ESCUELA SUPERIOR DE GUERRA
"General Rafael Reyes Prieto"
Colombia

Defensa en Profundiadad: Fortaleza Digital de "TechSolutions Corp.

MY. URIBE CARLOS - MY. MAHECHA ALEXANDER – CC. CONTRERAS RUBEN
MY. DANIEL TORRES - MY. MARIO GÓMEZ – MY. MANUEL REY – CC. MARTÍNEZ JOHAN
MY.

AGENDA

01 Presentación Integrantes

02 Caso de Estudio

03 Fases 1, 2 y 3

04 Técnica de Explotación

05 Defensa de Profundidad

06 Conclusiones

07 Bibliografía

2. CASO DE ESTUDIO

Contexto: TechSolutions Corp. es una empresa global líder en el desarrollo de software y servicios en la nube, con una base de clientes masiva y una vasta cantidad de datos sensibles, incluyendo información financiera, propiedad intelectual y datos personales de clientes. Su infraestructura de TI es compleja, abarcando centros de datos locales, entornos de nube híbrida (AWS y Azure), una red de oficinas distribuidas globalmente y una fuerza laboral remota significativa.

El Incidente Es el 10 de junio de 2025. Su equipo como expertos en ciberseguridadha detectado una serie de actividades anómalas:

Fase 1 (Vectores de Ataque Iniciales)

Fase 2 (Movimiento Lateral y Persistencia)

Fase 3 (Objetivo Final - Exfiltración/Destrucción)

3. FASES 1, 2 Y 3

- **Fase 1 (Vectores de Ataque Iniciales):**

  - Múltiples empleados han recibido correos electrónicos de *phishing* altamente sofisticados, suplantando a la dirección de TI, solicitando credenciales de acceso a un "nuevo portal de empleados".
  - Se ha identificado un intento de explotación de una vulnerabilidad de día cero en un servidor web público que ejecuta un software de gestión de proyectos obsoleto (versión no parcheada) dentro de la DMZ.
  - Un empleado de reciente contratación descargó accidentalmente un archivo adjunto malicioso desde una red social profesional (LinkedIn) que se hizo pasar por una oferta de capacitación.

3. FASES 1, 2 Y 3

- **Fase 2 (Movimiento Lateral y Persistencia):**

  - Parece que el atacante ha logrado comprometer una estación de trabajo de ingeniería de software a través del *phishing* exitoso, utilizando credenciales robadas.
  - Desde esta estación de trabajo, se han observado intentos de escaneo de red interno y de elevación de privilegios.
  - Hay indicios de que el atacante está intentando establecer persistencia mediante la creación de cuentas de usuario ocultas y la modificación de tareas programadas en algunos sistemas comprometidos.

