Seminario en Gestión de Ciberseguridad y Análisis de Ciberseguridad Organizacional

Análisis de Ciberseguridad Organizacional en TechSolutions Ltda.

Corporación Universitaria Remington.

Nombre de la facultad: Ingeniería

Nombre del programa académico: Ingeniería de Sistemas

Cristian Alberto Pineda Romero

Jorge Leonardo Ramírez Restrepo

Seminario en Gestión de Ciberseguridad en Organizaciones con énfasis en riesgos y respuesta a incidentes

2026

Dedicatoria

Este trabajo está dedicado a mi familia, ya que como siempre me han dado todo el apoyo necesario para cumplir mis objetivos y metas, con este trabajo quiero reflejar ese apoyo y entrega que siempre me han brindado.

Agradecimientos

Agradezco al docente por el acompañamiento y las orientaciones brindadas durante el desarrollo de este trabajo. También reconocemos el apoyo de la institución y de nuestras familias, quienes fueron fundamentales durante el proceso académico.

Tabla de Contenidos

Figuras y tablas

Resumen

El presente trabajo analiza la situación actual de ciberseguridad de la empresa TechSolutions Ltda., organización dedicada al desarrollo de software y servicios tecnológicos en Colombia. El estudio se desarrolló con base en principios de gestión de riesgos y en lineamientos de seguridad utilizados actualmente en entornos empresariales.

Durante el análisis se revisaron los activos de información más importantes de la compañía, la infraestructura tecnológica, los mecanismos de acceso, así como las posibles amenazas internas y externas que podrían afectar la operación. También se identificaron vulnerabilidades relacionadas con controles de acceso, gestión de respaldos, monitoreo de eventos y ausencia de políticas formales de seguridad.

Como resultado, se priorizaron riesgos asociados a accesos no autorizados, ransomware y exposición de información financiera. Adicionalmente, se propusieron controles orientados a fortalecer la seguridad de la organización, incluyendo doble factor de autenticación, segmentación de red, monitoreo centralizado y programas de capacitación para usuarios.

El desarrollo de este trabajo permitió evidenciar que la empresa requiere fortalecer su modelo de seguridad de la información para disminuir riesgos operacionales, mejorar la continuidad del negocio y cumplir con requisitos normativos aplicables en Colombia.

Palabras clave: Ciberseguridad, Gestión de riesgos, Activos de información, Vulnerabilidades, Controles de seguridad, Matriz de riesgos, Políticas de seguridad, Respuesta a incidentes, Cultura organizacional

Marco conceptual

La ciberseguridad organizacional comprende el conjunto de controles técnicos, administrativos y operacionales orientados a proteger la confidencialidad, integridad y disponibilidad de la información dentro de una organización (ISO, 2022). En organizaciones como TechSolutions, la protección de datos no solo involucra herramientas tecnológicas, sino también procesos administrativos y buenas prácticas internas.

Dentro del análisis realizado, los activos de información corresponden a todos aquellos recursos que tienen valor para la organización, como bases de datos, servidores, aplicaciones, credenciales y conocimiento técnico del personal. La pérdida o afectación de estos activos podría generar impactos económicos y operacionales.

Las amenazas identificadas incluyen ataques de phishing, ransomware, errores humanos y posibles incidentes relacionados con terceros proveedores. Estas amenazas pueden aprovechar vulnerabilidades presentes en los sistemas, por ejemplo, contraseñas débiles, falta de actualizaciones o ausencia de controles de monitoreo.

El riesgo se entiende como la posibilidad de que una amenaza aproveche una vulnerabilidad y genere consecuencias negativas para la empresa. Por esta razón, resulta importante implementar controles de seguridad que reduzcan la probabilidad de ocurrencia y minimicen el impacto de los incidentes.

Marco contextual

TechSolutions Ltda. desarrolla actividades relacionadas con consultoría tecnológica, desarrollo de software y servicios en la nube. En los últimos años la empresa ha tenido un crecimiento importante en número de empleados y clientes, situación que incrementó la necesidad de fortalecer sus controles de seguridad. El crecimiento acelerado de las organizaciones puede generar debilidades en la infraestructura tecnológica y aumentar la exposición frente a incidentes de seguridad si no existen procesos formales de control y monitoreo (Acosta & García, 2021).

