

PLAN DE RESPUESTA A INCIDENTE DE RANSOMWARE

Arturo Roa

Basado en el Marco de Ciberseguridad NIST

Caso de Estudio: TechCo

1. INTRODUCCIÓN

En el contexto actual de transformación digital, las organizaciones que gestionan información sensible enfrentan una creciente amenaza por parte del ransomware, uno de los tipos de malware más destructivos y lucrativos para los ciberdelincuentes. TechCo, una empresa ficticia dedicada a la provisión de servicios en la nube y al almacenamiento de información crítica de clientes, ha sido víctima de un ataque de ransomware que comprometió seriamente su continuidad operativa, la confidencialidad de los datos y la confianza de sus clientes.

El presente documento tiene como objetivo desarrollar un **Plan de Respuesta a Incidentes de Ransomware** alineado con el **Marco de Ciberseguridad del NIST (National Institute of Standards and Technology)**, estructurado en sus cinco funciones fundamentales: Identificar, Proteger, Detectar, Responder y Recuperar. Este plan permitirá a TechCo fortalecer su postura de seguridad, minimizar el impacto de futuros incidentes y establecer procedimientos formales de actuación ante eventos similares.

2. FUNCIÓN NIST: IDENTIFICACIÓN (IDENTIFY)

2.1 Contexto organizacional

TechCo opera infraestructura crítica que soporta:

- Servicios de almacenamiento en la nube.
- Gestión de bases de datos de clientes.
- Procesamiento de información financiera.
- Plataformas de respaldo y recuperación.
- Sistemas de autenticación y gestión de identidades.

La naturaleza del negocio convierte a TechCo en un objetivo atractivo para ataques de ransomware, ya que la indisponibilidad de los servicios impacta directamente en la operación de sus clientes y genera alta presión para el pago de rescates.

2.2 Activos críticos identificados

Los principales activos comprometidos o en riesgo son:

a) Servidor de archivos corporativo

Contiene documentación operativa, contratos, información legal y datos técnicos necesarios para la operación diaria.

b) Base de datos de clientes

Incluye:

- Información personal (PII).
- Datos financieros.
- Credenciales cifradas.
- Historial de transacciones.

Este activo es crítico desde el punto de vista legal, reputacional y regulatorio.

c) Infraestructura de backups

- Copias de seguridad en línea.
- Repositorios de recuperación.
- Sistemas de replicación.

Su compromiso eliminó la capacidad de recuperación rápida.

d) Red interna

- Servidores de producción.
- Equipos de usuario.
- Controladores de dominio.
- Sistemas de virtualización.

e) Cuentas y credenciales

Especialmente:

- Usuario inicial comprometido por phishing.
- Cuentas con privilegios elevados.
- Accesos administrativos.

2.3 Amenazas identificadas

- Campañas de phishing dirigidas.
- Malware con capacidad de movimiento lateral.
- Ransomware con cifrado fuerte (AES + RSA).
- Exfiltración de datos previa al cifrado (doble extorsión).
- Ataques a infraestructura de respaldo.

2.4 Vulnerabilidades que facilitaron el ataque

a) Técnicas

- Falta de segmentación de red.
- Ausencia de EDR.
- Backups accesibles desde el dominio.
- Falta de MFA.
- Sistemas sin parches actualizados.

b) Organizativas

- Falta de plan de respuesta formal.
- No existía un CSIRT definido.
- Escasa formación en ingeniería social.
- Inexistencia de simulacros.

c) Procedimentales

- Privilegios excesivos en estaciones de trabajo.
- Falta de monitoreo centralizado.
- No se realizaban pruebas de restauración de backups.

3. FUNCIÓN NIST: PROTECCIÓN (PROTECT)

3.1 Objetivo

Implementar salvaguardas para garantizar la entrega de servicios críticos y reducir la probabilidad de éxito de un ataque de ransomware.

