TRABAJO DE GRADO
Opción Seminario-Diplomado.

Informe técnico

El día que la plataforma colapsó

Corporación Universitaria Remington.
Especialización en seguridad de la información
Introducción a la ciberseguridad organizacional

Jose Luis Mena Asprilla
Jorge Leonardo Ramírez Restrepo
Seminario
2026

Agradecimientos

La realización de este trabajo de grado y la culminación de esta etapa profesional no habrían sido posibles sin el respaldo y la compañía de la empresa, personas e institución que fueron piezas clave, y a quienes deseo expresar mi más profundo agradecimiento.

A la corporación Montesol: Por creer en mi potencial y brindarme su invaluable ayuda económica. Su apoyo fue el pilar fundamental que me permitió enfocarme, investigar y culminar con éxito mi formación como ingeniero de sistemas y especialista en seguridad de la informática.

A mis padres. Les doy unas gracias infinitas por ser mi mayor inspiración. Su apoyo emocional, amor incondicional y sus palabras de aliento en los momentos difíciles fueron el motor principal para no desfallecer durante todo mi proceso.

A mi esposa. Le agradezco de todo corazón por tu paciencia inagotable ante las largas jornadas de estudio y el desarrollo de este proyecto. Tú comprensión, tu apoyo constante y tu compañía incondicional han sido pieza vital para alcanzar esta meta. Este logro no solo es mío también es tuyo.

A la Universidad Remington. A todos mis docentes y directivos, extiendo mi inmensa gratitud por su excelencia académica. Gracias por ser esa gran institución que me brindó las herramientas, las bases sólidas y el gran conocimiento necesario para mi desarrollo profesional.

A todos ustedes, mi más sincera gratitud. Este logro es el reflejo de su apoyo incondicional.

Tabla de Contenidos

Resumen

El presente informe técnico expongo el diagnóstico y la propuesta de mitigación para la arquitectura de Zendira S.A.S., una organización cuyo crecimiento acelerado generó una severa falta técnica y una exposición de riesgos. El objetivo central es evaluar las deficiencias sistémicas derivadas de priorizar la escalabilidad operativa sobre la seguridad desde el diseño, exponiendo los activos críticos como son las pasarelas transaccionales y el enrutamiento.

"Mediante una gestión de riesgos estructurada bajo la norma ISO 27005, se identificó vulnerabilidades estructurales de alto impacto, destacando la ausencia de cifrado robusto en tránsito mediante el protocolo (TLS), la falta de cifrado en reposo (AES-256) y la carencia de toma de decisiones (OWASP, 2021)." Estas debilidades no solo facilitan la materialización de amenazas externas, sino que exponen a la compañía a un inminente incumplimiento de la Ley 1581 de 2012 sobre protección de datos personales.

Para neutralizar este panorama, se diseña una estrategia integral de ciberseguridad organizacional. Esta ruta de acción incluye la implementación de controles técnicos, el diseño de una matriz de respuesta a incidentes para asegurar la continuidad del negocio y la formalización de políticas de seguridad alineadas con ISO 27001 y las directrices de ENISA.

El informe concluye que la tecnología debe complementarse con la transformación del factor humano, una cultura de seguridad sólida y medible que permitirá a la alta dirección transitar de una postura reactiva hacia un modelo de fortaleza corporativa a largo plazo.

Palabras clave

- ✓ Ciberseguridad organizacional
- ✓ Gestión de riesgos
- ✓ Activos de información
- ✓ Vulnerabilidades
- ✓ Políticas de seguridad

Marco conceptual y contextual

Marco conceptual

La protección de los entornos corporativos modernos se exige una aproximación estructural y denominada ciberseguridad organizacional. Este concepto trasciende la simple adopción de herramientas informáticas, consolidándose como un eje enfocado en resguardar la disponibilidad, integridad y privacidad de los recursos críticos de una entidad o empresa. Los recursos, conocidos como activos de información, engloban las bases de datos, infraestructuras, aplicativos y procesos operacionales que otorgan valor competitivo y viabilidad a una compañía.