En Colombia, las empresas que administran datos personales deben implementar medidas de protección que garanticen el tratamiento adecuado de la información conforme a la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012). Actualmente la organización administra información de clientes, datos financieros y proyectos tecnológicos que requieren protección adecuada. Aunque existen algunos controles básicos, se evidenció que varios procesos dependen de prácticas informales y no de procedimientos documentados.

Durante el análisis también se identificó que la empresa no cuenta con una estrategia integral de monitoreo ni con políticas formalmente aprobadas para la gestión de incidentes. Esto representa un riesgo importante considerando el aumento de amenazas cibernéticas dirigidas a empresas del sector TI.

Normativa aplicable

La empresa está regulada por normas colombianas e internacionales que enmarcan su obligación de proteger información, tales como:

La Ley 1581 de 2012 establece disposiciones generales para la protección de datos personales en Colombia y define responsabilidades para las organizaciones que administran información sensible (Congreso de la República de Colombia, 2012).

El Decreto 1377 de 2013 reglamenta parcialmente la Ley 1581 y establece lineamientos relacionados con autorización, tratamiento y protección de datos personales (Agencia Nacional del Espectro [ANE], 2013).

Resoluciones SIC (Superintendencia de Industria y Comercio): Define sanciones por incumplimiento de protección de datos.

Los controles propuestos en el presente análisis toman como referencia buenas prácticas de seguridad establecidas en ISO/IEC 27001 y en el NIST Cybersecurity Framework (ISO, 2022; NIST, 2018).

Contratos con clientes: Incluyen cláusulas explícitas de seguridad de datos y confidencialidad

Descripción de la empresa

TechSolutions Ltda. es una empresa colombiana fundada en 2015, ubicada en Bogotá, con presencia en Medellín y Cali. Cuenta con aproximadamente 120 empleados y se especializa en desarrollo de software, consultoría digital y servicios en la nube. Su portafolio de servicios incluye:

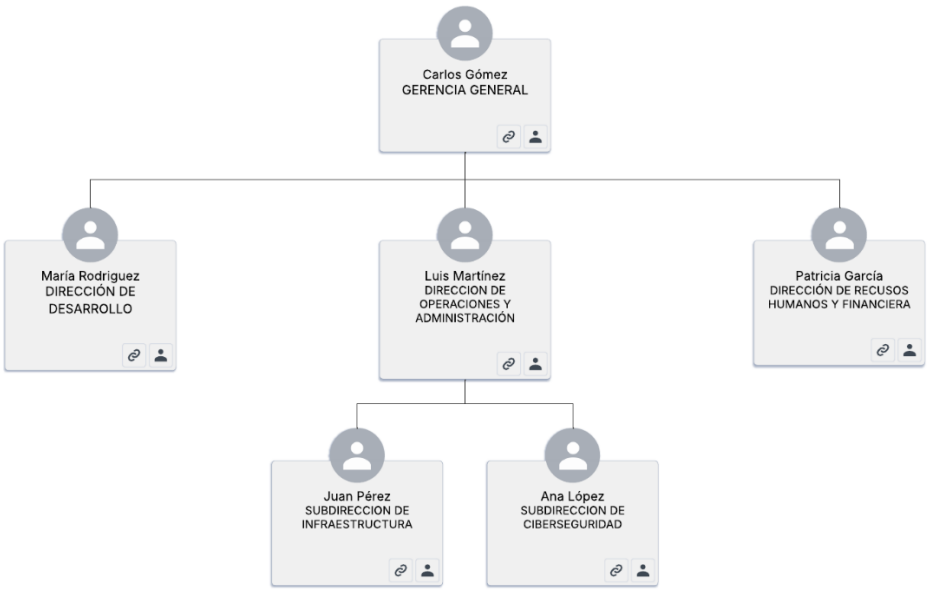
- Desarrollo de aplicaciones web y móviles

- Consultoría en transformación digital
- Implementación de sistemas de información empresarial (ERP)
- Servicios de hosting y infraestructura en la nube
- Soporte técnico y mantenimiento de sistemas

Organigrama.

