TRABAJO DE GRADO
Opción Seminario-Diplomado.

Informe técnico empresa TECNO S.A.S.

Corporación Universitaria Remington.

Facultad Ingenierías

Ingeniería de sistemas

Jhon Alexander Carmona Carmona y Yeferson Osorio Zapata.

Doc. Jorge Leonardo Ramírez

Seminario ciberseguridad

2026.

Tabla de Contenidos

Resumen

Este informe está enfocado en la infraestructura de TECNO S.A.S en cual se realiza un análisis de brechas y la simulación de un ataque de ransomware controlando para evaluar la capacidad de respuesta de la organización

El ejercicio abarca sitios web publicados en la WAN y servidores alojados en el Data Center, en el cual se evidenciaron vulnerabilidades criticas asociadas al factor humano como la susceptibilidad al phishing, y la entrega de credenciales, a partir de este hallazgo se estructura un plan de mejoras que incluyen la contratación de servicios de auditoria ofensiva de caja blanca y gris. Permitiendo a la entidad mitigar riesgos proteger sus bases de datos registrales y fortalecer el sistema de gestión de seguridad de la información.

Palabras clave

Ciberseguridad organizacional, Ransomware, Ingeniería social, Respuestas a incidentes , SGSI, Normatividad, ISO 27001

Marco conceptual y contextual

La protección de activos críticos exige una compresión profunda de las metodologías de ataques y los marcos de defensa normativa con la ISO 27001, TECNO S.A.S gestiona información altamente sensible mediante una infraestructura tecnológica que abarca servidores con sistemas operativos Windows en su data center (como DC-TECNO y BACKUPHPE-TECNO) servicios en AWS S3 y firewalls perimetrales (FG 100F, FGT40).

A pesar de contar con seguridad perimetral los ciberdelincuentes modernos en especial los grupos de amenazas persistentes avanzadas (APT) enfocan sus esfuerzos en la cadena de suministros y en el factor humano aprovechando entrega de contraseñas e información confidencial por parte de los colaboradores este informe analiza la materialización de un riesgo critico en este contexto y propone un marco defensivo de hiper-resiliencia

Análisis del incidente de Seguridad

Vector de ataque Inicial:

Compromiso de la cadena de suministro mediante la vulneración del dominio de correo de un proveedor legitimo

Técnica de Intrusión:

Campañas de Spear Phishing dirigida a colaboradores con privilegios de acceso utilizando ingeniería social para forzar la descarga de un documento adjunto ofuscado (Dropper)

Ejecución y evasión:

Ejecución exitosa del PayLoad malicioso en el endpoint logrando inyección en memoria y evadiendo los controles perimetrales iniciales para establecer una conexión de comando y control (C2).

Detección y Contención:

Identificación de la amenaza en fase de movimiento lateral mediante la telemetría del sistema Bit defender se detectaron intentos de escalamiento de priviligecios y escaneo de red dirigidos al control de dominio y servidores de respaldo lo que desencadeno el aislamiento automático del EndPonit.

Desarrollo e implementación del aprendizaje

El incidente demostró que las herramientas activadas y desplegadas por la institución no son suficientes para poder mitigar estos escenarios de alta severidad y proteger los 18 sitios web y 9 servidores se estructuro el siguiente plan de acción:

Auditoria Ofensiva Avanzada:

Se ejecutará un modelo de intrusión profundo de caja blanca y gris con esto garantizamos la ejecución de pruebas completas de ingeniería social (Phishing, llamadas y chat corporativo) permitiendo a TECNO S.A.S medir su resisliciencia real ante la manipulación psicológica de su empelados

Arquitectura Zero Trust y Sandboxing:

Implementar entornos aislados (sandbox) en la pasarela de correo para la detonación y análisis dinámico de adjuntos sospechosos antes de que alcancen la bandeja de colaborador

Endurecimiento del Endpoint:

Optimizar la configuración Bit defender hacia un modelo estricto de respuesta extendida (XDR) automatizando el aislamiento de red (Network Containment)de cualquier máquina que presente anómalos de lectura masiva de archivos

Cultura de Ciberseguridad (HUMAN FIREWALL):

Para poder erradicar la susceptibilidad a ataques de phishing se implementará un programa continuo de simulación inmersivos

Activos

TECNO S.A.S gestiona un conjunto de activos críticos de información que sustentan su operatividad. Estos activos incluyen recursos humanos, tecnológicos, de infraestructura datos sensibles cuya protección es prioritaria dentro del sistemas de gestión de seguridad de la Información (SGSI)

Entre los activos más relevantes se identifican: el personal administrativo y técnico con acceso privilegiado a la red la plataforma de correo electrónico corporativo (NUVA) las estaciones de trabajo (endpoints), la base de datos de clientes con información de facturación y datos personales y el controlador de dominio que gestiona permisos y accesos en toda la infraestructura
Adicionalmente la empresa opera 18 sitios web publicados en la WAN y 9 servidores en su Data Center incluyendo DC-TECNO y BACKUPHPE-TECNO con servicios en AWS S3 y firewalls perimetrales FG 100F y FGt40

Tabla 1. Inventario de Activos Críticos de Información y Superficie de Ataque

Categoría de Activo	Activo	Descripción	Responsable	Criticidad
Humana	Empleados	Personal administrativo y técnico con acceso a la red	G. Humana /TI	Alta
software	Correo electrónico (NUVA)	Herramientas de comunicación externa con proveedores y clientes	Administrador TI	Alta
Hardware	Endpointd (Estaciones de trabajo)	Equipos Físicos utilizados por los empleados para su labor diaria	Soporte Técnico	Media
Datos	BD de Clientes	Información sensible de facturación y datos personales	Dirección Financiera	Critica
Infraestructura	Controlador de dominio	Servidor que gestiónalos permisos y accesos de toda la red	Administrador de red	Critica

Amenazas y Vulnerabilidades

El análisis de amenazas y vulnerabilidades realizado sobre la infraestructura de TECNO S.A.S identifico cuatro vectores críticos que representan el mayor riesgo parala continuidad operacional de la organización

1 ingeniería social (Phishing /Spear Phishing)

la principal vulnerabilidad identificada es la susceptibilidad del factor humano ante técnicas de engaño los colaboradores con privilegios de acceso son blanco de campaña dirigidas que aprovechan la confianza depositada en proveedores legítimos la ausencia de protocolos de verificación de comunicaciones externas facilitar la entrega de credenciales e información confidencial

2 robo de credenciales y ausencia de MFA

La gestión de identidades no cuenta con mecanismos de autenticación multifactorial (MFA)lo que facilita el acceso no autorizado una vez comprometidas las credenciales. esta vulnerabilidad expone directamente el controlador de dominio y los sistemas de respaldo

3 ejecución de malware en endpoints

Los equipos de trabajo carecen de configuraciones estrictas que bloquean la ejecución de adjuntos maliciosos la ausencia de análisis dinámico (sandbox) en la pasarela de correo permitió que un Dropper ofuscado alcanzara el endpoint y ejecutara en payload estableciendo una conexión de comando y control (C2)

4 segmentación de red ineficiente

La infraestructura no cuenta con una segmentación adecuada que aísla los servidores de respaldo de resto de la red facilitando el movimiento lateral del atacante hacia activos críticos como el controlador de dominio y los Backups.