En el desarrollo de las actividades, las empresas enfrentan diversas amenazas, las cuales representan cualquier peligro, fenómeno o circunstancia capaz de atentar contra la estabilidad tecnológica. Estas amenazas logran materializarse de manera efectiva cuando aprovechan las vulnerabilidades, entendidas como aquellas falencias o fallas estructurales, técnicas o procedimentales presentes en los esquemas de la empresa. La convergencia entre una debilidad sistémica y un agente hostil configura un riesgo cibernético, cuya evaluación permite dimensionar el impacto financiero, operativo y reputacional de un potencial evento hostil.

Frente a este panorama, resulta imperativo el despliegue de controles de seguridad, abarcando medidas preventivas y correctivas diseñadas para reducir la probabilidad de incidentes y garantizar la efectividad de estas contramedidas, su implementación debe articularse con referentes globales como la norma ISO/IEC 27001, “la cual establece las directrices fundamentales para estructurar sistemas de gestión de seguridad de la información(SGSI) (ISMS.online, 2026)”, el fortalecimiento de estas defensas responde al estricto acatamiento de la Ley 1581 de 2012,

legislación estatutaria que exige a las organizaciones salvaguardar celosamente la información de carácter personal de los usuarios o clientes que administran.

Marco contextual

El entorno de estudio para el desarrollo de este informe corresponde a Zendira S.A.S., una empresa sumergida en el sector del comercio electrónico y la distribución logística. Su modelo de negocio se caracteriza por una dependencia tecnológica absoluta, soportando la totalidad de su ciclo operativo a través de plataformas digitales interconectadas. Esta modalidad abarca desde aplicaciones móviles y sistemas de enrutamiento logístico, hasta complejas pasarelas transaccionales y repositorios masivos de datos.

En el transcurso de los últimos tres años, la compañía ha experimentado un crecimiento acelerado y una destacada entrada en el mercado nacional. No obstante, esta rápida escalabilidad comercial entrevió una anomalía organizacional crítica. La priorización de la expansión operativa no estuvo acompañada de una estrategia proporcional enfocada en la protección de sus entornos digitales.

En la actualidad, la infraestructura de Zendira presenta carencias estructurales que comprometen seriamente su seguridad. A nivel corporativo, se destaca la ausencia de un área especializada o de un liderazgo enfocado en la gestión de la seguridad, lo que imposibilita la articulación de respuestas frente a posibles incidentes. Desde el punto de vista técnico y administrativo, la organización procesa información altamente confidencial sin aplicar mecanismos de criptografía, y opera sin normativas internas de concienciación dirigidas a sus colaboradores. Esta debilidad sistémica frente a un medio de amenazas en constante evolución

fundamenta la realización del presente análisis, cuya intención central es diseñar soluciones estratégicas que prevengan el inminente colapso de la plataforma tecnológica.

Desarrollo e implementación del aprendizaje

El día que la plataforma colapsó

La empresa Zendira S.A.S., es una compañía tecnológica de rápido crecimiento dedicada al comercio electrónico y entregas a domicilio. Cuenta con cientos de colaboradores y maneja el 100% de su operación a través de sistemas digitales interconectados. Aplicación móvil, pasarelas de pago, logística de rutas, control de inventarios y una masiva base de datos de usuarios. Durante los últimos tres años, la empresa había experimentado un éxito comercial explosivo y una excelente acogida en el país, pero no había invertido de manera formal y proporcional en ciberseguridad. Al priorizar la expansión rápida, no contaban con un equipo dedicado a la seguridad de la información, ni con protocolos de cifrado de datos o políticas claras de prevención de riesgos para sus empleados.

