TRABAJO DE GRADO
Opción Seminario-Diplomado.

Informe Tecnico

Corporación Universitaria Remington.
Nombre de la facultad: Facultad de Ingeniería
Nombre del programa académico: Tecnología en desarrollo de software

Jorge David Mercado Serje
Jorge Leonardo Ramirez Restrepo
Gestión de Ciberseguridad en las Organizaciones
2026

Tabla de Contenidos

Resumen

El presente informe desarrolla un análisis de ciberseguridad organizacional aplicado a la empresa hipotética TechStore S.A.S., dedicada a la comercialización de productos tecnológicos mediante una tienda física y una plataforma de comercio electrónico. El propósito principal del trabajo es identificar los activos de información críticos, analizar las amenazas y vulnerabilidades a las que está expuesta la organización y proponer controles que permitan fortalecer su seguridad.

El enfoque utilizado se basa en la gestión de riesgos, permitiendo evaluar el impacto y la probabilidad de posibles incidentes de seguridad; durante el desarrollo del seminario se llevaron a cabo actividades como la identificación y clasificación de activos, el análisis de vulnerabilidades presentes en la infraestructura tecnológica y en los procesos organizacionales, así como la identificación de amenazas internas y externas.

Posteriormente, se realizó una evaluación de riesgos mediante la relación entre activos, amenazas y vulnerabilidades, lo cual permitió establecer un panorama claro de los riesgos más críticos para la organización. Entre los principales hallazgos, se destacan debilidades en la gestión de contraseñas, la falta de autenticación en dos factores, la escasa capacitación del personal frente a ataques de phishing y la ausencia de políticas formales de seguridad de la información.

Como resultado, se propusieron diversas medidas de control como la implementación de políticas de seguridad, el fortalecimiento de los mecanismos de autenticación, la realización de copias de seguridad periódicas y la capacitación del personal, el trabajo evidencia la aplicación práctica de los conocimientos adquiridos en ciberseguridad organizacional, permitiendo comprender la importancia de proteger los activos de información y gestionar adecuadamente los riesgos en un entorno empresarial

Palabras clave

1. Phishing
2. Infraestructura
3. Amenazas
4. Vulnerabilidades
5. Activos

Marco conceptual y contextual

Marco Conceptual

La ciberseguridad de una organización incluye estrategias, políticas, procesos y herramientas para proteger sus activos de información frente a amenazas internas y externas. Su objetivo principal es garantizar la confidencialidad, la integridad y la disponibilidad de la información y los sistemas tecnológicos que utiliza la organización.

Según Cisco Cybersecurity, la ciberseguridad protege las redes, los dispositivos, las aplicaciones y los datos frente a ataques digitales que podrían poner en peligro la continuidad del negocio de la empresa (Cisco, 2025). Normas internacionales como ISO/IEC 27001 ofrecen orientación para la implementación de sistemas de gestión de la seguridad de la información mediante controles en las áreas de control de acceso, auditoría, protección de datos y gestión de incidentes (ISO, 2022).

En TechStore S.A.S., la implementación de las mejores prácticas de acuerdo con la ISO 27001 es especialmente importante, ya que la empresa almacena información financiera y datos personales de clientes a través de una plataforma de comercio electrónico. La implementación de controles adecuados reduce el riesgo de acceso no autorizado, pérdida de datos y ciberataques.

Los activos de información incluyen recursos tecnológicos, procesos organizativos, documentos y empleados con acceso a información crítica. Estos activos

pueden verse comprometidos por amenazas como malware, phishing, robo de datos, ataques de denegación de servicio y acceso no autorizado (IBM, 2025). Las vulnerabilidades son brechas de seguridad en sistemas, procesos o comportamientos humanos que pueden ser explotadas por atacantes. La interacción entre amenazas y vulnerabilidades genera riesgos que pueden afectar negativamente las operaciones comerciales, la reputación y la estabilidad financiera de una empresa.

En Colombia, la Ley 1581 de 2012 regula la protección de datos personales y establece obligaciones para el procesamiento seguro de datos (Congreso de Colombia, 2012). Dado que TechStore S.A.S. procesa datos personales y financieros de sus clientes, el incumplimiento de esta normativa podría tener consecuencias legales y dañar la reputación de la empresa.

Este análisis también hace referencia al NIST Cybersecurity Framework, que proporciona orientación para identificar, proteger, detectar, responder y recuperarse de incidentes de ciberseguridad (NIST, 2024). Estas medidas fortalecen la gestión de riesgos y mejoran la protección de los activos de información de una empresa.

Marco Contextual

TechStore S.A.S. es una empresa especializada en la distribución de productos tecnológicos a través de tiendas físicas y una plataforma de ventas en línea. La empresa cuenta con aproximadamente 25 empleados y procesa datos confidenciales relacionados con clientes, proveedores y transacciones financieras.

La infraestructura tecnológica de la empresa incluye una plataforma de ventas web, servidores, sistemas de gestión de inventario, bases de datos de clientes, redes internas y equipos informáticos utilizados por los empleados. Debido a la naturaleza de su negocio, la empresa depende en gran medida de la disponibilidad y seguridad de sus sistemas tecnológicos.