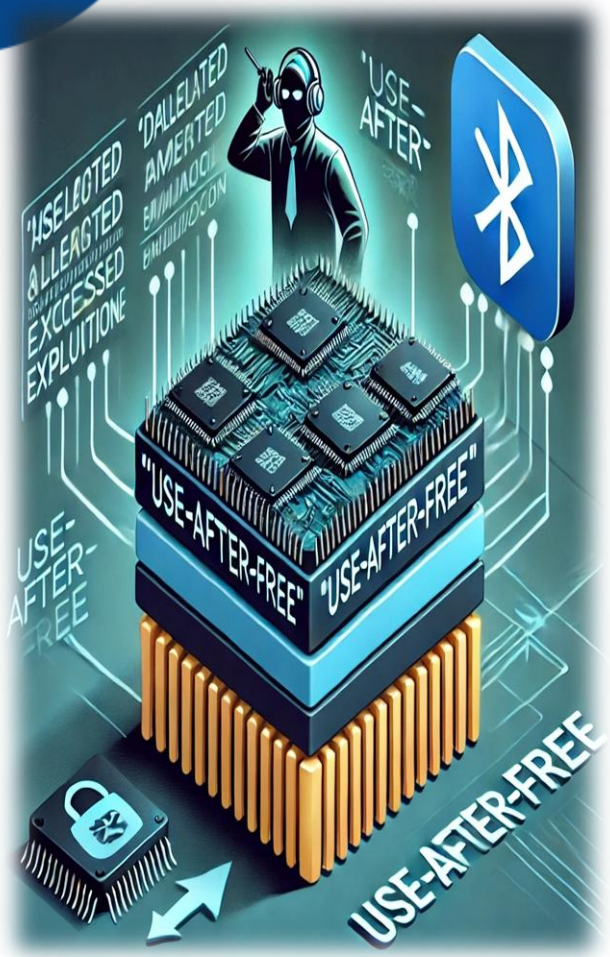
3. FASES 1, 2 Y 3

•**Fase 3 (Objetivo Final - Exfiltración/Destrucción):**

- La actividad principal del atacante parece dirigirse a la base de datos de propiedad intelectual (ubicada en la nube) y a los servidores de desarrollo que contienen el código fuente de los productos estrella de la empresa.
- Se han detectado grandes volúmenes de tráfico saliente inusual hacia direcciones IP externas no identificadas.
- En algunos sistemas críticos, se han encontrado archivos con extensiones cifradas y notas de rescate, lo que evidencia una actividad de *ransomware* como un segundo vector de ataque o distracción.

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.



1. Análisis de Amenazas y Vulnerabilidades

Las vulnerabilidades explotadas incluyen la **falta de concienciación del personal**, filtros de correo insuficientes (spam, DMARC), ausencia de mecanismos de doble factor (MFA) y contraseñas débiles. Según informes, alrededor del 74 % de los ataques comienzan por errores humanos, por ejemplo dar clic en enlaces maliciosos, por lo que la carencia de formación y controles antiphishing es crítica.

1.1 Amenazas identificadas:

- **Phishing dirigido:** correos simulando comunicaciones internas para capturar credenciales.
- **Vulnerabilidad de día cero:** software de gestión desactualizado expuesto en la DMZ (Zona Desmilitarizada).
- **Malware desde redes sociales:** vector alterno mediante ingeniería social.
- **Movimiento lateral y persistencia:** escaneo de red interna, creación de cuentas ocultas y tareas automatizadas.
- **Exfiltración y ransomware:** tráfico anómalo a IPs externas y cifrado de archivos con notas de rescate.