Valoración técnica de activos enfocados ISO 27005

Teniendo en cuenta y sabiendo que los activos de una empresa son todos los bienes y recursos, tangibles e intangibles, que esta posee. De mucho valor económico que garantizan la operatividad y resultan vitales para generar beneficios futuros.

La identificación de los siguientes activos en Zendira S.A.S. se fundamenta por su nivel de criticidad y para la continuidad del negocio es de vital importancia analizar. En la siguiente tabla se evalúan las dimensiones de seguridad en una escala de 1 a 5, donde 5 representa el máximo impacto ante una pérdida de Confidencialidad (C), Integridad (I) y Disponibilidad (D).

Tabla 1

Matriz de identificación, relación y nivel de criticidad.

Activo	Tipo	C	I	D	Criticidad	Justificación Técnica
Bases de datos clientes	Datos	5	5	4	4.7	Contiene información sensible sujeta a la Ley 1581.
Pasarelas de pagos	Procesos	5	5	5	5.0	Punto crítico para la validación financiera y APIs.
Aplicación móvil	Tecnología	3	5	5	4.3	Interfaz exclusiva para la interacción y motor de ingresos.
Sistema de logística de rutas	Tecnología	2	4	5	3.7	Vital para la optimización de entregas y cadena física.
Sistema de control inventarios	Datos	2	5	4	3.7	Refleja el stock real; su alteración causa desajustes.
colaboradores	Personas	4	3	3	3.3	Principal vector para ataques de ingeniería social.

Evaluación de riesgos, amenazas y vulnerabilidades

Análisis de probabilidades

El siguiente análisis de riesgos para Zendira S.A.S. trasciende las evaluaciones genéricas de infraestructura tecnológica, enfocándose en su realidad operativa particular de un modelo de crecimiento donde la inmediatez logística y la transaccionalidad financiera sostienen la viabilidad del negocio. La priorización histórica de la escalabilidad comercial sobre la seguridad desde el diseño ha generado una extensa ausencia técnica. En este escenario, la convergencia entre activos

digitales críticos altamente expuestos y la falta de un gobierno de seguridad formal, configura un entorno que favorece la materialización de eventos dañinos.

A continuación, se detalla la matriz de riesgos, diferenciando rigurosamente las deficiencias internas (vulnerabilidades) de los agentes hostiles (amenazas), y justificando sus métricas en función del impacto directo a la continuidad del servicio y el cumplimiento normativo. "Basado en los marcos NIST y ISO 27005, los cuales hablan de la gestión de riesgos de la seguridad, se analiza cómo las vulnerabilidades detectadas en Zendira permiten la materialización de amenazas (NIST, 2025)."

Tabla 2

Matriz de evaluación de riesgo, amenazas y vulnerabilidades

Amenaza	**Vulnerabilidad**	**Activo Afectado**	**Probabilidad**	**Impacto**	**Riesgo (P*I)**
Robo de datos - MITM (hombre en el medio)	Ausencia de protocolos de cifrado.	Base de Datos / Pasarelas	5	5	25 (Crítico)
Ingeniería social phishing	Falta de políticas de prevención.	Colaboradores	5	4	20 (Muy Alto)
Malware - Ransomware	Inversión insuficiente en seguridad.	Sistema de Logística e Inventario	4	5	20 (Muy Alto)
Ataques DDoS (denegación de servicios)	Falta de equipo de seguridad dedicado.	Aplicación Móvil	3	5	15 (Alto)

Justificación técnica de impacto y probabilidad

Para asegurar la rigurosidad del análisis de riesgos de Zendira S.A.S., y los valores asignados en la matriz anterior se fundamentan en un cruce entre la realidad operativa de la compañía y los estándares internacionales de gestión de la seguridad.

A continuación, se detalla la lógica técnica detrás de cada valoración.