Actualmente, la empresa se enfrenta a diversos desafíos de ciberseguridad, como deficiencias en la gestión de accesos, intentos de fraude en línea, vulnerabilidad a ataques de phishing y la falta de políticas formales de seguridad de la información.

Por lo tanto, este informe busca identificar los riesgos de seguridad más significativos de la empresa y recomienda medidas de control para fortalecer la protección de los activos de información y reducir la probabilidad de ciberataques.

Desarrollo e implementación del aprendizaje

4.1 Identificación de activos

El análisis realizado en TechStore S.A.S. identificó una serie de activos críticos esenciales para las operaciones comerciales de la empresa. Estos activos representan recursos vitales para las actividades comerciales, tecnológicas y administrativas de la compañía, y cualquier interrupción podría ocasionar pérdidas financieras, interrupción de la actividad y daños a la reputación.

Además de los activos tecnológicos, también se identificaron activos humanos y organizativos relacionados con los procesos internos y los empleados con acceso privilegiado a la información.

Tabla 1

Identificación de activos

ACTIVO	**DESCRIPCIÓN**	**IMPORTANCIA**
Base de datos de clientes	Almacena información personal y financiera	Critica
Plataforma web	Permite las ventas en línea	Alta
Sistema de inventario	Gestiona productos y stock	Alta
Red interna	Conecta los sistemas corporativos	Alta

Equipos de cómputo	Herramientas de trabajo de empleados	Media
Credenciales de acceso	Permiten acceso a sistemas internos	Critica
Información financiera	Registro contables y pagos	Critica
Personal administrativo	Gestiona información sensible	Alta
Área de ventas	Ejecuta procesos comerciales	Alta
Atención al cliente	Maneja información de usuarios	Alta
Reputación empresarial	Imagen y confianza de clientes	Crítica

La clasificación de prioridades se determinó en función del impacto operativo y financiero de cada fallo de activo en la continuidad del negocio. Por ejemplo, una interrupción en la plataforma web puede paralizar las ventas en línea, mientras que una base de datos de clientes comprometida puede ocasionar pérdidas financieras y consecuencias legales relacionadas con los datos personales.

4.2 Amenazas y vulnerabilidades

Se han identificado diversas amenazas que podrían comprometer la seguridad de los activos de información de una empresa. Estas amenazas explotan vulnerabilidades en la infraestructura tecnológica y los procesos internos de la compañía.

Tabla 2

Identificación de amenazas y vulnerabilidades

Activo	**Amenaza**	**Vulnerabilidad**
Base de datos	Robo de información	Contraseñas débiles
Página web	Ataque DDoS	Falta de firewall
Equipos	Malware	Software desactualizado
Red interna	Intrusión	WiFi inseguro
Sistema inventario	Acceso indebido	Sin control de accesos
Empleados	Phishing	Falta de capacitación
Informacion financiera	Fraude digital	Falta de monitoreo
Atención al cliente	Ingeniería social	Escasa concientización

Las vulnerabilidades identificadas aumentan significativamente el riesgo de incidentes de seguridad en una organización. Por ejemplo, el uso de contraseñas débiles permite el acceso no autorizado a sistemas críticos, mientras que una capacitación inadecuada incrementa la probabilidad de que los empleados sean víctimas de ingeniería social o ataques de phishing.

Además, la falta de mecanismos de seguridad adecuados en la plataforma web puede dar lugar a ataques de denegación de servicio distribuido (DDoS), que pueden ocasionar interrupciones temporales en las ventas en línea, pérdidas financieras y daños a la reputación de TechStore S.A.S.

Las amenazas de ciberseguridad representan uno de los principales riesgos para las organizaciones modernas debido al crecimiento de ataques digitales dirigidos a plataformas web, redes y bases de datos (HPE, 2025).

4.3 Análisis de riesgos

El análisis de riesgos ayudó a determinar el nivel de vulnerabilidad de la empresa ante diversas amenazas de ciberseguridad, evaluando tanto la probabilidad de que ocurrieran como el impacto potencial en las operaciones comerciales.

Tabla 3

Análisis de riesgos

Activo	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
Base de datos	Robo de información	Contraseñas débiles	Alta	Alto	Critico
Plataforma web	Ataque DDoS	Falta de protección	Media	Alto	Alto

Equipos de cómputo	Malware	Software desactualizado	Alta	Medio	Alto
Red interna	Intrusion	Wifi inseguro	Media	Alto	Alto
Sistema de inventario	Acceso indebido	Sin control de accesos	Media	Medio	Medio
Información financiera	Fraude digital	Falta de monitoreo	Media	Alto	Alto

El riesgo más significativo identificado es el robo de datos de clientes debido a dificultades en el control de acceso y la autenticación. Este incidente puede ocasionar pérdidas financieras, consecuencias legales y daños a la reputación de la empresa.