1.2 Vulnerabilidades técnicas:

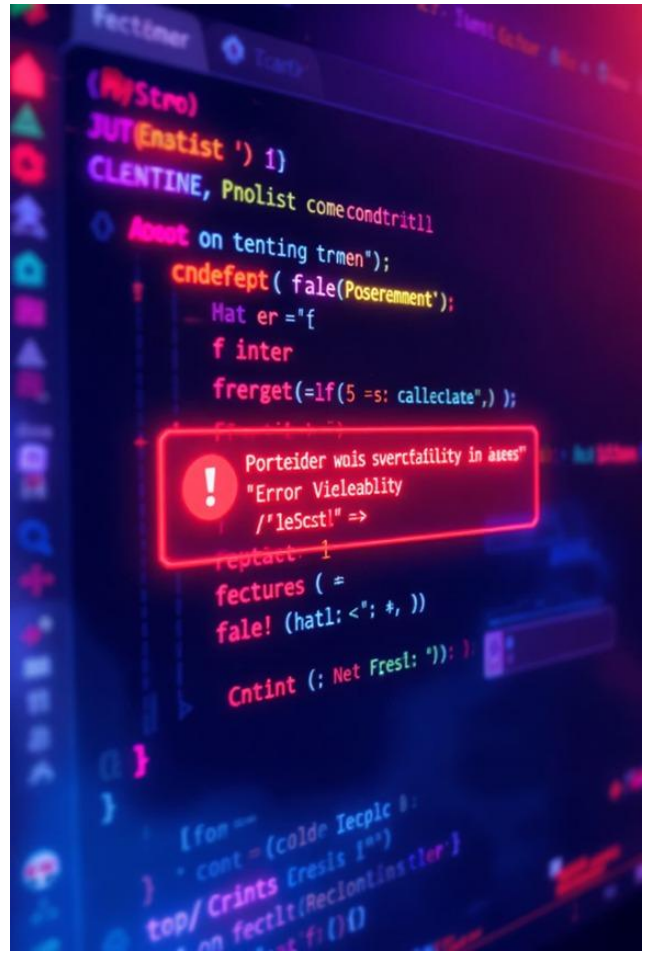
- **Ausencia de MFA (Autenticación Multifactor):** Permite que un atacante con solo las credenciales comprometidas tenga acceso total. Esto contradice lo recomendado por NIST (Instituto Nacional de Estándares y Tecnología) SP 800-63B.
- **Software no parcheado:** La falta de actualizaciones expone sistemas a vulnerabilidades conocidas, como se describe en NIST SP 800-40.
- **Falta de segmentación interna:** Permite el movimiento lateral libre dentro de la red tras una intrusión inicial, contrario al enfoque Zero Trust (Confianza Cero) descrito en NIST SP 800-207.
- **Control de acceso débil:** El uso de privilegios excesivos y cuentas mal gestionadas facilita la escalada de privilegios, contraviniendo ISO/IEC (Organización Internacional de Normalización / Comisión Electrotécnica Internacional) 27001 A.9.
- **Deficiencias en monitoreo y detección:** La ausencia de registros detallados y correlación de eventos limita la capacidad de detectar y contener ataques, como alerta NIST SP 800-92.

Normas de referencia: NIST SP 800-30, 40, 63B, 92, 207; ISO/IEC 27005, OWASP (Open Worldwide Application Security Project) Top 10.

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

2. Principios de Defensa en Profundidad

La **defensa en profundidad** busca capas superpuestas de controles de seguridad para que la falla de uno no comprometa todo el sistema. La implementación de múltiples productos y prácticas de seguridad puede ayudar a detectar y prevenir ataques a medida que van surgiendo, permitiendo mitigar eficazmente una amplia gama de amenazas.
En la práctica, TechSolutions debe aplicar controles físicos, técnicos y administrativos en cada nivel de su infraestructura (perímetro, red interna, endpoints, aplicaciones, datos, identidad, operaciones).