Figura 1.

Organigrama TechSolutions Ltda.



Nota. Organigrama elaborado para representar la estructura organizacional de TechSolutions Ltda. con base en el caso de estudio desarrollado.

TechSolutions ha experimentado un crecimiento significativo en los últimos 3 años, pasando de 45 a 120 empleados. Este crecimiento ha generado los siguientes cambios a nivel de organización y procesos:

- Oportunidades: Mayor cartera de clientes, diversificación de servicios;

- Desafíos: Gestión de procesos más complejos, necesidad de infraestructura más robusta, mayor riesgo de seguridad de la información;

Hardware

Se realiza identificación del hardware de la organización a nivel nacional con el cual opera en sus diferentes áreas y se de detallan en la tabla a continuación.

Tabla 1.

Hardware empresa TechSolutions

Hardware	Cantidad	Descripción
Servidores	12	servidores físicos en data center local (Bogotá)
Estaciones de trabajo	120	computadores de escritorio (principalmente Windows 10/11)
Dispositivos móviles	85	laptops corporativas (MacBook y Windows)
Dispositivos periféricos	8	Impresoras, routers, switches, UPS
Servidores en la nube	8	instancias en AWS para servicios a clientes

Nota. Inventario de hardware elaborado con base en la infraestructura tecnológica identificada en TechSolutions Ltda.

Software

Se identifica el siguiente software tanto en sistemas operativos como en aplicaciones de ofimática, desarrollo, bases de datos y sistema de telefonía:

- Sistema Operativo: Windows Server 2019/2022, Linux (CentOS)
- Aplicaciones corporativas: ERP: SAP (licencia corporativa), CRM: Salesforce, Correo electrónico: Microsoft 365, Ofimática: Microsoft Office 365
- Herramientas de desarrollo: Visual Studio, Git, Jenkins (para CI/CD)
- Base de datos: SQL Server, PostgreSQL, MongoDB

- Telefonía: Sistema PBX IP local

Red

Se cuenta con la siguiente configuración de red con la cual opera en sus sedes.

- Conexión a internet: Dos enlaces de 100 Mbps redundantes con ISPs diferentes
- Segmento de red: Una red local de clase C (192.168.1.0/24)
- Acceso remoto: VPN con clientes basada en OpenVPN
- Wifi corporativo: Dos SSID (corporativo e invitados)

Situación de Seguridad de la Información

Controles Existentes

La falta de capacitación continua en seguridad puede aumentar los incidentes relacionados con errores humanos y malas prácticas dentro de las organizaciones (López & Hernández, 2020). Esta falta de capacitación y pocas prácticas de auto prevención impactan no solo a la organización internamente si no también su reputación y claridad con clientes existentes y futuros, con el fin de iniciar procesos de prevención mitigación e identificación se identifican los siguientes controles de seguridad para las diferentes capas de acceso a los sistemas o aplicaciones:

- Firewall perimetral básico
- Antivirus instalado en estaciones de trabajo (Windows Defender)
- Contraseñas para acceso a sistemas
- Copias de seguridad manuales (realizadas cada fin de mes)
- Algún personal con acceso VPN

Brechas de Seguridad Identificadas

Realizando un análisis se determinaron las siguientes brechas de seguridad, en las cuales no se evidencia un plan claro para su remediación:

- Falta de política de seguridad formal: No existe documentación oficial de políticas de seguridad;
- Control de acceso débil: Las contraseñas no tienen requisitos de complejidad;
- Sin MFA (doble factor de autenticación): La mayoría de sistemas no requieren MFA;
- Segmentación de red inexistente: Toda la red en un mismo segmento;
- Falta de monitoreo: No hay sistema centralizado de logs;
- Gestión de cambios informal: Los cambios en sistemas no están documentados;
- Capacitación limitada: Los empleados no reciben capacitación regular en seguridad;
- Recuperación ante desastres débil: Plan de continuidad no formalizado;
- Gestión de terceros incompleta: No hay evaluación de seguridad para proveedores;
- Datos sin clasificación: No hay criterios formales de clasificación de datos;

Implementación de políticas y cultura organizacional

Para fortalecer la cultura organizacional en seguridad de la información, TechSolutions debe establecer un programa formal de capacitación dirigido a todos los empleados. Estas capacitaciones deberían realizarse trimestralmente y estar enfocadas en

reconocimiento de correos fraudulentos, manejo seguro de credenciales, protección de información sensible y buenas prácticas de navegación.

