. Las amenazas pueden ser intencionales, como un ataque de phishing o un acceso no autorizado, o accidentales, como una falla tecnológica o un error humano. Según reportes especializados, América Latina registra más de 2.200 ciberataques por minuto, lo que evidencia la magnitud del problema en la región (*Estrada, s.f.*).

Una vulnerabilidad es una debilidad o falla en un sistema, proceso o control que puede ser aprovechada por una amenaza para comprometer la seguridad de un activo. Las vulnerabilidades pueden ser técnicas, como una falla de software, o humanas, como la falta de capacitación o incumplimiento de procedimientos.

El riesgo se entiende como la combinación de la probabilidad de que ocurra un evento adverso y el impacto que este tendría sobre los activos de la organización. La gestión de riesgos implica identificar, evaluar y tratar los riesgos de manera sistemática para reducirlos a niveles aceptables.

Los controles de seguridad son las medidas implementadas para prevenir, detectar o corregir los efectos de las amenazas sobre los activos de información. Estos controles pueden ser de naturaleza técnica, como firewalls y sistemas de autenticación multifactor; organizacionales, como políticas y procedimientos; o físicos, como sistemas de videovigilancia y control de acceso.

La gestión de incidentes es el proceso mediante el cual una organización identifica, responde y se recupera de eventos que comprometen la seguridad de la información. Un incidente puede ser un ataque cibernético, una falla tecnológica, una pérdida de equipos o cualquier situación que ponga en riesgo los activos de la organización. Finalmente, la continuidad del negocio se refiere a la capacidad de una organización para mantener o restablecer sus operaciones esenciales después de un evento disruptivo, garantizando que los servicios críticos sigan disponibles para los clientes y usuarios.

Marco normativo

Para el análisis del caso de TransMovil Nacional S.A.S., es fundamental considerar el marco normativo colombiano que regula la protección de datos, la seguridad digital y los delitos informáticos. La siguiente tabla presenta las principales normas y estándares aplicables:

Tabla 1. Normatividad aplicable.

<i>Norma o estándar</i>	<i>Propósito</i>	<i>Aplicabilidad en la organización</i>
Ley 1581 de 2012	Establecer las disposiciones generales para la protección de datos personales en Colombia, regulando el tratamiento de información personal por parte de entidades públicas y privadas (<i>Distrital, RÉGIMEN LEGAL DE BOGOTÁ D.C., 2012</i>).	Totalmente aplicable, ya que TransMovil maneja datos personales de aproximadamente 1.200.000 pasajeros al año, incluyendo, reservas, itinerarios y métodos de pago.
Ley 1273 de 2009	Modificar el código penal colombiano para crear nuevos tipos penales relacionados con delitos informáticos y la protección de la información y los datos (<i>Distrital, RÉGIMEN LEGAL DE BOGOTÁ D.C., 2009</i>).	Aplicable en caso de accesos no autorizados, daños a sistemas informáticos, interceptación ilegal de datos o cualquier conducta que afecte la integridad de los sistemas de la organización.
CONPES 3995 de 2020	Establecer la Política Nacional de Confianza y Seguridad Digital en Colombia, con el objetivo de fortalecer las capacidades de seguridad digital y reducir vulnerabilidades en el ciberespacio (<i>comunicaciones, 2025</i>).	Aplicable como referente estratégico para que la organización alinee sus prácticas de seguridad con los lineamientos nacionales de confianza digital.

Decreto 1377 de 2013	Reglamentar parcialmente la Ley 1581 de 2012, estableciendo requisitos específicos para el tratamiento de datos personales, incluyendo la obtención de autorización y la implementación de medidas de seguridad.	Aplicable para garantizar que TransMovil cumpla con los requisitos técnicos y administrativos para el manejo de datos de pasajeros y colaboradores.
ISO/IEC 27001	Definir los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI) basado en buenas prácticas internacionales (NYCE, s.f.).	Aplicable como estándar de referencia para que la organización implemente un sistema estructurado de gestión de seguridad, alineado con las mejores prácticas globales.

La Ley 1581 de 2012 resulta especialmente relevante para TransMovil Nacional, ya que la empresa maneja grandes volúmenes de información personal de pasajeros, lo que la convierte en responsable del tratamiento de datos personales según la normatividad de Colombia (*Distrital, RÉGIMEN LEGAL DE BOGOTÁ D.C., 2012*). El incumplimiento de esta ley puede generar sanciones económicas significativas por parte de la Superintendencia de Industria y Comercio, además de afectar la reputación de la empresa.

Por parte la Ley 1273 de 2009 tipifica conductas delictivas relacionadas con el acceso abusivo a sistemas informáticos, la obtención indebida de datos, el daño informático y la interpretación ilegal de comunicaciones (*T., s.f.*). Esta norma resulta aplicable ante situaciones como el evento 1 del caso, donde se detectaron intentos de acceso no autorizado a sistemas corporativos.

El CONPES 3995 de 2020 establece un marco estratégico para que las organizaciones colombianas fortalezcan sus capacidades de seguridad digital (*digwatch, 2020*). Este documento reconoce que la inversión en ciberseguridad no solo protege los activos de la empresa, sino que también fortalece la confianza de los clientes y garantiza el cumplimiento normativo (*Software, s.f.*).

La implementación de estándares internacionales como la ISO 27001 permite a las organizaciones adoptar un enfoque sistemático para la gestión de riesgos de seguridad de la información (*NQA, s.f.*). En el caso de TransMovil, este estándar serviría como guía para estructurar políticas, procedimientos y controles que respondan de manera integral a las vulnerabilidades identificadas durante el diagnóstico inicial.

Marco contextual

Descripción de la organización

TransMovil Nacional S.A.S. es una empresa colombiana dedicada al transporte terrestre intermunicipal de pasajeros, con más de treinta años de experiencia en el mercado. La organización opera rutas en diferentes departamentos del país, conectando ciudades principales, municipios intermedios y zonas rurales, lo que la convierte en un actor relevante dentro del sistema de transporte nacional.