Análisis de probabilidad

La probabilidad se calculó bajo el concepto de deuda técnica de seguridad. Dado que Zendira ha priorizado la escalabilidad del negocio sobre la robustez de su infraestructura, los niveles de probabilidad se justifican de la siguiente manera:

Frecuencia de exposición nivel

En activos como las pasarelas de pago y el personal operativo, su probabilidad de que pase es máxima debido a la ausencia de controles compensatorios. La falta de cifrado TLS y de programas de concienciación convierte vulnerabilidades teóricas en vectores de ataque activos y constantes.

Visibilidad del activo

Al ser una plataforma con un crecimiento del 100%, la atracción para agentes hostiles externos aumenta proporcionalmente, elevando la probabilidad de intentos de intrusión sistemáticos.

Análisis de impacto

El impacto no solo se mide la falla técnica, sino la repercusión sistémica en la organización. La cual se ha determinado bajo tres criterios críticos de la siguiente manera:

Continuidad del negocio

Para una entidad como Zendira, el impacto en el sistema de enrutamiento y logística es crítico de Nivel 5, ya que su indisponibilidad detiene el flujo de caja en tiempo real, generando pérdidas económicas directas por cada minuto de caída.

Cumplimiento legal y regulatorio

El impacto en las bases de datos y pasarelas de pago se califica con la máxima severidad debido a las implicaciones de la Ley 1581 de 2012 en Colombia. “Una brecha de datos financieros no solo conlleva sanciones económicas de entes reguladores, sino que también puede derivar en la revocación de licencias operativas (Congreso de la República de Colombia, 2012).”

Reputación y confianza

En el sector de servicios digitales, la pérdida de integridad de los datos de los usuarios genera un daño reputacional que, en muchos casos, es irreversible para empresas en etapa de mayor expansión.

Clasificación de riesgos

La clasificación de los riesgos en niveles Alto y Crítico se fundamenta en el impacto directo a la continuidad del negocio de Zendira. Ejemplo, la caída de los servidores o el secuestro de la base de datos (Ransomware) se consideran críticos porque no solo detienen el 100% de la facturación en línea, sino que exponen a la empresa a severas multas por incumplimiento de la Ley 1581 de 2012 (Protección de Datos), además de una pérdida irreversible de confianza por parte de los clientes.

Análisis de riesgo como base para la toma de decisiones

En la estructuración de la matriz de riesgos y la propuesta de controles técnicos para Zendira S.A.S. no establecen únicamente un diagnóstico operativo, sino que representan la base

estratégica para la toma de decisiones directivas. Al evidenciar matemáticamente el nivel de exposición extrema frente a vulnerabilidades críticas como la falta de cifrado en pasarelas de pago. la gerencia debe tener en cuenta ahora como instrumento u objetivo para justificar y priorizar la asignación de presupuesto hacia el área de seguridad de la información.

Asimismo, el despliegue de las contramedidas propuestas no solo se fundamenta en la norma ISO 27005 para la gestión sistemática del riesgo, sino que se alinea con las directrices y buenas prácticas recomendadas por ENISA (Agencia de la Unión Europea para la Ciberseguridad). La adopción de las guías de ENISA, especialmente en lo referente a la protección de infraestructuras críticas de comercio electrónico, garantiza que Zendira realice un modelo de defensa en profundidad probado a nivel internacional, mitigando riesgos de paralización de su plataforma.

Propuesta de mitigación y definición de políticas

Trazabilidad y propuesta de controles

La estrategia de mitigación para Zendira S.A.S. no se basa en la adopción de controles genéricos, sino que se fundamenta estrictamente en los riesgos críticos previamente identificados. Para garantizar la coherencia arquitectónica y responder a la realidad operativa de la empresa (un ecosistema de comercio electrónico en crecimiento sin madurez defensiva), se definen las siguientes políticas de seguridad, acompañadas de sus respectivos controles de implementación:

Alineación frente al riesgo de interceptación

Política de criptografía y protección de la privacidad.

Se establece el mandato corporativo de proteger la confidencialidad e integridad de toda la información transaccional y personal, garantizando el cumplimiento estricto de la Ley 1581 de 2012.