El área de tecnología y seguridad de la información sería responsable de coordinar las jornadas de formación, realizar evaluaciones periódicas y verificar el cumplimiento de las políticas definidas por la organización. Adicionalmente, se recomienda implementar controles diferenciados de acceso según el rol de cada usuario, restringiendo privilegios administrativos únicamente al personal autorizado.

También resulta importante formalizar políticas relacionadas con uso de dispositivos corporativos, acceso remoto, clasificación de información y gestión de contraseñas. Estas políticas deben ser comunicadas oficialmente y revisadas periódicamente para garantizar su cumplimiento y actualización frente a nuevas amenazas.

Desarrollo e implementación del aprendizaje

Esta sección presenta la aplicación práctica de conceptos de gestión de riesgos en TechSolutions, incluyendo identificación de activos, análisis de amenazas y vulnerabilidades, evaluación de riesgos mediante matriz, definición de políticas, plan de respuesta a incidentes y cultura organizacional.

Identificación de activos

La identificación de activos críticos es una actividad fundamental dentro de la gestión de riesgos de seguridad de la información, ya que permite determinar los recursos que requieren mayor nivel de protección (ISO, 2022). Se determinan los siguientes

activos de información críticos con base a la estructura de la organización, infraestructura y procesos:

Activos Tecnológicos Críticos:

- Servidores y servicios en la nube (12 servidores locales + 25 instancias AWS)
- Bases de datos de clientes (información confidencial regulada por Ley 1581)
- Aplicaciones web y móviles (propiedad intelectual de la empresa)
- Sistemas de información empresarial (SAP ERP, Salesforce CRM)
- Equipos de cómputo y dispositivos móviles corporativos (120 computadores, 85 laptops)
- Infraestructura de red (firewalls, VPN, switches, routers)

Activos de Información Críticos:

- Información financiera (nómina, estados financieros, facturas, presupuestos)
- Credenciales y llaves de API (acceso a sistemas y servicios)
- Datos de clientes (contactos, historiales, contratos, documentación de proyectos)
- Código fuente de aplicaciones desarrolladas

Activos Humanos y Organizacionales:

- Personal especializado (desarrolladores, administradores, especialista de seguridad)
- Conocimiento y experiencia en desarrollo de software
- Relaciones con clientes y reputación corporativa

Análisis de amenazas

Los ataques de phishing y ransomware continúan siendo una de las principales amenazas para organizaciones del sector tecnológico en Latinoamérica (Centro Cibernético Colombiano, 2022). Por esta razón se identifican las posibles amenazas a las que la organización puede verse expuesta o vulnerable.

Se realiza un análisis de amenazas externas donde se logran identificar las siguientes amenazas que pueden vulnerar o afectar a la organización y se relacionan en la tabla a continuación.

Tabla 2.

Identificación amenazas externas

Amenaza	Descripción	Probabilidad	Impacto
Ataques de Phishing	Correos fraudulentos dirigidos a empleados para obtener credenciales.	Alta	Alto
Malware y Ransomware	Software malicioso que compromete sistemas y demanda rescate.	Media-Alta	Crítico
Ataques DDoS	Saturación de servicios para interrumpir disponibilidad.	Media	Alto
Ataques dirigidos (APT)	Ciberdelincuentes profesionales enfocados en robo de información.	Media	Crítico
Fugas de información	Divulgación de datos confidenciales de clientes.	Media	Crítico

Nota. Las amenazas externas fueron identificadas considerando el contexto operativo y tecnológico de TechSolutions Ltda.