Figura2: Proceso de vulnerabilidad

Riesgos

La evaluación de riesgo de TECNO S.A.S se a realizo considerando la probabilidad de ocurrencia y el impacto potencial sobre la confidencialidad, integridad y disponibilidad de activos de información, los riegos se clasifican según la siguiente escala:

- **Extremo** (acción inmediata)
- **Alta** (acción prioritaria)
- **Media** (acción programada)
- **Baja** (monitoreo continuo)

Los riesgos críticos identificados son:

1- Riesgo **extremo** de compromiso de factor humano mediante ingeniería social con alta probabilidad e impacto crítico sobre toda la cadena operativa
2- Riesgo **extremo** de infección por malware en endpoint con alta probabilidad dado el flujo constante de correos externos
3- Riesgo **Alto** de robo de credenciales por ausencia de MFA que expone directamente el Active Directory
4- Riesgo **alto** de movimiento lateral hacia infraestructura Core por segmentación deficiente que podría comprometer la disponibilidad total de los sistemas estos riesgos están detallados en la tabla 3 de este informe

Tabla 3. Matriz de Hallazgos y Vulnerabilidad Identificadas

Activo Afectado	Amenaza	Vulnerabilidad Identificada	Probabilidad	Impacto	Nivel de Riesgo	Control Propuesto (Acción)
Factor Humano	Ingeniería social (Phishing)	Susceptibilidad a engaños /Falta de concientización	Alta	critico	Extremo	Cultura de ciberseguridad (simulaciones continuas)
Gestión de Identidad	Robo de Credenciales	Ausencia de validación robusta /MFA	media	Alto	Alto	Auditoría Ofensiva /Arquitectura Zero Trust
Endpoints (PC)	Infección por Malware	Ejecución de adjuntos maliciosos no bloqueados	Alta	Critico	Extremo	Endurecimiento del Endpoint (implementación XDR)
Infraestructura Core	Movimiento Lateral	Segmentación de red ineficiente hacie Backups	Baja	Critico	Alto	Entornos aislados y Sandboxing

Políticas y controles

Con base a los a hallazgos en los incidentes encontrados basándonos en la ISO/IEC 27001:2022, se proponen las siguientes políticas y controles:

Política de control de acceso: Se debe usar obligatoriamente la autenticación multifactorial, para todos los usuarios que tengan accesos a sistemas críticos, se deben usar roles y funciones dentro de la organización.

Política de seguridad en el correo: Todo archivo adjunto externo debe ser sometido a un análisis dinámico en entorno sandbox antes de ser entregado al destinatario

Política de gestión de endpoints: Configuración de Bit defender en modo XDR estricto con aisalamiento automatico de la red ante comportamientos inusuales, se procede al bloqueo de macros y archivos que no estén firmados digitalmente en todos los endpoints

Incidentes y respuesta:

El incidente de ransomware simulado permitió evaluar de forma controlada la capacidad de respuesta de TECNO S.A.S. ante una amenaza de alto nivel. A continuación, se da a conocer la cadena de respuesta ejecutada y las lecciones aprendidas.

Fase de detección: la telemetría de bitdefender detecto patrones de lectura masiva de archivos y escaneo de red en fase de movimientos lateral, identificado con intentos de escalamiento de orivilegios dirigidos al controlador del dominio y servidor.

Fase de contención: Se ejecuto el aislamiento automático del endpoint comprometido, evitando la propagación lateral del codigo malisioso hacia los otros sistemas de la red.

Fase de erradicación: Se procedió al análisis forense del endpoint, eliminación del payload malicioso y restitución del sistema desde imágenes limpias. Y los accesos que fueron comprometidos fueron revocados y las contraseñas fueron restablecidas para todos los usuarios que fueron afectados.

Fase de lección aprendida: Con el ejercicio logro evidenciar que los controles perimetrales existentes son insuficientes ante los ataques dirigidos al factor humano. Se recomienda formalizar un plan de respuesta ante los incidentes documentando los roles y responsabilidades, tiempos de respuesta y comunicación interna y externa durante una crisis.