La empresa cuenta con una flota de 180 vehículos compuesta por sus buses, busetas y microbuses, con los cuales atiende aproximadamente 1.200.000 pasajeros al año. Para sostener esta operación, TransMovil dispone cerca de 480 colaboradores distribuidos en diversas áreas, incluyendo conductores, personal administrativo, despachadores, personal de tecnología, personal operativo y directivos.

En cuanto a su estructura organizacional, la empresa cuenta con doce áreas principales: gerencia general, dirección operativa, dirección comercial, tecnología y sistemas, gestión de flota, despacho y control operacional, atención al cliente, talento humano, compras y contratación, contabilidad y finanzas, seguridad física y mantenimiento vehicular.

Los procesos principales de la organización incluyen la venta de tiquetes (presenciales, telefónicos, digitales), la gestión de pasajeros (información personal, reservas, itinerarios), la gestión de flota (programación, disponibilidad y seguimiento de vehículos), el monitoreo operacional (supervisión de rutas, tiempos de viaje y ubicación de vehículos), la atención al cliente y la gestión financiera.

En términos de infraestructura tecnológica, TransMovil dispone cerca de 170 computadores de escritorio, 55 computadores portátiles, plataforma de venta de tiquetes en línea, aplicación móvil para pasajeros, sistema ERP empresarial, sistema de gestión de flota, sistema GPS para monitoreo vehicular, sistema CRM para atención al cliente, plataforma de recaudo electrónico, correo electrónico corporativo, plataforma de respaldo de información, infraestructura híbrida local y en la nube, red WiFi corporativa, red wifi para pasajeros en terminales principales, sistema de video vigilancia y plataforma de monitoreo operacional.

El área de tecnología está conformada por un director de tecnología, un administrador de infraestructura, un administrador de base de datos, tres analistas de soporte, un desarrollador de software y un analista de seguridad informática. Esta estructura resulta relativamente pequeña considerando la magnitud de la operación y la criticidad de los sistemas tecnológicos para el negocio.

Problemática identificada

A partir del diagnóstico inicial realizado por una firma consultora especializada, se identificaron múltiples situaciones que evidencian una postura de seguridad de la información deficiente en TransMovil Nacional S.A.S. estas situaciones pueden agruparse en varias categorías que revelan problemas estructurales.

En primer lugar, se observaron problemas en la gestión de accesos y credenciales. Algunos despachadores comparten credenciales de acceso para agilizar operaciones durante horarios de alta demanda, lo que anula la trazabilidad de las acciones realizadas en los sistemas. Adicionalmente, existen usuarios con privilegios superiores a los requeridos por sus funciones actuales, y no todos los accesos administrativos utilizan autenticación multifactor. También se identificaron cuentas activas pertenecientes a excolaboradores, lo que representa un riesgo significativo de acceso no autorizado.

En segundo lugar, se identificaron deficiencias en la gestión de la información. No existe una política formal de clasificación de la información, lo que impide establecer niveles adecuados de protección según la sensibilidad de los datos. Algunas terminales aplican procedimientos diferentes para el manejo de la información sensible, generando inconsistencias operativas. Adicionalmente, no existe un inventario actualizado de activos de la información ni una estrategia formal de gobierno de datos.

En tercer lugar, se observaron problemas técnicos y de infraestructura. Algunos equipos utilizados en terminales presentan retrasos en la instalación de actualizaciones de seguridad, lo que los expone a vulnerabilidades conocidas. Algunos dispositivos móviles corporativos utilizados por supervisores no cuentan con mecanismos robustos de protección, y no existe una política formal para el uso seguro de los dispositivos y sistemas GPS.

En cuarto lugar, se identificaron problemas en la gestión de incidentes y continuidad. No existe un procedimiento formal para la gestión de incidentes de seguridad, y los respaldos, aunque se realizan regularmente, no cuentan con pruebas documentadas recientes de recuperación.

Finalmente, se evidenciaron problemas culturales y de concientización. Muchos empleados consideran que la seguridad de la información es responsabilidad exclusiva del área de tecnología, algunos colaboradores utilizan aplicaciones de mensajería personal para compartir información operativa, y no se realizan campañas periódicas de sensibilización sobre ciberseguridad. Las capacitaciones sobre seguridad son esporádicas y algunos incidentes menores no son reportados oportunamente.

Durante los últimos tres años, la organización ha experimentado cinco eventos significativos relacionados con la seguridad: un correo electrónico fraudulento seguido de intentos de acceso no autorizado, una falla tecnológica que afectó la venta de tiquetes en

línea durante un fin de semana de alta demanda, el extravío de un dispositivo móvil corporativo con la información operativa, una interrupción de conectividad que afectó la transmisión de información desde dispositivos GPS, y un acceso no autorizado a información operacional utilizando credenciales compartidas.

Esta problemática justifica plenamente el desarrollo del presente informe, ya que la combinación de vulnerabilidades técnicas, deficiencias procedimentales y una cultura organizacional débil en materia de seguridad crea un escenario de alto riesgo para la continuidad operativa de la empresa y la protección de la información de sus pasajeros y colaboradores.

Identificación y análisis de activos

Inventario de activos

Para realizar una adecuada gestión de riesgos, es fundamental identificar y clasificar los activos de información más relevantes de la organización. La siguiente tabla presenta los principales activos identificados en TransMovil Nacional S.A.S., junto con su tipo, descripción y nivel de criticidad.