Dentro del análisis realizado de amenazas también se identificaron amenazas internas que pueden llegar a ser las de mayor riesgo si no se cuenta con los lineamientos adecuados y se describe en la siguiente tabla.

Tabla 3.

Identificación de amenazas internas

Amenaza	Descripción	Probabilidad	Impacto
Errores humanos	Configuraciones incorrectas, eliminación accidental de datos.	Alta	Medio-Alto
Amenazas internas maliciosas (Insider threats)	Empleados malintencionados accediendo a información sensible.	Baja-Media	Crítico
Falta de cumplimiento normativo	Incumplimiento de políticas de seguridad.	Media	Alto

Nota. Las amenazas internas fueron definidas a partir de posibles riesgos asociados a procesos y personal de la organización.

Con un análisis más detallado se determinan las posibles amenazas que pueden derivar de la cadena de suministros como se expone en la siguiente tabla.

Tabla 4.

Identificación de amenazas a la cadena de suministros.

Amenaza	Descripción	Probabilidad	Impacto
Compromiso de proveedores (AWS, Microsoft 365, Salesforce)	Vulnerabilidades en servicios terceros.	Baja	Crítico

Nota. La identificación de amenazas de terceros se realizó considerando los proveedores tecnológicos utilizados por la organización.

Análisis de vulnerabilidades

Durante el análisis también de identificaron las principales vulnerabilidades que podrían afectar la operación y seguridad de la organización y a lo que se debe dar una solución o mitigación con el fin de ser proactivos ante cualquier posible amenaza o incidente de seguridad de la información lo que puede generar una alteración en la operación diaria de la organización.

Durante el análisis se determinan vulnerabilidades con un nivel crítico, que deben ser mitigadas de manera prioritaria y se detallan en la siguiente tabla.

Tabla 5.

Identificación de vulnerabilidades críticas.

Vulnerabilidad	Descripción	Nivel
Falta de políticas de seguridad claras	No existe documentación formal de políticas de seguridad.	Crítico
Contraseñas débiles	Ausencia de requisitos de complejidad y cambio regular.	Crítico
Sin MFA (Doble Factor de autenticación)	La mayoría de sistemas no requieren segunda capa de autenticación.	Crítico
Control de acceso insuficiente	Acceso excesivo de usuarios a recursos sensibles.	Crítico

Nota. Las vulnerabilidades críticas corresponden a debilidades que podrían comprometer directamente activos sensibles de la organización.

Se obtuvo una serie de vulnerabilidades altas las cuales representan un riesgo importante y deben ser contenidas con controles preventivos y correctivos las cuales se identifican en la siguiente tabla.

Tabla 6.

Identificación de vulnerabilidades altas

Vulnerabilidad	Descripción	Nivel
Falta de capacitación en ciberseguridad	Los empleados no reciben entrenamiento regular.	Alto
Sistemas sin actualizaciones	Servidores y aplicaciones sin parches de seguridad.	Alto
Segmentación de red inexistente	Toda la red en un mismo segmento, sin DMZ.	Alto
Falta de monitoreo centralizado	No hay SIEM (Security Information and Event Management).	Alto

Nota. Las vulnerabilidades altas representan riesgos importantes que requieren controles preventivos y correctivos.

Continuando con el análisis se evidencias una serie de vulnerabilidades de nivel medio las cuales se clasificaron por su impacto y nivel de exposición frente a la organización y se resume en la siguiente tabla.

Tabla 7.

Identificación de vulnerabilidades medias

Vulnerabilidad	Descripción	Nivel
Falta de encriptación de datos en tránsito	Algunos datos transmitidos sin cifrado.	Medio
Gestión de cambios informal	Los cambios en sistemas no están documentados.	Medio
Evaluación de proveedores incompleta	No hay auditoría formal de seguridad en terceros.	Medio
Datos sin clasificación	No existe esquema formal de clasificación de datos.	Medio

Nota. Las vulnerabilidades medias fueron clasificadas de acuerdo con su impacto potencial y nivel de exposición actual.