Implementación de un estándar de cifrado robusto. Esto exige el despliegue forzoso de protocolos TLS, para asegurar los túneles de comunicación en las APIs de las pasarelas de pago (datos en tránsito) y la aplicación del algoritmo AES-256 para salvaguardar los repositorios de bases de datos de clientes (datos en reposo).

Alineación frente al riesgo de ingeniería social

Política de concienciación y control de acceso lógico.

Se determina que el factor humano debe dejar de ser el eslabón más débil para convertirse en la primera línea de defensa, normalizando el acceso a los sistemas críticos logísticos y de inventarios.

La ejecución de un programa de entrenamiento técnico continúo enfocado en la higiene digital y la detección de phishing. Como control técnico y compensatorio, se debe configurar la autenticación Multifactor (MFA) totalmente obligatoria para todos los colaboradores que ingresen a las plataformas internas de la empresa.

Alineación frente al riesgo de interrupción operativa

Política de continuidad de negocio y gobernanza de seguridad.

La organización asume el compromiso directivo de garantizar la disponibilidad ininterrumpida de su aplicación móvil y su sistema de enrutamiento físico, creando la estructura organizacional necesaria para responder a incidentes.

Creación formal de un comité de seguridad de la información o la designación de un director de seguridad de la información para liderar el SGSI basado en ISO 27001. A nivel de infraestructura, se requiere la integración de servicios de mitigación perimetral como Firewall y escudos Anti-DDoS) para absorber y mitigar picos anómalos de tráfico malicioso y proteger el motor de ingresos de Zendira.

Gestión y respuesta a incidentes de ciberseguridad

Ante la definición de incidente en el contexto de Zendira S.A.S. un incidente de ciberseguridad no se limita a una simple falla informática, se define como cualquier evento adverso, confirmado o bajo sospecha, que comprometa la confidencialidad, integridad o disponibilidad de sus activos críticos como aplicación móvil, pasarelas de pago y logística de rutas.

En el contexto de su crecimiento, un incidente es toda aquella alteración técnica que detenga el flujo de transacciones en tiempo real o que vulnere los datos personales de los clientes, activando escenarios de incumplimiento bajo la Ley 1581 de 2012.

Identificación de posibles incidentes y protocolo de respuesta

Alineado con los riesgos previamente evaluados y las políticas de seguridad establecidas, se definen los siguientes escenarios de incidentes y sus mecanismos de respuesta.

Incidente de exfiltración de datos

Incidente. Captura de credenciales financieras en tránsito debido a un ataque Man-in-The-Middle (hombre en el medio) en la API de la pasarela de pagos, como opera esta modalidad el agresor se filtra en la red y todo paquete enviado de un lugar a otro es interceptado inmediatamente.

Respuesta ante el incidente. Aislamiento inmediato del punto de conexión o API comprometida en la pasarela de pagos para frenar la fuga de datos.

Erradicación y recuperación. Forzar la renegociación de certificados y activar el túnel más protegidos como TLS de emergencia.

Notificaciones. Activación del protocolo legal para reportar la brecha de datos personales ante la Superintendencia de Industria y Comercio en cumplimiento de la normativa colombiana.

Incidente de secuestro operativo

Incidente. La infección por Ransomware en el sistema de enrutamiento logístico y control de inventarios, originado por un colaborador víctima de Phishing esto ya es una falla del factor humano.

Respuesta ante el incidente. Desconexión física y lógica o segmentación de red de los servidores de logística afectados para evitar el movimiento lateral del malware hacia la base de datos central.

Erradicación y recuperación. Ejecución del plan de recuperación de desastres, limpiando los equipos afectados y restaurando la operatividad desde la última copia de seguridad inmutable disponible. Cambiar a un modelo de despacho manual temporal mientras se restablece los daños en el sistema.