Tabla 2. Inventario de activos

<i>Activo</i>	<i>Tipo</i>	<i>Descripción</i>	<i>Criticidad</i>
Base de datos de pasajeros	Información	Contiene datos personales, historiales de viaje, información de contacto y métodos de pago de aproximadamente 1.200.000 pasajeros anuales.	Alta
Plataforma de venta de tiquetes en línea	Software/Hardware	Sistema que permite la comercialización digital de tiquetes, procesando transacciones y reservas en tiempo real.	Alta

Sistema de gestión de flota y GPS	Software/Hardware	Plataforma que controla la programación, disponibilidad y seguimiento en tiempo real de los 180 vehículos de la flota.	Alta
Sistema ERP empresarial	Software	Sistema integrado que gestiona procesos administrativos, financieros, de talento humano y operaciones de la organización.	Alta
Aplicación móvil para los pasajeros	Software	Herramienta digital que permite a los usuarios consultar rutas, compra de tiquetes y hacer seguimiento de sus viajes.	Media – Alta
Plataforma de recaudo electrónico	Software/Hardware	Sistema que administra los pagos, recaudos y transacciones financieras asociadas a la operación de transporte.	Alta
Correo electrónico corporativo	Software/Servicio	Plataforma de comunicación oficial utilizada por los 480 colaboradores para comunicación interna y externa.	Media
Infraestructura de servicio y red	Hardware	Equipos de cómputo, servidores locales, dispositivos de red y elementos de conectividad que soportan la operación tecnológica.	Alta

Dispositivos móviles corporativos	Hardware	Computadores portátiles y dispositivos móviles utilizados por supervisores y personal de campo con información operativa.	Media
Información operacional y de rutas	Información	Datos relacionados con programaciones de servicios, rutas, itinerarios, tiempos de viaje y novedades operativas.	Alta
Credenciales de acceso y contraseñas	Información	Credenciales de autenticación que permiten el acceso a sistemas corporativos por parte de colaboradores.	Alta
Plataforma de respaldo de información	Software/Hardware	Sistema encargado de realizar copias de seguridad de la información crítica de la organización.	Alta

La justificación de los activos más importantes se fundamenta en su impacto directo sobre la operación del negocio y la protección de información sensible. La base de datos de pasajeros es sin duda uno de los activos más críticos, no solo por el volumen de información personal que contiene, sino también por las obligaciones legales que impone la Ley 1581 de 2012 respecto al tratamiento de datos personales. Un compromiso de esta base de datos podría generar sanciones económicas, demandas legales y un daño reputacional severo.

La plataforma de venta de tiquetes en línea es crítica porque representa un canal fundamental de generación de ingresos para la organización. El Evento 2 demuestra como una falla en este sistema puede generar múltiples reclamaciones de usuarios y afectaciones operativas significativas, especialmente durante periodos de alta demanda.

El sistema de gestión de flota y GPS es esencial para la operación diaria de la empresa. El Evento 4 evidencia como una interrupción en este sistema puede dejar a la organización sin visibilidad en tiempo real de parte de su flota durante varias horas, lo que compromete la seguridad de los pasajeros y la eficiencia operativa.

El sistema ERP empresarial es crítico porque integra múltiples procesos de la organización. Un compromiso de este sistema podría afectar simultáneamente áreas como contabilidad, talento humano, compras y operaciones, generando un impacto transversal en la empresa.

La plataforma de recaudo electrónico maneja transacciones financieras directas, lo que la convierte en un activo de alta criticidad desde la perspectiva de integridad y disponibilidad. Cualquier alteración o interrupción en este sistema podría generar pérdidas económicas y problemas de conciliación financiera.

Finalmente, la información operacional y de rutas es fundamental para la toma de decisiones estratégicas y la planificación de servicios. El Evento 3 demostró cómo la pérdida de un dispositivo con esta información puede comprometer la seguridad operacional de la empresa.

Análisis de amenazas y vulnerabilidades

Una vez identificados los activos más críticos de la organización, es necesario analizar las amenazas que podrían afectarlos y las vulnerabilidades que podrían ser explotadas. La siguiente tabla presenta el análisis de amenazas y vulnerabilidades para los principales activos identificados.

Tabla 3. Amenazas y vulnerabilidades

<i>Activo</i>	<i>Amenaza</i>	<i>Vulnerabilidad</i>
Base de datos de pasajeros	Acceso no autorizado por actores externos o internos	Credenciales compartidas entre colaboradores, privilegios excesivos, cuentas activas de excolaboradores, falta de autenticación multifactor en accesos administrativos.
Base de datos de pasajeros	Phishing o ingeniería social dirigida a colaboradores	Desconocimiento de riesgos, confianza excesiva en comunicaciones externas, falta de campañas periódicas de sensibilización.
Plataforma de venta de tiquetes en línea	Ataques de denegación de servicio	Dependencia creciente de plataformas tecnológicas, falta de planes de contingencia documentados.

Plataforma de venta de tiquetes en línea	Falla tecnológica o errores de software	Retrasos en instalación de actualizaciones de seguridad, infraestructura que crece más rápido que los controles.
Sistema de gestión de flota y GPS	Interrupción de conectividad o interferencia de señal	Dependencia de conectividad externa, falta de redundancia en comunicaciones.
Sistema de gestión de flota y GPS	Pérdida o robo de dispositivos móviles con información operativa	Dispositivos sin mecanismos robustos de protección, falta de política formal para uso seguro de dispositivos.
Sistema ERP empresarial	Acceso no autorizado mediante credenciales comprometidas	Credenciales compartidas, falta de autenticación multifactor, cuentas de excolaboradores activos.
Sistema ERP empresarial	Malware o ransomware	Equipos con actualizaciones de seguridad desactualizadas, uso de aplicaciones de mensajería personal para compartir información operativa.
Dispositivos móviles corporativos	Pérdida o robo físico	Falta de mecanismos robustos de protección, ausencia de políticas de cifrado y borrado remoto.
Información operacional	Acceso no autorizado por personal interno	Credenciales compartidas, falta de clasificación de información, procedimientos inconsistentes entre terminales.
Plataforma de respaldo	Falla en recuperación de información	Ausencia de pruebas documentadas de recuperación, respaldo realizado, pero no verificado.
Correo electrónico corporativo	Phishing dirigido a colaboradores	Falta de capacitación, incidentes menores no reportados, resistencia a mecanismos adicionales de autenticación.