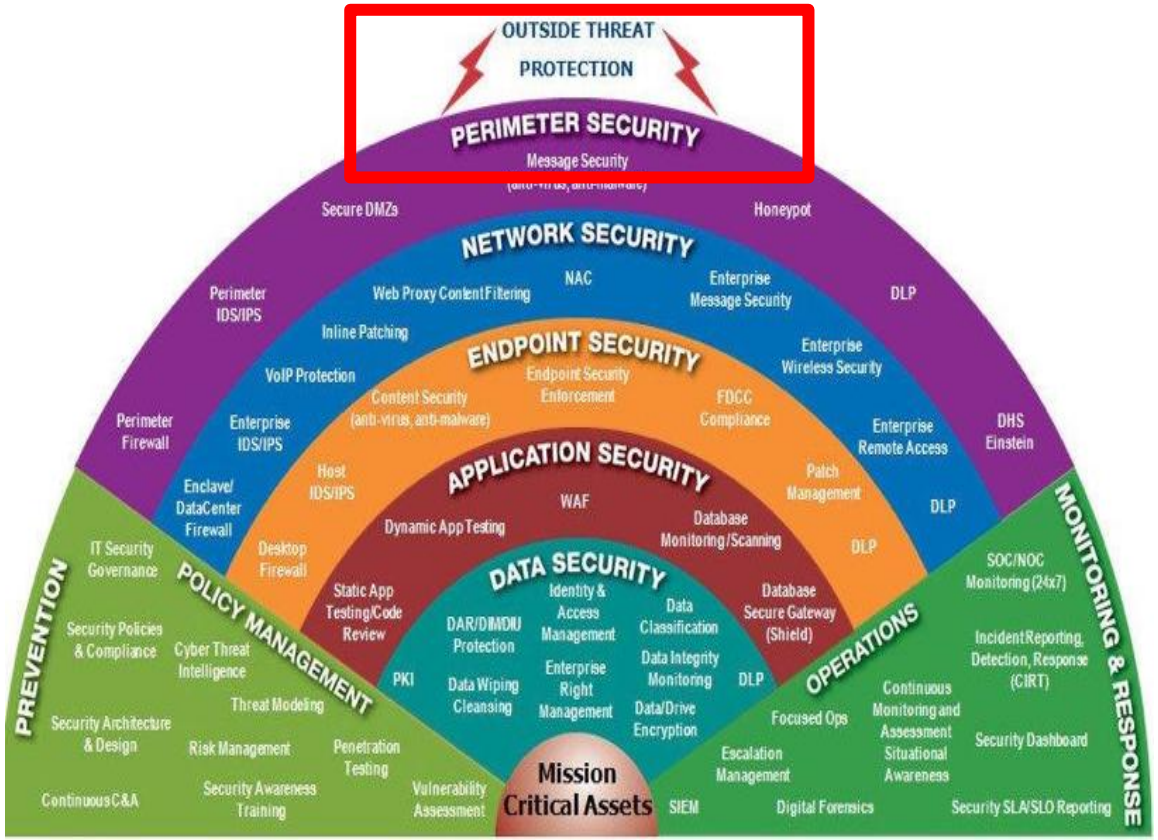
2.1 Controles redundantes: Múltiples medidas de seguridad en cada capa del entorno de TI (Tecnologías de la Información). Si una medida falla, otras mitigan el riesgo. Aplicable según NIST SP 800-53 CA-7 (monitoreo continuo) y SI-3 (protección contra código malicioso).
2.2 Segmentación y control de accesos: Separar lógicamente redes y servicios, limitar comunicaciones innecesarias entre dominios. NIST SP 800-207 (Zero Trust) y CIS (Center for Internet Security) Control 14 recomiendan microsegmentación para evitar desplazamientos laterales.
2.3 Mecanismos de detección y respuesta: Uso de SIEM (Gestión de Información y Eventos de Seguridad), EDR (Detección y Respuesta en el Endpoint) y NDR (Detección y Respuesta en la Red) para capturar y analizar eventos. NIST SP 800-137 y SP 800-61 Rev. 2 guían sobre monitoreo continuo y respuesta estructurada.
2.4 Principio de menor privilegio: Usuarios y procesos deben tener acceso mínimo necesario. NIST SP 800-53 AC-6 e ISO/IEC 27001 A.9.1.2 obligan a aplicar controles de privilegios rigurosos.
2.5 Recuperación y continuidad operativa: Capacidad de volver a operar después de un incidente. Requiere backups (copias de seguridad) verificados, redundancia de infraestructura y planes DRP (Planes de Recuperación ante Desastres) según NIST SP 800-34 Rev.1 e ISO 27031.
2.6 Cultura y procesos: Además de soluciones técnicas, la concienciación del personal y procedimientos claros (políticas de seguridad, planes de respuesta) son capas defensivas críticas. La formación continua y auditorías internas aseguran que las medidas técnicas funcionen correctamente y que el equipo sepa cómo reaccionar ante incidentes.

Normas de referencia: NIST SP 800-53 Rev. 5, 207, 137, 34; CIS Controls v8; ISO/IEC 27001, 27031.

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

Fuente: https://www.conytec.com/mis-plataformas-y-sistemas-son-realmente-seguros-frente-a-cualquier-tipo-de-ataque/

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.