Cultura Organizacional

La cultura de seguridad de la información es el pilar fundamental para la sostenibilidad del SGSI en TECNO S.A.S el incidente demostró que la inversión en tecnología no es suficiente si los colaboradores no están preparados para reconocer y resistir técnicas de ingeniería social por ello se propone un programa integral de cultura organizacional en ciberseguridad articulado en tres ejes:

Eje 1 – Programa Human Firewall

Implementación de simulación continuas e inmersivas de phishing, vishing y smishig dirigidas a todos los niveles de la organización. Las simulaciones se realizarán de forma periódica (mensual o trimestral) con retroalimentación inmediata y formación remedial para quienes caigan en el engaño

Los resultados serán medidos mediante indicadores de tasa de clic reporte de incidentes y tiempo de detección.

Eje 2 – Capacitación y concientización

Desarrollo de un plan anual de capacitación en seguridad de la información obligatorio para todos los empleos y diferenciado por rol los contenidos incluirán identificación de correos maliciosos manejo seguro de contraseñas uso responsable de dispositivos corporativos y protocolos de reporte de incidentes

Eje 3 – Gobernanza y liderazgo en seguridad

El compromiso de alta dirección es indispensable para consolidar una cultura de seguridad solida se propone la designacion formal de un responsanle de seguridad de la informacion (CISO o equivalente) la inclusion de objetivos de seguridad en los planes estrategicos anuales y la realización de revisiones periódicas del SGSI con reporte a la direccion ejecutiva en cumplimiento del articulo 9 de la ISO / IEC 27001:2022

Tabla 2.

Análisis Comparativo de Proveedores de Auditoria de Seguridad

Proveedor Evaluado	Tipo de pruebas	Alcance Ingeniería Social	Valor de la Propuesta
Juan Felipe	Caja Blanca y Gris	Completo (Phishing, Vishing, Chat)	$19´0000.000
Dinco TI SAS	Caja Gris	Detallado (Phishing)	$37´000.000
AntiFraude /Schart	Red team (Real)	Muy Robusto (Persistencia)	$38´900.000
Infocomunicaciones SAS	Caja Negra Limitada	Básico (Correo y SMS)	16´660.000

Conclusiones

Se identifico que, a pesar de contar con herramientas perimetrales, el factor humano sigue siendo el eslabón más crítico en la cadena de seguridad la materialización

del riesgo de Spear Phishing demostró que la confianza en las comunicaciones con proveedores debe ser validada mediante políticas estrictas de verificación

La implementación de tecnologías de tecnologías de detección basadas en comportamiento (EDR), como Bitdefender, resulto ser el control más efectivo para contener el movimiento lateral del Ransomware. Esto resalta la necesidad la necesidad la migrar de esquemas de protección pasivos a sistemas de respuesta activa ante incidentes

El fortalecimiento del SGSI bajo el marco de la ISO 27001 no solo protege la operatividad de TECNO S.A.S. sino que asegura el cumplimiento legal frente a la ley 1581 de 2012 mitigando riesgos reputacionales y sanciones económicas derivadas de una posible fuga de datos.

Referencias

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 n.° 48587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Hadnagy, C. (2018). Social engineering: The science of human hacking (2.ª ed.). John Wiley & Sons.

Mitre Corporation. (2023). MITRE ATT&CK: Adversarial tactics, techniques and common knowledge. https://attack.mitre.org/

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (versión 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Organización Internacional de Normalización. (2022). Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos (ISO/IEC 27001:2022). ISO.

Sikorski, M., y Honig, A. (2012). Practical malware analysis: The hands-on guide to dissecting malicious software. No Starch Press.

TECNO S.A.S. (2026a). Análisis comparativo de cotizaciones: Pruebas de vulnerabilidad a sitios publicados [Documento interno]. Dirección Administrativa y Financiera.

TECNO S.A.S. (2026b). Solicitud de cotizaciones: Pruebas de vulnerabilidad a sitios públicos y servidores del data center [Documento interno]. Sistema de Gestión de Seguridad de la Información.

World Economic Forum. (2022). The global risks report 2022 (17.ª ed.). WEF. https://www.weforum.org/reports/global-risks-report-2022/