Las vulnerabilidades identificadas permiten que diferentes amenazas afecten directamente los activos críticos de la organización. Por ejemplo, la ausencia de doble factor de autenticación (MFA) y el uso de contraseñas débiles incrementan el riesgo de acceso no autorizado a bases de datos de clientes y sistemas financieros. De igual forma, la falta de capacitación en seguridad de la información facilita ataques de phishing dirigidos al personal, comprometiendo credenciales corporativas y acceso a servicios internos.

Asimismo, la inexistencia de segmentación de red y monitoreo centralizado aumenta la posibilidad de propagación de malware o ransomware dentro de la infraestructura tecnológica. En consecuencia, los controles propuestos buscan reducir la

probabilidad de materialización de estas amenazas mediante políticas de acceso seguro, monitoreo continuo, capacitación y fortalecimiento de la infraestructura.

Análisis de riesgo

Se ha desarrollado una matriz de riesgos integral que permite identificar, evaluar y priorizar los riesgos encontrados en TechSolutions para determinar las acciones de mitigación más apropiadas. La matriz incluye 12 riesgos que abarcan toda la cadena de valor: datos de clientes, infraestructura, acceso remoto, integridad de sistemas, y relaciones con proveedores.

El riesgo se puede expresar de la siguiente manera: **Riesgo = Probabilidad × Impacto**

Tabla 8.
Matriz de identificación y evaluación del riesgo

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	Controles Propuestos
R1	Base de datos clientes	Acceso no autorizado	Contraseñas débiles, sin MFA	Media	Crítico	Alto	MFA, contraseñas fuertes, encriptación
R2	Servidores en la nube (AWS)	Ransomware	Falta de backups validados	Media-Alta	Crítico	Alto	Backups automatizados, plan de recuperación
R3	Información financiera	Fuga de datos	Control de acceso débil	Media	Crítico	Alto	RBAC, auditoría de accesos, DLP
R4	Correos corporativos	Phishing	Falta de capacitación	Alta	Alto	Alto	Formación, filtros, MFA
R5	Servidores locales	Malware	Software desactualizado	Media	Alto	Alto	Parches, antivirus, filtrado web
R6	Aplicaciones web	Ataques DDoS	Infraestructura débil	Baja-Media	Alto	Medio-Alto	WAF, redundancia, CDN
R7	Red interna	Intrusión	Falta de monitoreo	Media	Alto	Medio-Alto	SIEM, IDS/IPS, segmentación
R8	Personal	Error humano	Falta de políticas claras	Alta	Medio	Medio-Alto	Políticas formales, capacitación
R9	Acceso remoto (VPN)	Acceso no autorizado	Control débil de VPN	Media	Alto	Medio-Alto	Auditoría VPN, MFA en VPN
R10	Aplicaciones de terceros	Compromiso de proveedores	Evaluación incompleta	Baja	Crítico	Medio	Evaluación SLA, auditorías
R11	Datos en tránsito	Interceptación	Falta de encriptación	Baja-Media	Alto	Bajo-Medio	TLS/SSL, VPN, HTTPS
R12	Sistemas	Obsolescencia	Versiones antiguas	Media	Medio	Medio	Plan de actualización

Nota. La matriz de riesgos fue elaborada con base en la identificación de activos, amenazas, vulnerabilidades y controles aplicables en TechSolutions Ltda.

Interpretación de la matriz

Riesgos Críticos: Requieren acción inmediata. Implementación de controles en máximo 1-2 meses. Estos riesgos pueden paralizar la empresa o causar daño legal/regulatorio significativo.

Riesgos Altos: Deben ser mitigados en el corto plazo (3-6 meses). Su materialización afectaría operaciones o causaría pérdida de datos.

Riesgos Medios: Incluirse en plan de mejora continua (6-12 meses). Impacto menor, pero deben ser atendidos en la estrategia integral.