Asimismo, un ataque DDoS a la plataforma en línea de TechStore S.A.S. podría provocar una interrupción temporal de las ventas en línea y afectar directamente los ingresos y la satisfacción del cliente. Una interrupción prolongada del servicio también podría generar una pérdida de confianza y daños a la reputación.

Además, las infecciones por malware representan una amenaza importante para la continuidad del negocio, ya que pueden comprometer información confidencial,

interrumpir el funcionamiento de los dispositivos y afectar los procesos internos de la empresa.

4.4 Políticas y controles de seguridad

Para mitigar los riesgos identificados, se han propuesto diversas medidas de control técnicas, administrativas y físicas, destinadas a reforzar la seguridad de la información dentro de la organización.

Tabla 4

Identificación de controles

Riesgo identificado	**Control propuesto**
Robo de información	Implementación de autenticación multifactor
Malware	Instalación de antivirus corporativo
Intrusion à la red	Firewall y segmentación de red
Pérdida de información	Copias de seguridad periódicas
Accesos indebidos	Gestión de roles y permisos
Phishing	Capacitación y concientización

La autenticación multifactor mejora la seguridad al acceder a sistemas críticos y bases de datos confidenciales. El firewall, administrado por el personal de TI, supervisa

el tráfico entrante y saliente de la red corporativa. Las conexiones sospechosas se bloquean para minimizar el riesgo de acceso no autorizado.

La implementación de controles de seguridad permite reducir vulnerabilidades y fortalecer la protección de la información empresarial (Cisco, 2025).

Las bases de datos de clientes y la información financiera se respaldan semanalmente y se almacenan en medios de almacenamiento externos seguros para garantizar la recuperación de datos en caso de incidente o fallo del sistema.

La empresa también debe implementar políticas estrictas de protección de datos, establecer controles de acceso, actualizar el software periódicamente y realizar auditorías de seguridad internas trimestrales para identificar vulnerabilidades y mejorar los controles existentes.

La capacitación de los empleados se lleva a cabo trimestralmente mediante talleres sobre temas como la prevención del phishing, la seguridad de los certificados, el comportamiento humano y las mejores prácticas de ciberseguridad.

4.5 Cultura organizacional y concientización

La cultura corporativa es fundamental para TechStore S.A.S. Una gran proporción de los incidentes de seguridad se debe a errores humanos, procedimientos desconocidos o falta de conocimiento por parte de los empleados.

Por lo tanto, es importante implementar programas continuos de capacitación y concientización centrados en las mejores prácticas digitales, la prevención del fraude por correo electrónico, la seguridad de los prestatarios y el manejo adecuado de los recursos tecnológicos de la empresa.

La gerencia de TechStore S.A.S. debe adoptar activamente las iniciativas de seguridad, aplicando políticas internas y fomentando una cultura de protección de la información.

También se recomienda realizar campañas de concientización periódicas, simulacros de ataques de phishing y evaluaciones internas para medir el conocimiento de los empleados sobre las amenazas de seguridad.

La participación activa de los empleados en la protección de los activos de información contribuye significativamente a la reducción de riesgos y a la seguridad general de la empresa.

La capacitación y concientización del personal son fundamentales para reducir errores humanos y fortalecer la seguridad dentro de las organizaciones (IBM, 2025).

Conclusiones

El análisis identificó varias vulnerabilidades en la infraestructura tecnológica de TechStore S.A.S., particularmente en las áreas de gestión de accesos, protección de datos sensibles y la falta de políticas formales de ciberseguridad.

Además, se determinó que los mayores riesgos para la empresa eran el robo de datos, los ataques maliciosos, el phishing y la intrusión en la red interna, todos los cuales podrían tener importantes consecuencias económicas y operativas.

Los controles técnicos y administrativos, como la autenticación multifactor, las copias de seguridad de datos, las políticas de seguridad y la capacitación del personal, reducirían significativamente la vulnerabilidad ante las ciberamenazas.

Finalmente, el informe permitió aplicar los conocimientos adquiridos en el seminario "Gestión de la Ciberseguridad en las Organizaciones" y subrayó la importancia de la gestión de riesgos y la protección de los activos de información en las empresas modernas.

Referencias

Cisco Security: A better way of doing security. (2025, 15 julio). [Vídeo]. Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html

¿Qué es una amenaza de ciberseguridad? | Glosario. (n.d.). HPE LAMERICA. https://www.hpe.com/lamerica/es/what-is/cybersecurity-threats.html

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

Ley 1581 de 2012 - Gestor Normativo. (n.d.). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Jonker, A., Lindemulder, G., & Kosinski, M. (2025, 27 noviembre). Ciberseguridad. *IBM*. https://www.ibm.com/es-es/think/topics/cybersecurity

Cybersecurity Framework | NIST. (2026, May 8). NIST. https://www.nist.gov/cyberframework

¿Qué es la ciberseguridad empresarial? | Defender los activos empresariales. (n.d.). OpenText. https://www.opentext.com/es/what-is/cyber-security

Amazon Web Services. (n.d.). *¿Qué es la ciberseguridad?* Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/cybersecurity/