3.2 Controles técnicos

a) Seguridad del correo electrónico

- Filtros antiphishing con análisis de adjuntos en sandbox.
- Bloqueo de macros por defecto.

b) Protección de endpoints

- EDR con detección de comportamiento.
- Bloqueo de ejecución desde carpetas temporales.
- Listas blancas de aplicaciones.

c) Segmentación de red

- Separación de:
 - Usuarios
 - Servidores

- Backups
- Administración
- Firewalls internos y microsegmentación.

d) Gestión de identidades

- MFA obligatorio.
- Principio de mínimo privilegio.
- Revisiones periódicas de accesos.

e) Backups resilientes

- Regla 3-2-1:
 - 3 copias
 - 2 medios distintos
 - 1 offline/inmutable
- Pruebas de restauración mensuales.

3.3 Controles administrativos

- Política formal anti-ransomware.
- Programa de concienciación.
- Simulaciones de phishing.
- Manual de respuesta a incidentes.
- Evaluaciones de riesgo periódicas.

4. FUNCIÓN NIST: DETECCIÓN (DETECT)

4.1 Monitoreo

- SIEM centralizado.
- Correlación de eventos:
 - Cifrado masivo.

- Movimiento lateral.
- Elevación de privilegios.
- Alertas por:
 - Creación masiva de archivos .locked, .enc, etc.
 - Borrado de shadow copies.

4.2 Protocolo de alerta temprana

1. Detección por EDR/SIEM.
 2. Clasificación del incidente.
 3. Notificación automática al CSIRT.
 4. Aislamiento de equipos.
 5. Activación del plan IR.
-

5. FUNCIÓN NIST: RESPUESTA (RESPOND)

5.1 Estructura del Equipo de Respuesta (CSIRT)

Rol	Responsabilidad
CISO	Dirección estratégica
Líder IR	Coordinación operativa
Forense	Análisis técnico
Redes	Contención
Legal	Cumplimiento y denuncias
Comunicaciones	Gestión de crisis
Dirección	Decisiones ejecutivas

5.2 Procedimiento paso a paso

1. Confirmación del ataque.
2. Aislamiento de red.

3. Desconexión de backups.
 4. Bloqueo de credenciales.
 5. Identificación del ransomware.
 6. Análisis de alcance.
 7. Evaluación legal (*Evaluación de la viabilidad de descifrado vs. reconstrucción antes del vencimiento del plazo de extorsión (72h), manteniendo la política de no pago recomendada*)
 8. Comunicación interna.
 9. Comunicación a clientes.
 10. Coordinación con autoridades.
 11. Erradicación del malware.
 12. Preparación de entorno limpio.
-

6. FUNCIÓN NIST: RECUPERACIÓN (RECOVER)

6.1 Restauración técnica

- Reinstalación de sistemas.
- Validación de integridad.
- Restauración desde backups inmutables.
- Cambios de contraseñas globales.
- Reemisión de certificados.

6.2 Continuidad del negocio

- Activación de DRP.
- Uso de infraestructura alterna.
- Prioridad de servicios:
 1. Autenticación
 2. Base de datos clientes

- 3. Aplicaciones core
- 4. Servicios secundarios

6.3 Reincorporación progresiva

- Pruebas de seguridad.
 - Auditoría post-restauración.
 - Monitoreo reforzado 30 días.
-

7. MEJORA CONTINUA

7.1 Lecciones aprendidas

- Análisis de causa raíz (RCA).
- Evaluación de controles fallidos.
- Revisión de tiempos de detección y respuesta.

7.2 Actualización del plan

- Simulacros semestrales.
- Red Team / Blue Team.
- Actualización de políticas.
- Formación continua.

7.3 Métricas

- MTTR (Mean Time To Recover)
 - MTTD (Mean Time To Detect)
 - Porcentaje de restauración exitosa
 - Nivel de cumplimiento NIST
-

8. CONCLUSIÓN

La implementación de este Plan de Respuesta a Incidentes basado en NIST permitirá a TechCo:

- Reducir la superficie de ataque.
- Detectar amenazas tempranamente.
- Responder de forma organizada y legalmente correcta.
- Recuperar operaciones sin depender del pago de rescates.
- Fortalecer su madurez en ciberseguridad.