Normativa aplicable

La Superintendencia de Industria y Comercio también establece lineamientos y sanciones relacionadas con el incumplimiento de medidas de protección de datos personales en Colombia (SIC, 2020). Según el análisis realizado a la empresa TechSolutions, se determina que para una práctica eficaz y eficiente y con el fin de prevenir que se presenten más situaciones en las que no es clara la información de responsables, buenas prácticas y brechas de seguridad se deben aplicar las siguientes normativas teniendo en cuenta los aspectos más importantes de la actividad que ejecuta TechSolutions.

Ley 1581 de 2012 (Habeas Data - Protección de Datos Personales)

Decreto 1377 de 2013 (Regulación de procesamiento de datos)

Resoluciones SIC (Superintendencia de Industria y Comercio)

Norma ISO/IEC 27001 (Estándar de gestión de seguridad de información)

NIST Cybersecurity Framework (Marco de referencia de seguridad)

Contratos con clientes: Incluyen cláusulas de seguridad de datos

Plan de respuesta a incidentes

Durante el análisis realizado a TechSolutions Ltda. se evidenció que la organización no cuenta con un procedimiento formal para la gestión y respuesta ante incidentes de seguridad de la información. Esta situación representa un riesgo importante, ya que ante eventos como ataques de ransomware, accesos no autorizados, pérdida de información o campañas de phishing, la empresa podría presentar retrasos en la contención del incidente y afectar la continuidad de la operación.

Actualmente varios procesos dependen de acciones informales del personal de tecnología, sin una estructura clara de escalamiento, comunicación y recuperación. La ausencia de lineamientos definidos también dificulta la identificación temprana de incidentes y aumenta la probabilidad de impacto sobre activos críticos, bases de datos y servicios empresariales.

Con base en lo anterior, se propone implementar un plan de respuesta a incidentes que permita actuar de manera organizada frente a eventos de seguridad. Este plan debe incluir las siguientes fases con el fin de garantizar una respuesta oportuna frente a incidentes:

Identificación del incidente

Consiste en detectar actividades inusuales dentro de la infraestructura tecnológica, tales como accesos sospechosos, tráfico no autorizado, fallos repetitivos, malware o intentos de phishing. Para ello se recomienda implementar monitoreo centralizado de eventos y herramientas de registro de logs.

Contención

Una vez identificado el incidente, se deben aplicar medidas inmediatas para evitar su propagación. Entre las acciones recomendadas se encuentran:

- Aislamiento de equipos comprometidos.
- Bloqueo de cuentas afectadas.
- Suspensión temporal de accesos remotos.
- Segmentación de servicios comprometidos.

Estas medidas buscan reducir el impacto sobre la operación y proteger la información crítica.

Erradicación y recuperación

Después de contener el incidente, la organización debe eliminar la causa raíz del problema. Esto puede incluir:

- Eliminación de malware.
- Actualización de sistemas vulnerables.
- Cambio de credenciales comprometidas.
- Restauración de respaldos validados.

Posteriormente, se deben recuperar los servicios afectados verificando que los sistemas funcionen correctamente antes de volver a operar normalmente.

Comunicación y escalamiento

Se recomienda definir responsables específicos para la gestión de incidentes, estableciendo niveles de escalamiento dependiendo de la criticidad del evento. Además, debe existir comunicación clara con:

- Dirección de la empresa.
- Personal de TI.
- Clientes afectados.
- Proveedores tecnológicos.

En incidentes relacionados con datos personales, también se deben considerar las obligaciones legales establecidas por la normatividad colombiana.

Lecciones aprendidas y mejora continua

Finalmente, después de cada incidente, la empresa debe realizar un análisis de causas y documentar las acciones ejecutadas. Esto permitirá identificar debilidades en los controles actuales y fortalecer continuamente las políticas y procedimientos de seguridad.

La implementación de este plan permitiría a TechSolutions mejorar significativamente su capacidad de reacción frente a incidentes cibernéticos, reducir tiempos de recuperación y disminuir el impacto operacional y reputacional derivado de eventos de seguridad.

Escenario práctico de aplicación

En un escenario hipotético de ransomware, un empleado recibe un correo fraudulento y descarga un archivo malicioso que compromete varios equipos de la organización. Ante esta situación, TechSolutions debería activar inmediatamente el plan de respuesta a incidentes, iniciando con la identificación del comportamiento anormal mediante herramientas de monitoreo y reportes del personal.