El análisis de las situaciones que representan mayor riesgo permite identificar varios patrones preocupantes. En primer lugar, la gestión deficiente de accesos y de credenciales constituye una de las vulnerabilidades más críticas de la organización. El hecho de que algunos despachadores compartan credenciales durante horarios de alta demanda anula por completo la trazabilidad de las acciones realizadas en los sistemas, haciendo imposible determinar quién realizó una operación específica. Esta situación se vio materializada en el Evento 5, donde se identificó acceso no autorizado a información operativa utilizando credenciales compartidas.

En segundo lugar, la falta de clasificación de información impide establecer niveles adecuados de protección según la sensibilidad de los datos. Sin una clasificación clara, no es posible identificar qué información requiere cifrado, qué datos deben estar registrados a ciertos roles, o qué información puede compartirse libremente. Esta deficiencia se combina con la aplicación de procedimientos diferentes entre terminales para el manejo de información sensible, creando inconsistencias que los atacantes podrían aprovechar.

En tercer lugar, la ausencia de una cultura de seguridad representa un riesgo transversal que afecta a todos los activos de la organización, cuando los empleados consideran que la seguridad es exclusiva del área tecnológica, se genera una falsa sensación de seguridad que lleva a comportamientos de riesgo, como el uso de aplicaciones de mensajería personal para compartir información operativa o la no reportación de incidentes menores. Esta cultura débil hace que incluso los controles técnicos más robustos resulten ineficaces.

En cuarto lugar, la falta de pruebas de recuperación de respaldos representa un riesgo operativo significativo. Aunque los respaldos se realizan regularmente, la ausencia de pruebas documentadas significa que la organización no tiene certeza de que podrá recuperar su información en caso de un incidente grave. Esto podría resultar en pérdida de datos críticos y tiempos de recuperación prolongados que afectarían la continuidad del negocio.

Finalmente, la protección insuficiente de dispositivos móviles constituye un riesgo particularmente relevante dado que supervisores y personal de campo utilizan estos dispositivos con información sensible. El Evento 3 demostró cómo el extravío de un dispositivo puede comprometer información operacional crítica. La falta de mecanismos como cifrado, autenticación robusta y capacidad de borrado remoto amplifica significativamente este riesgo.

Análisis y gestión de riesgos

Metodología de análisis

Para la valoración de los riesgos identificados en TransMovil Nacional S.A.S., se adoptó una metodología de enfoque cualitativo. Este enfoque es ampliamente recomendado en organizaciones que, si bien cuentan con un alto volumen de operaciones, no disponen de datos históricos cuantitativos robustos sobre pérdidas financieras derivadas de ciber – incidentes. De acuerdo con los lineamientos institucionales de la Universidad Surcolombiana, la matriz de riesgos funciona como un instrumento fundamental para ubicar los riesgos en una determinada zona de riesgo según su calificación cualitativa, facilitando la toma de decisiones por parte de la alta dirección (*SURCOLOMBIANA, 2025*).

Para estructurar esta evaluación, se analizaron dos variables principales: el impacto y la probabilidad. El impacto se define como el nivel de afectación que materializaría una amenaza sobre los activos críticos de la empresa, evaluando consecuencias que van desde la parálisis operativa en los terminales de despacho hasta las severas sanciones legales que podría imponer la Superintendencia de Industria y Comercio por el incumplimiento de la ley 1581 de 2012. Por su parte, la probabilidad estima la factibilidad de que el evento ocurra, considerando las vulnerabilidades técnicas y humanas ya detectadas en el diagnóstico inicial.

En consonancia con las guías de gestión integral de riesgo aplicadas en el contexto nacional, se utilizó una escala de tres niveles (Bajo, Medio, Alto) para ambas variables, lo que permite consolidar una matriz de calor de 3x3 para determinar el nivel final del riesgo (*Pública, 2025*). Este enfoque pragmático se alinea con los principios de la norma ISO 31000, que promueve la estructuración de directrices claras para la gestión del riesgo, adaptadas al contexto específico y a la tolerancia al riesgo de cada entidad (*Pardo Alvarado, 2025*).

Matriz de riesgos

Tabla 4. Matriz de riesgos

<i>Riesgo</i>	<i>Impacto</i>	<i>Probabilidad</i>	<i>Nivel</i>
Fuga o robo de base de datos de pasajeros por uso de credenciales compartidas.	Alto	Alta	Crítico

Interrupción de la plataforma de venta de tiquetes en línea por ataques de denegación de servicios o fallas de infraestructura.	Alto	Media	Alto
Compromiso de información operativa y de rutas por extravío o robo de dispositivos móviles corporativos sin cifrado.	Medio	Alta	Alto
Infección por ransomware en el sistema ERP corporativo a través de campañas de phishing dirigidas.	Alto	Media	Alto
Perdida de visibilidad y control de flota (180 vehículos) por caída de la red GPS o conectividad.	Medio	Media	Medio

Análisis de riesgos prioritarios

Al analizar la matriz anterior, resulta evidente que el riesgo de fuga de la base de datos de pasajeros se posiciona en un nivel crítico. Esta situación no es hipotética; el Evento 5 del caso demuestra que el acceso no autorizado utilizando credenciales compartidas entre despachadores ya es una realidad en la compañía. Al tratarse de información personal de aproximadamente 1.200.000 pasajeros anuales, la materialización de este riesgo no solo detendría la operación por investigaciones de autoridades, sino que destruiría la confianza del mercado y acarrearía multas millonarias.