Incidente de indisponibilidad comercial

Incidente. La caída de la aplicación móvil el motor principal de ingresos, producto de un Ataque de denegación de servicio distribuido (DDoS).

Respuesta ante el incidente. El comité de seguridad de la información debe ordenar la activación inmediata de un Firewall o WAF para esclarecer nuevas reglas de filtrado contra una negación de servicios (DDoS).

Recuperación. Desvío del tráfico malicioso hacia zonas de mitigación a un scrubbing centers. Esto funciona como un filtro que limpia el tráfico de internet, permitiendo que solo los clientes reales entren a la app y evitando que el sistema se bloquee por ataques falsos conocido como centro de depuración, para garantizar que únicamente las peticiones legítimas de los clientes alcancen los servidores de Zendira.

Tabla 3

Matriz ejecutiva de respuesta a incidentes para Zendira S.A.S.

Categoría del Incidente	Método de intrusión	Contención Inmediata	Erradicación y Recuperación	Post-Incidente y Cumplimiento
Exfiltración de datos	Ataque MITM en API de pagos por deficiencia de cifrado.	Bloqueo lógico y aislamiento del punto de conexión vulnerado.	Renegociación de certificados y activación forzosa de TLS	Notificación de brecha a la SIC (Cumplimiento Ley 1581).
Secuestro logístico	Infección por Ransomware originada vía Phishing.	Desconexión física y segmentación estricta de red.	Ejecución del DRP: Restaurar sistema desde backup inmutables.	Análisis forense de la máquina cero y reentrenamiento del personal.
Indisponibilidad comercial	Ataque volumétrico (DDoS) dirigido a la aplicación móvil.	Activación de reglas dinámicas de mitigación vía WAF perimetral.	Redireccionamiento de tráfico anómalo a scrubbing centers centro de depuración.	Ajuste de umbrales de alerta y auditoría de balanceo de carga.

Evaluación de la cultura organizacional en ciberseguridad

Para que la implementación del sistema de gestión de seguridad de la información (SGSI) sea sostenible en Zendira S.A.S., es necesario trascender la visión puramente tecnológica y consolidar una robusta cultura organizacional orientada y capacitados a la ciberseguridad. En un entorno de crecimiento, las herramientas perimetrales y los algoritmos de cifrado necesarios

resultan ser insuficientes si el factor humano continúa siendo el eslabón más vulnerable frente a técnicas de ingeniería social.

La transformación cultural se debe originar desde la alta dirección, demostrando un compromiso más visible que penetre hacia todos los niveles operativos. Así la ciberseguridad dejará de ser percibida como un obstáculo de un sistema estructurado del área de tecnología, para integrarse como un valor corporativo fundamental que protege el motor de ingresos de la empresa y garantiza el cumplimiento normativo.

Estratégicas de madurez cultural

Para medir la evolución de esta cultura organizacional y asegurar la mejora continua, se establecen las siguientes recomendaciones claves orientados al comportamiento humano.

Resiliencia humana frente a un taque por phishing. Se mide la relación entre los correos maliciosos simulados que son reportados proactivamente por los colaboradores frente a los que son aceptados. Una cultura madura y comprometida se evidencia cuando la tasa de reporte supera ampliamente la tasa de interacción.

Adopción de higiene digital. Se evalúa el porcentaje de la plantilla que completa satisfactoriamente los módulos de concientización y aplica las políticas de contraseñas seguras y Autenticación Multifactor (MFA) sin requerir escalamientos o ayuda a soporte técnico.

Proactividad en el reporte de incidentes. Sumar el número de reportes voluntarios sobre posibles anomalías o errores humanos ejemplo, envío accidental de información sensible. Un aumento inicial en este indicador es positivo, ya que demuestra que los empleados confían en los canales internos y no ocultan los incidentes por temor a sanciones disciplinarias.

A través de las mediciones constantes de estas variables, Zendira logrará que sus colaboradores actúen como la primera línea de defensa activa en sí, garantizando que el crecimiento comercial esté respaldado por un equipo humano consciente y preparado.