3. Capas de Defensa Propuestas

3.1 Capa 1: Perímetro/Red Externa

Medidas Técnicas

- **NGFW (Firewall de Nueva Generación):** Filtrado de tráfico con inspección profunda de paquetes (NIST SP 800-41).
- **IDS/IPS (Sistemas de Detección/Prevención de Intrusos):** Detecta intentos de intrusión y bloquea tráfico sospechoso.
- **WAF (Firewall de Aplicaciones Web):** Filtrado HTTP para proteger APIs (Interfaces de Programación de Aplicaciones) y aplicaciones web ante OWASP Top 10.
- **DMZ (Zona Desmilitarizada):** Contención de servicios expuestos al público, evitando que una intrusión llegue a la red interna (ISO/IEC 27033).
- **Filtrado DNS (Sistema de Nombres de Dominio) y reputación IP:** Prevención de comunicaciones maliciosas (CIS Control 9).

Medidas Administrativas

Políticas de seguridad perimetral (segregación de DMZ, revisión de reglas de firewall periódicamente); monitoreo continuo de logs de perímetro; revisiones regulares de configuraciones de red pública; acuerdos de nivel de servicio (SLAs) con proveedores de Internet para contingencias; procedimientos de respuesta rápida ante intrusiones detectadas.

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

3.2 Capa 2: Red Interna/Segmentación

Medidas Técnicas

- **VLANs (Redes de Área Local Virtuales):** Segmentación lógica de tráfico según funciones (NIST SP 800-207).
- **SDN (Red Definida por Software):** Control programable de tráfico interno.
- **ACLs (Listas de Control de Acceso):** Reglas para limitar tráfico entre segmentos.
- **NAC (Control de Acceso a la Red):** Autenticación previa al acceso.

Medidas Administrativas

Políticas de segmentación de red documentadas; clasificación de activos y asignación de niveles de confianza; análisis de flujo de red para identificar comunicaciones inusuales; pentesting interno y auditorías de configuración de switches y routers; actualización periódica de reglas de VPN y filtrado inter-sucursal. Se reduce así la capacidad de los atacantes de propagarse y filtrar datos, ya que “la segmentación de red ayuda a limitar la exposición interna […] y a contener la propagación del malware”

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

3.3 Capa 3: Endpoint/Dispositivos

Medidas Técnicas

- **EDR (Detección y Respuesta en el Endpoint):** Amenazas en tiempo real con contención automatizada (NIST SP 800-128).
- **MDM (Gestión de Dispositivos Móviles):** Control sobre configuración de equipos móviles.
- **Hardening (Endurecimiento de sistemas):** Reducción de superficie de ataque según CIS Benchmarks.

Medidas Administrativas

Políticas de uso de dispositivos (solo software autorizado, sin permisos administrativos innecesarios); gestión de inventario de hardware/software; formación a usuarios sobre buenas prácticas de seguridad (p. ej. no descargar software de fuentes no confiables); escaneo regular de vulnerabilidades en estaciones de trabajo; uso de cuentas no-administrador para tareas diarias.