En segundo lugar, la interrupción de la plataforma de ventas y el compromiso del ERP representan un riesgo alto debido a la dependencia tecnológica que ha desarrollado la empresa en los últimos años. Como se observó en el Evento 2, una falla de apenas un fin de semana de alta demanda generó múltiples reclamaciones y afectaciones operativas. Si a esto le sumamos la vulnerabilidad humana frente al phishing (evidenciada en el Evento 1), la probabilidad de que un actor malintencionado logre cifrar los servidores

administrativos mediante ransomware es preocupante, dejando a la empresa sin capacidad de facturación ni gestión de nómina.

Finalmente, el riesgo asociado a los dispositivos móviles refleja una debilidad en los controles físicos y tecnológicos. El Evento 3, donde un supervisor perdió un equipo con información de programación de servicios, expone cómo la movilidad de la operación (rutas, inspecciones en carretera) choca con la falta de políticas de protección de datos en equipos de campo.

Políticas y controles de seguridad

Políticas propuestas

Frente al panorama de riesgos, es importante que TransMóvil Nacional S.A.S. formalice reglas de juego claras que oriente el comportamiento de los 480 colaboradores. Las siguientes políticas se proponen como el cimiento del nuevo Sistema de Gestión de Seguridad de la Información (SGSI).

Tabla 5. Políticas de seguridad

<i>Política</i>	<i>Objetivo</i>	<i>Riesgo asociado</i>
Política de control de accesos y autenticación.	Garantizar que cada acción en los sistemas sea trazable e intransferible, eliminando las cuentas genéricas y compartidas.	Fuga de datos por credenciales compartidas; acceso de excolaboradores.
Política de clasificación y manejo de información.	Establecer niveles de sensibilidad (Pública, Interna, Confidencial, Restringida) para aplicar controles diferenciados según el valor del dato.	Exposición de datos de pasajeros; fugas por dispositivos extraviados.
Política de seguridad en dispositivos móviles y teletrabajo.	Regular el uso, protección física, cifrado y borrado remoto de equipos corporativos utilizados fuera de las sedes principales.	Robo o extravío de equipos con información operativa y de rutas.

Controles propuestos

Para materializar las políticas anteriores, se diseñó un portafolio de controles que abarcan las dimensiones administrativas, técnicas y físicas, asegurando una defensa en profundidad.

Tabla 6. Controles de seguridad

<i>Riesgo</i>	<i>Control</i>	<i>Justificación</i>
Credenciales compartidas y accesos no autorizados.	(Técnico) Implementación de Autenticación Multifactor (MFA) y sistema de gestión de identidades (IAM).	El MFA mitiga el riesgo de que una contraseña comprometida o compartida permita el acceso a los sistemas críticos como el ERP o la base de datos.
Desconocimiento y resistencia a la seguridad.	(Administrativo) Programa continuo de sensibilización con simulacros de phishing y métricas de participación por terminal.	Ataca la raíz cultural del problema. Los empleados deben entender que la seguridad es responsabilidad de todos, no solo del área de Tecnología.
Extravíos de móviles corporativos.	(Técnico) Despliegue de una solución de Gestión de Dispositivos Móviles (MDM) con cifrado de disco y capacidad de borrado remoto.	Permite a la administración inutilizar el equipo y borrar los datos de flota y rutas de forma remota en caso de hurto o pérdida en carretera.
Acceso físico a cuartos técnicos y servidores.	(Físico) Instalación de controles biométricos o de tarjeta de proximidad con bitácora de acceso en los cuartos de equipo.	Evita que personal no autorizado o visitantes en los terminales principales puedan manipular la infraestructura híbrida local.
Falta de trazabilidad en despachos.	(Administrativo) Actualización de la matriz de roles y responsabilidades (RBAC) y firma de acuerdos de confidencialidad anuales.	Asegura el principio de menor privilegio; cada despacho solo tendrá acceso a las rutas y vehículos que gestiona, mejorando la trazabilidad.

Justificación de la estrategia de controles

La articulación de estos controles administrativos, técnicos y físicos contribuye directamente a disminuir la superficie de ataque de TransMovil. Por ejemplo, la resistencia cultural a los mecanismos adicionales de autenticación (mencionada en el diagnóstico) se mitiga no solo con la imposición técnica del MFA, sino con el control administrativo de capacitación, donde se explica al colaborador el “porqué” de la medida. Asimismo, los controles físicos en los cuartos técnicos y los casilleros seguros para dispositivos en los puntos de despacho complementan la seguridad lógica, entendiendo que en el sector transporte la operación ocurre en la calle, lejos del entorno controlado de una oficina tradicional.

Gestión de incidentes y continuidad del negocio

Incidentes potenciales

Dada la naturaleza crítica del servicio de transporte intermunicipal, la organización debe estar preparada para escenarios disruptivos que van más allá de las fallas cotidianas.

Tabla 7. Incidentes potenciales

<i>Incidente</i>	<i>Descripción</i>	<i>Impacto</i>
Ataques de Ransomware al ERP y servidores de respaldo.	Actor malicioso cifra la base de datos financiera y de pasajeros, exigiendo un rescate económico y amenazando con publicar los datos.	Parálisis total de la facturación, incapacidad de pagar a conductores y proveedores, y crisis reputacional severa.
Caída prolongada de la plataforma de ventas web por DDoS.	Ataque masivo de tráfico falso satura los servidores en temporada alta (ej. Semana santa o fin de año), impidiendo la venta digital.	Perdida millonaria de ingresos, saturación de las taquillas físicas y colapso en la atención al cliente.

Sabotaje o interferencia masiva a la red GPS de la flota.	Inhibición de señal o ataque a la plataforma de monitoreo, dejando a los 180 buses “ciegos” en carretera.	Riesgo inminente para la seguridad física de los pasajeros, secuestros o desvíos de ruta no detectados por la central.
---	---	--

Plan básico de respuesta

Para que TransMóvil Nacional S.A.S. pueda reaccionar de manera estructurada ante un incidente de seguridad, se propone un plan básico de respuesta organizado en cinco fases. Este esquema permite que, cuando ocurra un evento adverso, los colaboradores y el área de tecnología sepan exactamente qué hacer, evitando la improvisación que ha caracterizado a la empresa en eventos pasados.