En fin, El fortalecimiento de la cultura organizacional en Zendira S.A.S. trasciende en la simple capacitación teórica constante hasta convertirse en un hábito operativo diario. Consiste en transformar a cada colaborador, desde el área administrativa hasta el equipo de desarrollo, en la primera línea de defensa activa contra las amenazas cibernéticas. Para lograr esto de manera práctica, la empresa adopta un programa de concientización continua que reemplaza el enfoque punitivo por uno colaborativo. De este modo, “acciones como el reporte temprano de correos sospechosos, la participación en simulacros de phishing y la aplicación rigurosa de los controles de acceso se integran de forma natural en los procesos de negocio (Proofpoint, 2026)”, garantizando una resiliencia humana que complementa y blinda la infraestructura tecnológica.

Conclusiones

En la aplicación de los marcos de referencia analizados durante este seminario en la estructura operativa de Zendira S.A.S. me permite concluir que la ciberseguridad no debe ser tratada como un gasto tecnológico, sino como un recurso estratégico del negocio. El principal hallazgo de este estudio revela una cierta cantidad de riesgos, la organización alcanzó un volumen transaccional de gran importancia, pero mantuvo una postura defensiva reactiva propia de una entidad primitiva. Esta brecha se denomina una deuda técnica de seguridad y es la causa raíz de la fragilidad que llevó a la plataforma al borde del colapso.

A través de un análisis técnico crítico, se identificó que el riesgo más relevante no reside únicamente en las amenazas externas, sino en la exposición estructural de los activos críticos. El procesamiento de información financiera en texto plano y la ausencia de un sistema de gestión de la información (SGSI) representan vulnerabilidades que trascienden lo técnico, impactando directamente la esfera legal bajo la Ley 1581 de 2012. La materialización de un ataque a las pasarelas de pago o al sistema logístico no solo paralizaría la facturación de la empresa, sino que destruiría el activo más difícil de recuperar para una marca en crecimiento como seria la confianza del consumidor.

No obstante, esta crisis se presenta como una oportunidad única de mejora para la gestión de la ciberseguridad. El cambio hacia un modelo de defensa en profundidad, apoyado en estándares internacionales como ISO 27001 y las guías de ENISA, ayudaría a Zendira a profesionalizar su infraestructura. La verdadera oportunidad de mejora reside en la formación de una cultura en seguridad para que cada uno de los colaboradores entiendan su papel como primera línea de defensa ante un ataque hostil. También al integrar la seguridad desde el diseño y fomentar una

conciencia organizacional proactiva, la empresa no solo mitigará riesgos en su estructura, sino que blindará su competitividad y sostenibilidad en un mercado digital que cada vez es más hostil.

Referencias

Congreso de la república de Colombia. (2012, 18 de octubre). *ley estatutaria 1581 de 2012*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

ENISA - Agencia de la Unión Europea para la Ciberseguridad. (2026*). Good Practices for Supply Chain Cybersecurity*. https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

GlobalSuite Solutions. (2026). *ISO/IEC 27005:2024*. https://www.globalsuitesolutions.com/es/iso-27005-vs-iso-27001-gestion-riesgos/

ISMS.online. (2026). *ISO 27001:2022*. https://es.isms.online/iso-27001/requirements-2022/

NIST - Instituto nacional de estándares y tecnología. (2025, 16 de septiembre). *Ciberseguridad y privacidad*. https://www.nist.gov/cybersecurity-and-privacy

Organización Internacional de Normalización (ISO). (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información (ISO/IEC 27002:2022)*. https://www.iso.org/standard/75652.html

OWASP. (2021). *OWASP Top 10: Vulnerabilidades de aplicaciones web.* https://owasp.org/Top10/es/

Proofpoint. (2026). *Qué es phishing. https://www.proofpoint.com/es/threat-reference/phishing*