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

3.4 Capa 4: Aplicaciones

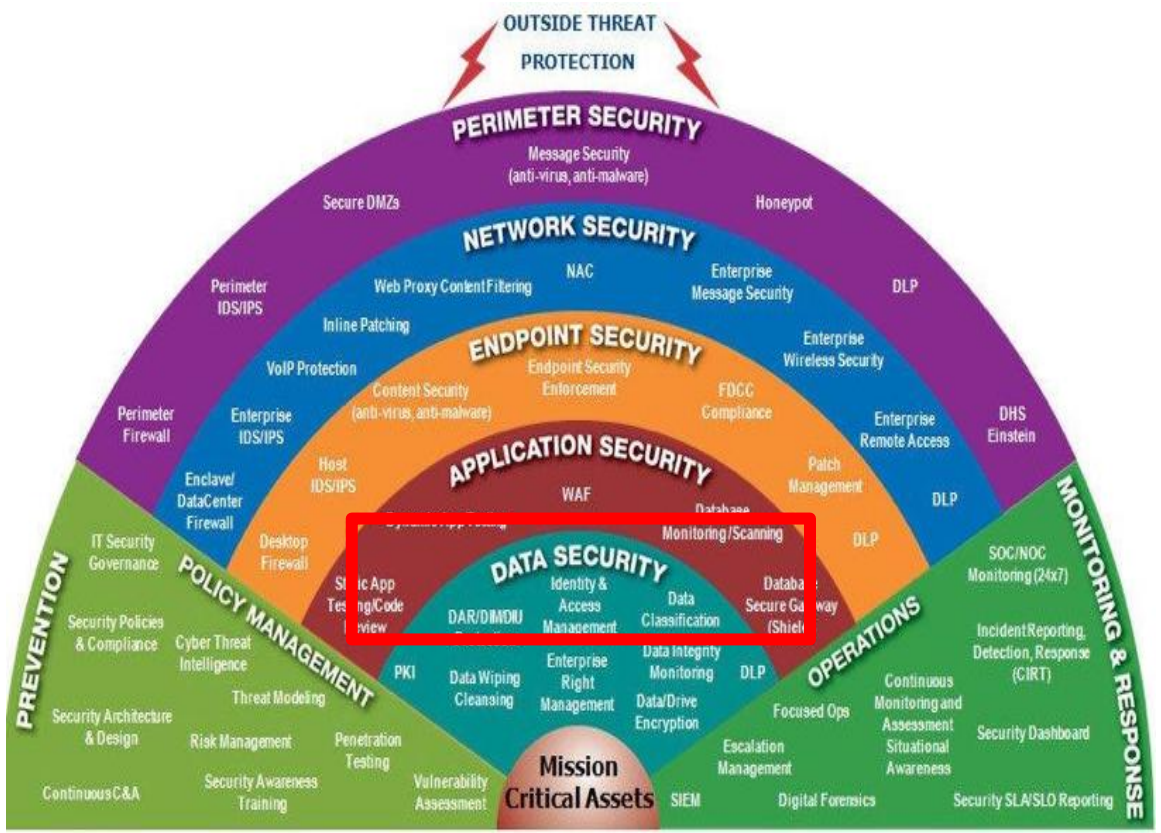
Medidas Técnicas

- **SAST/DAST (Análisis Estático/Dinámico de Seguridad):** Identificación de vulnerabilidades (NIST SP 800-218 SSDF - Marco de Desarrollo Seguro).
- **DevSecOps (Desarrollo Seguro en DevOps):** Seguridad desde la fase de diseño (ISO/IEC 27034).
- **OAuth/SAML (Protocolos de Autenticación):** Federación segura de identidad.
- **Pentesting (Pruebas de Penetración):** Validación de controles (OWASP ASVS - Estándar de Validación de Seguridad de Aplicaciones).

Medidas Administrativas

Ciclo de desarrollo seguro (Secure SDLC) con revisión de código y pruebas de seguridad; proceso de gestión de parches de aplicaciones; lista blanca de aplicaciones permitidas (whitelisting); revisiones de configuración de servidores de aplicaciones; políticas de gestión de cambios y control de versiones. Estas medidas previenen la explotación de fallos en el software de la empresa.

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.



3.5 Capa 5: Datos

Medidas Técnicas

- **AES (Estándar de Cifrado Avanzado):** Cifrado con AES-256 y TLS (Seguridad de la Capa de Transporte) 1.3 (ISO/IEC 27040).
- **DLP (Prevención de Pérdida de Datos):** Protección frente a fuga de información (NIST SP 800-111).