Posteriormente, el área de TI deberá aislar los equipos comprometidos para evitar la propagación del malware hacia servidores y servicios críticos. Después de la

contención, se procederá con la eliminación del software malicioso, restauración de respaldos previamente validados y cambio de credenciales comprometidas.

Finalmente, la organización deberá documentar el incidente, comunicar lo sucedido a las áreas afectadas y fortalecer las medidas preventivas mediante capacitación al personal y ajustes en los controles de seguridad.

Conclusiones

A partir del análisis realizado, se concluye que TechSolutions presenta debilidades relevantes en materia de seguridad de la información, especialmente en controles de acceso, gestión de respaldos y monitoreo de eventos de seguridad. Aunque la empresa dispone de mecanismos básicos de seguridad, todavía existen procesos que no están formalizados y dependen de prácticas operativas poco estandarizadas.

Uno de los aspectos más críticos identificados corresponde a la ausencia de doble factor de autenticación y políticas robustas de contraseñas, situación que aumenta la posibilidad de accesos no autorizados. De igual forma, la falta de validación periódica de copias de seguridad podría afectar la recuperación de la operación ante incidentes como ransomware.

También se evidenció la necesidad de fortalecer la cultura organizacional en seguridad, debido a que gran parte de los riesgos identificados involucran errores humanos y falta de capacitación del personal.

Finalmente, se considera que la implementación gradual de controles alineados con ISO 27001 y NIST permitiría reducir significativamente la exposición de la organización frente a incidentes de seguridad, mejorar la continuidad del negocio y aumentar la confianza de clientes y aliados comerciales.

Adicionalmente, el desarrollo de este seminario fortaleció competencias relacionadas con la gestión de ciberseguridad organizacional, especialmente en procesos de identificación de activos, análisis de amenazas y vulnerabilidades, evaluación de riesgos y definición de controles de seguridad. A través del análisis realizado se comprendió la importancia de establecer políticas claras, mecanismos de respuesta ante

incidentes y estrategias orientadas a la consolidación de una cultura de seguridad dentro de la organización. Este proceso formativo también facilitó la relación entre conceptos teóricos y escenarios empresariales reales, aportando una visión más práctica sobre la protección de activos críticos, la continuidad operativa y el cumplimiento normativo dentro de las organizaciones.

De igual forma, no implementar los controles y mejoras propuestas podría generar consecuencias significativas para TechSolutions, incluyendo pérdida de información sensible, afectaciones económicas, interrupción de servicios y deterioro de la confianza de clientes y aliados estratégicos. En organizaciones que dependen altamente de servicios tecnológicos, la ciberseguridad no solo representa un componente técnico, sino también un elemento clave para garantizar la continuidad operativa, la estabilidad del negocio y la reputación corporativa frente a un entorno digital cada vez más expuesto a amenazas.

Referencias

Acosta, J. E., & García, M. (2021). Análisis de vulnerabilidades en PYMES de Latinoamérica. *Revista Colombiana de Ciberseguridad, 5*(2), 45-62.

Agencia Nacional del Espectro (ANE). (2013). *Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. Diario Oficial de la República de Colombia.

Banco Interamericano de Desarrollo (BID). (2021). *Seguridad digital en América Latina: Diagnóstico y recomendaciones*. BID.

Centro Cibernético Colombiano. (2022). *Informe de amenazas cibernéticas en empresas de TI, 2022*. Ministerio de Tecnologías de la Información y Comunicaciones.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial de la República de Colombia.

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 Information security management systems – Requirements*. ISO.

López, R., & Hernández, S. (2020). Cultura organizacional y ciberseguridad: Un estudio en empresas medianas de Colombia. *Revista Iberoamericana de Tecnología e Información, 12*(3), 78-95.

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. U.S. Department of Commerce.

Superintendencia de Industria y Comercio (SIC). (2020). *Resoluciones de protección de datos personales*. República de Colombia.