Tabla 8. Plan básico de respuesta

<i>Fase</i>	<i>Acción</i>
1. Preparación	Conformación del Comité de Crisis integrado por Gerencia General, Dirección de Tecnología, Dirección Operativa, Jurídica y Comunicaciones. Elaboración de un directorio de contactos de emergencia. Configuración de respaldos inmutables almacenados fuera de línea.
2. Detección y Análisis	Monitoreo continuo de alertas en los sistemas críticos. Clasificación del incidente según su severidad (crítico si afecta ventas, flota o datos de pasajeros; medio si afecta procesos internos; bajo si es un evento aislado). Aislamiento inmediato de la red o sistema afectado para evitar la propagación.
3. Contención y Erradicación	Desconexión de servidores comprometidos de la red corporativa. Bloqueo de direcciones IP maliciosas y cuentas sospechosas. Restablecimiento obligatorio de credenciales administrativas. Eliminación del código malicioso o cierre de la vulnerabilidad explotada.

4. Recuperación	Restauración de base de datos y sistemas desde los respaldos verificados previamente. Retorno progresivo a la operación normal, iniciando por los servicios más críticos (venta de tiquetes y monitoreo de flota). Monitoreo intensivo durante las primeras 72 horas posteriores a la recuperación.
5. Lecciones Aprendidas	Elaboración de un informe que documente qué ocurrió, cómo se detectó, cuánto tiempo tomó la respuesta y qué impactos generó. Actualización de la matriz de riesgos y ajuste de controles técnicos y políticas con base en lo aprendido. Socialización de hallazgos con toda la organización.

Estrategia para la continuidad del negocio

La naturaleza del servicio que presta TransMovil Nacional S.A.S. hace que la continuidad operativa no sea solo un asunto tecnológico, sino una obligación con los más de 1.200.000 pasajeros que confían anualmente en la empresa para sus desplazamientos. Un ciberincidente severo no puede traducirse en la parálisis total del servicio, especialmente cuando se trata de transporte intermunicipal donde muchas personas dependen de estos vehículos para acceder a servicios de salud, educación y trabajo en Zonas rurales.

Ante la caída total del sistema ERP o de la plataforma de ventas en línea, la empresa debe habilitar procedimientos manuales de contingencia. Esto significa que cada terminal de despacho debe contar con talonarios de tiquetes físicos pre-impresos y debidamente foliados, planillas manuales para el registro de pasajeros y formatos en papel para la consignación de novedades operativas. Los despachadores, quienes según el diagnóstico priorizan la continuidad del servicio sobre los controles de seguridad, deben ser capacitados en estos procedimientos alternos para que la transición entre lo digital y lo manual sea fluida.

En cuanto a la flota de 180 vehículos, si el sistema GPS y la plataforma de monitoreo operacional colapsan, como ocurrió en el Evento 4, los conductores deben activar un protocolo de comunicación alternativo. Se propone establecer frecuencias radiales VHF como canales de respaldo, o en su defecto, líneas celulares de emergencia preestablecidas con la central de despacho. Los conductores reportarían su ubicación en puntos de control

específicos, como peajes o estaciones de servicio, cada cierto intervalo de tiempo. Esta redundancia analógica, aunque menos sofisticada que el monitoreo en tiempo real, garantiza que la empresa no pierda por completo la visibilidad de sus vehículos mientras los sistemas tecnológicos son restaurados.

Adicionalmente, se propone designar un responsable de continuidad del negocio en cada terminal principal, quien tendría la autoridad para activar los procedimientos manuales cuando se declare un incidente crítico, sin necesidad de esperar la aprobación del área de tecnología. Esta descentralización en la toma de decisiones es fundamental en una empresa con operaciones distribuidas geográficamente, donde cada minuto de inactividad puede traducirse en pasajeros varados, reclamaciones y daño reputacional.

Cultura organizacional en ciberseguridad

La cultura organizacional es quizás uno de los aspectos más determinantes, y a la vez más difíciles de transformar, en cualquier estrategia de seguridad de la información. En el caso de TransMovil Nacional S.A.S., el diagnóstico inicial reveló comportamientos profundamente arraigados que evidencian una cultura de seguridad débil, donde los controles se perciben como obstáculos para la operación y no como habilitadores de un servicio confiable.

Hallazgos organizacionales

Tabla 9. Hallazgos organizacionales

<i>Situación observada</i>	<i>Riesgo asociado</i>
Los empleados consideran que la seguridad es responsabilidad exclusiva del área de tecnología.	Desconexión entre las áreas operativas y los controles de seguridad, generando puntos ciegos donde los incidentes pueden ocurrir sin ser detectados ni reportados.
Las áreas priorizan la continuidad del servicio sobre el cumplimiento de controles.	Omisión sistemática de procedimientos de seguridad, como se evidenció con los despachadores que comparten credenciales para agilizar operaciones en horarios pico.
Confianza excesiva en comunicaciones externas de proveedores y entidades.	Alta susceptibilidad a ataques de ingeniería social y phishing, como el ocurrido en el Evento 1 donde un colaborador cayó ante un correo fraudulento.

Desconocimiento de los riesgos asociados al manejo de información de pasajeros.	Manipulación inadecuada de datos personales que puede derivar en sanciones bajo la ley 1581 de 2012 y pérdida de confianza por parte de los usuarios.
Incidentes menores no son reportados oportunamente.	Imposibilidad de identificar patrones de ataque tempranos, permitiendo que amenazas menores escalen a incidentes críticos.
Resistencia a mecanismos adicionales de autenticación.	Permanencia de vulnerabilidades en accesos administrativos y cuentas con privilegios elevados, facilitando el acceso no autorizado.