Medidas Administrativas

Políticas de respaldo y recuperación (evaluadas y probadas regularmente); clasificación formal de la información y manejo de datos sensibles; retención mínima de datos críticos; rotación de llaves de cifrado; registro de accesos a información crítica. Mantener redundancia de datos (almacenamiento multiregión, réplicas) incrementa la resiliencia frente a ransomware.

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

3.6 Capa 6: Identidad y Acceso

Medidas Técnicas

- **MFA (Autenticación Multifactor):** Segundo factor obligatorio (NIST SP 800-63B).
- **IAM (Gestión de Identidades y Accesos):** Centralización del control de identidades.
- **SSO (Inicio de Sesión Único):** Simplificación y control de autenticación.

Medidas Administrativas

Revisión periódica de permisos (asegurando que nadie tenga accesos excesivos); políticas claras de creación y eliminación de cuentas (on/off boarding); concienciación sobre higiene de contraseñas (no compartir credenciales, uso de MFA); gestión de cuentas de servicio y de administrador separadas; capacitación en reconocimiento de ataques de ingeniería social dirigidos a robar credenciales. Según la práctica Zero Trust, “no se debe confiar por defecto en ningún usuario”

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

3.7 Capa 7: Operaciones y Concienciación

Medidas Técnicas

- **SOC (Centro de Operaciones de Seguridad):** Monitoreo y respuesta en tiempo real (NIST SP 800-137).
- **SIEM (Gestión de Eventos e Información de Seguridad):** Correlación y análisis de eventos.
- **CTI (Inteligencia de Amenazas Cibernéticas):** Anticipación de amenazas (STIX/TAXII - Estandarización de Intercambio de Información).

Medidas Administrativas

Programa de entrenamiento y ejercicios de concienciación (phishing simulation, capacitación periódica); auditorías y pruebas de penetración regulares (red teams, CTF internos); plan de respuesta a incidentes y continuidad de negocio (realizar simulacros con todo el equipo); revisión constante de políticas de seguridad y cumplimiento de estándares (ISO 27001, NIST CSF); evaluación de nuevos riesgos y tecnologías emergentes mediante informes de inteligencia de amenazas y participación en comunidades de seguridad. Según diversos expertos, la mejora continua de la estrategia de defensa (incorporando lecciones de incidentes previos) es esencial

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

4. Respuesta al Incidente (10 de junio de 2025)

4.1 Contención:

- **Aislamiento de máquinas afectadas:** Se realiza mediante políticas de red en switches y firewalls para cortar la conectividad de dispositivos sospechosos, utilizando capacidades NAC (Control de Acceso a la Red) y EDR (Detección y Respuesta en el Endpoint).
- **Desactivación de cuentas sospechosas:** IAM (Gestión de Identidades y Accesos) se usa para suspender temporalmente usuarios comprometidos, aplicando procedimientos definidos en NIST SP 800-53 IA-5 y AC-2.
- **Bloqueo de conexiones externas:** Reglas de firewall y listas negras en sistemas perimetrales (NGFW y DNS Filtering) se ajustan para cortar comunicaciones maliciosas. Conforme con NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide).

4.2 Erradicación:

- **Eliminación de malware:** EDR y antivirus con capacidades heurísticas ejecutan análisis profundos y scripts de remediación. ISO/IEC 27035 establece estos pasos como parte del tratamiento de incidentes.
- **Parches de seguridad:** Se aplica una actualización inmediata del sistema comprometido mediante un proceso de gestión de parches documentado (NIST SP 800-40 Rev. 3).
- **Revocación y recreación de credenciales:** Uso de herramientas IAM para forzar el cambio de contraseñas e invalidar tokens activos, alineado con NIST SP 800-63B.