Recomendaciones de mejora

Tabla 10. Recomendaciones de mejora

<i>Hallazgo</i>	<i>Recomendación</i>
Seguridad percibida como responsabilidad exclusiva de Tecnología.	Implementar un programa de embajadores de seguridad en cada área operativa, donde colaboradores líderes reciban formación avanzada y repliquen buenas prácticas entre sus compañeros.
Priorización de la operación sobre los controles.	Rediseñar los procedimientos de seguridad para que se integren naturalmente al flujo operativo, en lugar de añadir pasos adicionales que los colaboradores perciban como burocráticos.
Confianza excesiva en comunicaciones externas.	Establecer un protocolo de verificación obligatorio para toda comunicación que solicite información sensible o acciones en sistemas, incluyendo un canal alternativo de confirmación con el remitente supuesto.
Desconocimiento de riesgos sobre datos de pasajeros.	Desarrollar cápsulas formativas breves y periódicas, con ejemplos reales del sector transporte, que ilustren las consecuencias legales, económicas y reputacionales de una fuga de datos.

Incidentes menores no reportados.	Crear un canal de reporte anónimo y simplificado, acompañado de una política de no represalias, que incentive a los colaboradores a comunicar cualquier situación inusual sin temor a sanciones.
Resistencia a autenticación multifactor.	Involucrar a los usuarios en la selección de las herramientas de autenticación, ofreciendo opciones que equilibren seguridad con facilidad de uso, y explicando con claridad los incidentes que el MFA habría prevenido.

Fortalecimiento de la cultura organizacional

Las recomendaciones propuestas no buscan imponer controles desde la dirección tecnológica, sino construir una cultura donde cada colaborador comprenda su rol en la protección de la información. El cambio cultural en TransMóvil Nacional S.A.S. debe partir del reconocimiento de que los 480 colaboradores son, en la práctica, la primera línea de defensa de la organización.

El programa de embajadores de seguridad es particularmente relevante en una empresa con operaciones distribuidas en múltiples terminales. Al identificar colaboradores líderes en cada sede, la empresa puede generar agentes de cambio que hablen el mismo lenguaje operativo que sus compañeros, traduciendo los conceptos técnicos de seguridad a situaciones cotidianas. Un despachador que comprenda por qué no debe compartir sus credenciales con un compañero, no porque un manual lo prohíba, sino porque eso impide rastrear quién cometió un error en un despacho específico, es mucho más valioso que cualquier firewall.

La integración de los controles al flujo operativo responde directamente a la percepción de que la seguridad afecta la eficiencia. Si los procedimientos se diseñan de manera que cumplir con las políticas de seguridad no requiera tiempo adicional significativo, la resistencia natural disminuirá. Por ejemplo, la autenticación multifactor puede implementarse mediante aplicaciones móviles que los colaboradores ya utilizan, evitando la fricción de tokens físicos o códigos SMS que llegan con retraso.

El canal de reporte anónimo y la política de no represalias abordan uno de los hallazgos más preocupantes: la ocultación de incidentes menores. En muchas organizaciones del sector transporte, la cultura del “no reportar para no generar problemas” es profundamente arraigada. Romper este patrón requiere señales claras desde la alta

dirección de que reportar un incidente es un acto de responsabilidad, no una confesión de culpa.

Finalmente, la involucración de los usuarios en la selección de herramientas de seguridad transforma la percepción de la ciberseguridad de una imposición técnica a una construcción colectiva. Cuando los colaboradores sienten que sus necesidades operativas fueron consideradas en el diseño de los controles, la adopción es significativamente mayor y la resistencia se reduce de manera sostenible en el tiempo.

Conclusiones

El análisis desarrollado permite extraer los siguientes hallazgos, aprendizajes y oportunidades de mejora fundamental sobre la integración de la ciberseguridad en la organización:

Primera conclusión.

La asimetría entre la acelerada adopción tecnológica y la nula madurez en seguridad de la información constituye el hallazgo estructural mas crítico. Se evidenció que digitalizar procesos operativos sin actualizar simultáneamente las políticas de protección transforma la infraestructura, diseñada para escalar el negocio, en la principal superficie de ataque. Como oportunidad de mejora, la organización debe comprender que la inversión tecnológica solo es sostenible si va acompañada de un Sistema de Gestión de Seguridad de la Información (SGSI) que gobierne los nuevos canales digitales.

Segunda conclusión.

La gestión de identidades y accesos se consolida como la vulnerabilidad de mayor exposición y el eslabón más débil de la cadena de defensa. El análisis demostró que la falta de trazabilidad individual y la compartición de credenciales anulan la eficiencia de cualquier control perimetro de seguridad; por tanto, la implementación de autenticación multifactor y el principio de menor privilegio no son opciones técnicas, sino requisitos ineludibles para garantizar la auditoría y responsabilidad de las acciones operativas.

Tercera conclusión.

La ausencia de esquema de clasificación de la información y de gobierno de datos impide la asignación eficiente de los recursos de ciberseguridad. Al tratar todos los datos con el mismo nivel de protección, la organización diluye su inversión y expone activos críticos al mismo nivel de riesgo que la información pública. Se identifica como oportunidad de mejora la urgencia de categorizar los activos según su impacto legal y operativo, lo que permitirá diseñar controles diferenciados y asegurar el cumplimiento normativo frente a la legislación de protección de datos personales.

Cuarta conclusión.

La cultura organizacional actúa actualmente como un multiplicador de riesgo, pero posee el mayor potencial de transformación. La percepción de la seguridad como un obstáculo para la eficiencia operativa y la subnotificación de incidentes revelan una profunda desconexión entre la estrategia corporativa y la realidad en los puntos de despacho. El aprendizaje fundamental es que los controles técnicos resultan ineficaces si no se acompañan de un cambio cultural participativo. Convertir al factor humano en la primera línea de defensa mediante programas de embajadores y canales de denuncia sin represalias es la mayor oportunidad de mejora a mediano plazo.

Quinta conclusión.