4.3 Recuperación:

- **Restauración desde backups validados:** Copias de seguridad almacenadas fuera de línea (air-gapped) se restauran según políticas BCP/DRP (NIST SP 800-34 Rev.1, ISO/IEC 27031).
- **Verificación de integridad:** Se aplican hashes criptográficos (SHA-256) para validar la autenticidad de los sistemas restaurados.
- **Reintegración por etapas:** Se aplica el enfoque de zonas seguras (clean zone) para reincorporar progresivamente los sistemas, priorizando servicios críticos con base en análisis de impacto al negocio (ISO/IEC 27005).

Normas: NIST SP 800-61 Rev. 2, NIST SP 800-40, NIST SP 800-63B, ISO/IEC 27035, 27031.

Defensa en Profundidad: Fortaleza Digital de TechSolutions Corp.

5. Monitoreo y Mejora Continua

- **Ciclo PDCA (Planificar-Hacer-Verificar-Actuar):** Aplicado mediante un programa de gestión de seguridad documentado. Se definen objetivos de control, se implementan, se auditan (internamente con ISO/IEC 27001 A.18.2.2) y se corrigen desviaciones.
- **Auditorías periódicas:** Se efectúan evaluaciones técnicas y de cumplimiento trimestrales, conforme con NIST CSF (Marco de Ciberseguridad) función "Detect" y control ISO/IEC 27001 A.18.2.3.
- **Ejercicios Red/Blue Team:** Simulaciones ofensivas/defensivas con reportes post mortem documentados. Alineado con NIST SP 800-115 (Technical Guide to Information Security Testing).
- **Métricas de desempeño:** Uso de KPIs (Indicadores Clave de Desempeño) y KRIs (Indicadores Clave de Riesgo) para evaluar efectividad. Ej: tiempo medio de detección (MTTD), tiempo medio de respuesta (MTTR), conforme a ISO/IEC 27004.
- **Integración de CTI e IoCs:** Consumo de feeds STIX/TAXII para enriquecer la detección con amenazas externas. Procesos respaldados por NIST SP 800-150 (Guide to Cyber Threat Information Sharing).
- **Entrenamiento continuo:** Programas de formación periódica y simulacros de phishing refuerzan la concienciación del personal. La cultura de seguridad se fortalece con campañas internas (boletines, talleres) y recordatorios de protocolos. El factor humano es crítico en casi tres cuartas partes de los ataques, por lo que el entrenamiento debe ser recurrente y actualizado con ejemplos reales.
- **Threat Intelligence:** Integrar fuentes de inteligencia sobre amenazas (por ejemplo CISA, CERTs, plataformas de inteligencia de código abierto) en el SOC/SIEM para ajustar defensas según actores conocidos. Analizar patrones de ataques recientes (e.g. campañas de ransomware) ayuda a actualizar firmas y políticas (IPS, EDR, filtros de correo)

Normas: NIST CSF, ISO/IEC 27004, ISO/IEC 27001 A.18, NIST SP 800-115, NIST SP 800-150.

7. CONCLUSIONES

Este plan técnico integral fortalece la postura de ciberresiliencia de TechSolutions Corp. mediante la implementación estructurada de controles de defensa en profundidad con base en estándares internacionales y mejores prácticas de la industria.

8. BIBLIOGRAFÍA

- NIST SP 800 Series (30, 40, 53, 61, 63, 92, 111, 115, 137, 150, 207, 218, 34).
- ISO/IEC 27000 Series (27001, 27002, 27004, 27005, 27031, 27035, 27040).
- CIS Controls v8.
- OWASP Top 10, ASVS, SSDF.
- MITRE ATT&CK Framework.

Preguntas

@EsdegCol

Escuela Superior de Guerra

Escuela Superior de Guerra

Escuela Superior de Guerra

www.esdegue.edu.co

La ***Escuela Superior de Guerra "General Rafael Reyes Prieto"*** está certificada bajo las normas internacionales **ISO 9001:2015** e **ISO 21001:2018.**

Gracias

@EsdegCol

Escuela Superior de Guerra

Escuela Superior de Guerra

Escuela Superior de Guerra

www.esdegue.edu.co