La dependencia tecnológica absoluta ha comprometido severamente la resiliencia del negocio. El análisis de los incidentes históricos demostró que la organización carece de mecanismos de redundancia que garanticen la prestación del servicio ante la indisponibilidad de los sistemas digitales. Como hallazgo vital, la continuidad operativa en el sector transporte no puede subordinarse a la infraestructura lógica. La oportunidad de mejora radica en institucionalizar procedimientos de contingencia analógicos y protocolos de comunicación alternos, asegurando que la misión esencial de la empresa prevalezca independientemente de las fallas o ciberataques que afecten su entorno digital.

Sexta conclusión.

El incumplimiento latente de la normativa de protección de datos y delitos informáticos representa un pasivo legal que amenaza la viabilidad financiera y reputacional de la empresa. Se concluye que la ciberseguridad no debe abordarse únicamente desde una perspectiva técnica de prevención de ataques, sino como un habilitador estratégico de cumplimiento legal. Adoptar estándares internacionales ofrece la oportunidad de blindar a la organización frente a sanciones, transformando la protección de la información en un activo que genera confianza en los usuarios y ventaja competitiva en el mercado.

Referencias

- Acevedo, M. D. (30 de 12 de 2024). *Revista Estudios en Seguridad y Defensa*. Obtenido de Revisión del estado actual de la ciberseguridad en Colombia:
<https://esdegrevistas.edu.co/index.php/resd/article/view/1999/5377#info>
- Amaya, Y. A. (13 de 10 de 2020). *Agencia Nacional Digital*. Obtenido de GUÍA DE GESTIÓN Y CLASIFICACIÓN DE ACTIVOS:
https://and.gov.co/sites/default/files/2022-05/Guia_De_Gestion_y_clasificacion_de_activos_de_informacon.pdf
- CIBERSEGURIDAD, B. E. (21 de 5 de 2015). *ESG Innova*. Obtenido de ISO 27001: ¿Qué significa la Seguridad de la Información?: <https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/>
- comunicaciones, m. d. (3 de 2025). *ESTRATEGIA NACIONAL DE SEGURIDAD DIGITAL*. Obtenido de seguridad digital de colombia 2025 - 2027:
https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
- digwatch. (7 de 2020). *digwatch*. Obtenido de Política nacional de Colombia sobre confianza y seguridad digital.: <https://dig.watch/resource/colombias-national-policy-on-digital-trust-and-security>
- Distrital, S. J. (5 de 1 de 2009). *RÉGIMEN LEGAL DE BOGOTÁ D.C.* Obtenido de Ley 1273 de 2009 Congreso de la República de Colombia:
<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>
- Distrital, S. J. (18 de 10 de 2012). *RÉGIMEN LEGAL DE BOGOTÁ D.C.* Obtenido de Ley 1581 de 2012 Congreso de la República de Colombia:
<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>
- Estrada, L. A. (s.f.). *siscotec*. Obtenido de Gestión de Riesgos de Ciberseguridad en el Sector Financiero de Bolivia y Latinoamérica: <http://siscotec.com/blog/xperti-1/gestion-de-riesgos-de-ciberseguridad-en-el-sector-financiero-de-bolivia-y-latinoamerica-26>
- finales, C. p. (s.f.). *Instituto Nacional de Aprendizaje*. Obtenido de Confidencialidad, integridad y disponibilidad:
https://www.inavirtual.ed.cr/pluginfile.php/2974195/mod_resource/content/5/confidencialidad_integridad_y_disponibilidad.html
- Fortinet. (s.f.). *Fortinet*. Obtenido de Tríada CIA: confidencialidad, integridad y disponibilidad: <https://www.fortinet.com/lat/resources/cyberglossary/cia-triad>
- NQA. (s.f.). *0005110_Tema_13_ISO-27001-Guia-de-implantacion.pdf*. Obtenido de ISO 27001:2013 guía de implementación para la seguridad de la información:
https://www.gob.mx/cms/uploads/attachment/file/811061/0005110_Tema_13_ISO-27001-Guia-de-implantacion.pdf
- NYCE. (s.f.). *NYCE*. Obtenido de ISO IEC 27001 Sistema de Gestión de Seguridad de la Información: <https://nyce.org.mx/iso-iec-27001-sistema-de-gestion-seguridad-de-la-informacion/>
- Pardo Alvarado, M. A. (2025). *Universidad Externado de Colombia*. Obtenido de Publicación: Exploración de la convergencia entre las normas ISO 22301:2012 y su actualización ISO 22301:2019 junto con la ISO 31000:2018 para unificar su

- aplicación en las organizaciones:
<https://bdigital.uexternado.edu.co/entities/publication/f96b31d8-ce87-4166-8f85-dbef4c2d83c4>
- Pública, F. (2025). *Función Pública*. Obtenido de Guía para la Gestión Integral del Riesgo en Entidades Públicas: https://umng.edu.co/wp-content/uploads/2026/04/Guia-para-la-gestion-integral-del-riesgo-en-entidades-publicas-2025_v7.pdf
- Software, A. (s.f.). *Aranda Software*. Obtenido de CIBERSEGURIDAD EN LATINOAMÉRICA: Un llamado a la acción empresarial: <https://arandasoft.com/blog/ciberseguridad-en-latinoamerica-un-llamado-a-la-accion-empresarial/>
- SURCOLOMBIANA, U. (2025). *UNIVERSIDAD SURCOLOMBIANA*. Obtenido de PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION: <https://www.usco.edu.co/documento/415305>
- T., J. C. (s.f.). *DELTA ASESORES*. Obtenido de Ley de Delitos Informáticos en Colombia: <https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/>
- Tecnología, I. y. (3 de 3 de 2021). *Unir la Universidad en Internet*. Obtenido de Disponibilidad en seguridad informática: ¿en qué consiste este término?: <https://www.unir.net/revista/ingenieria/disponibilidad-seguridad-informatica/>