Plan de Respuesta a Incidentes de Ransomware basado en NIST

Arturo Martín-Vegue González

Noviembre 2025

En este documento se desarrollará un **plan de respuesta** a incidentes en una organización (TechCo) basado en el marco de trabajo *NIST* para que se pueda recuperar y reaccionar en un futuro a posibles amenazas o ataques como el ya sufrido.

Descripción del incidente:

Origen del ataque: Un empleado de TechCo recibió un correo electrónico de phishing que parecía legítimo, con un archivo adjunto malicioso disfrazado de factura. El empleado descargó el archivo, permitiendo a los atacantes instalar el ransomware en la red interna de TechCo.

- **Propagación:** El ransomware se extendió rápidamente a varios servidores críticos. Los sistemas afectados incluyen:
  - El **servidor de archivos**, donde se almacenan documentos y datos esenciales para el funcionamiento diario.
  - La **base de datos de clientes**, que contiene información personal y financiera sensible.
  - Los **sistemas de backup** internos que, desafortunadamente, también se encontraban dentro de la misma red comprometida.
- **Impacto del ataque:** Los archivos fueron cifrados, y la empresa recibió un mensaje exigiendo el pago de 50 Bitcoins (equivalente a más de $1,000,000) para obtener la clave de descifrado. Los atacantes amenazaron con eliminar permanentemente todos los archivos si el rescate no se paga en un plazo de 72 horas.
- **Problemas adicionales:
  1. La red no contaba con una segmentación adecuada, lo que permitió que el ransomware afectara tanto los sistemas de producción como los backups.
  2. No había un protocolo de alerta temprana ni sistemas de monitoreo en tiempo real, por lo que la propagación del ransomware no fue

detectada hasta que los empleados comenzaron a notar la falta de acceso a los archivos.
3. Los esfuerzos por restaurar los sistemas desde los backups fallaron, ya que estos también estaban cifrados por el ransomware.

Nos centraremos en el núcleo en el que se sustenta el *NIST* que se divide en:

- **Identificar:** Entender los activos de riesgo y vulnerabilidades.
- **Protección:** Desarrollar y aplicar medidas preventivas y evaluar las políticas y controles de seguridad.
- **Detección:** Proporcionar métodos y herramientas para detectar el ataque y desarrollar un protocolo de alerta temprana para mejorar la detección de incidentes.
- **Respuesta:** Desarrollar y plan detallado para responder a futuros ataques, definiendo los pasos a seguir y los roles y responsabilidades en el equipo, así como, establecer canales de comunicación efectivos.
- **Recuperación:** Establecer un plan para la restauración de los sistemas y datos afectados por el ataque. Además de, desarrollar un plan de continuidad durante y después de la recuperación.
- **Mejora Continua:** Propuesta de un método para evaluar la eficacia del plan de respuesta del incidente para la integración adecuada y mejoras futuras.

Teniendo presente el ataque ya sufrido, se repasará punto por punto las acciones que se podían haber tomado teniendo en cuenta las infraestructura y las mejoras que se pueden integrar en la organización.

---

1. Identificación

Activos críticos identificados:

- Servidor de archivos.
- Base de datos de los clientes.
- Servidores y sistemas de copias de seguridad (backups).

Vulnerabilidades encontradas:

- Topología de red poco segura al no contar con la segmentación y aislamiento de sistemas críticos.

- Ausencia de monitoreo y alerta temprana.
- Falta de concienciación del personal (Phising).

La falta de concienciación de los empleados facilitó la entrada al ataque del ransomware siendo así el vector de ataque.

Los sistemas no estaban correctamente aislados en la red ni contaban con sistemas de monitoreo para alertar de posibles ataques o amenazas.

2. Protección

Las medidas preventivas que se debieron tomar por la organización considerando los activos y las vulnerabilidades detectadas son las siguientes:

- Implementación de subredes internas mediante **VLANs (Redes de Área Local Virtuales)** permitiendo la segmentación.
- Es fundamental crear una **subred completamente aislada** para los sistemas *backup* para evitar que el ransomware el ataque los hubiese afectado.
- Creación de una red **DMZ (Zona Desmilitarizada)**, clave para los servicios accesibles desde internet, protegiendo así la red interna de posibles ataques externos.

Evaluando las políticas y el ataque, se puede deducir que el ransomware se movió de forma lateral por el sistema. Para evitar posibles ataques se recomienda:

- Crear la política de **menor privilegio**. Enfoque de seguridad conocido como **Zero Trust (Confianza Cero)**, se asume que no se debe confiar en nadie por defecto, independientemente de su ubicación en la red.

3. Detección

Para la fase de detección se recomienda la implementación de los siguientes sistemas:

- **Agentes (EDR):** Un agente EDR (Endpoint Detection and Response) debería detectar y bloquear la **ejecución de binarios desconocidos** o **procesos anónimos**.
- **Monitoreo de Logs:** Implementar un SIEM (Security Information and Event Management) permite correlacionar eventos. Debe haber alertas configuradas para:
  - **Fallos de autenticación repetidos** o acceso inusuales (indicando un intento de credenciales robadas para moverse lateralmente).
  - **Conexiones salientes inusuales** a servidores de comando o control.

  - **Acceso desde una cuenta de servicio a la red de backups** para evitar la violación de la regla **"menor privilegio"**.

- **Monitoreo de Integridad de Archivos (FIM) y Comportamiento**:
  - El proceso de cifrado consume muchos recursos de disco y CPU. Un EDR o SIEM debe alertar si es un proceso inesperado comienza a tener un uso de disco anormalmente alto en el servidor de archivos.
  - **Monitoreo de Integridad (FIM):** El FIM verifica continuamente las firmas digitales (hashes) de los archivos críticos. Si detecta que una gran cantidad de archivos están siendo modificados o renombrados con extensiones nuevas y desconocidas (el proceso de cifrado), y sus hashes cambian drásticamente en un corto periodo de tiempo, genera una alerta de máxima prioridad que indica **cifrado activo**.

4. Respuesta

En este punto se definirán los pasos y roles y la comunicación que se recomienda a la organización para una correcta respuesta a incidentes.

4.1. Respuesta a Incidentes

1. **Aislamiento Lógico y Físico (Desconexión):** Retirar inmediatamente los sistemas afectados de la red.
2. **Identificación y Confirmación:** Confirmar qué sistemas están infectados y cuál es el vector de ataque inicial.
3. **Preservación de la Evidencia:** Realizar un **análisis forense digital y preservación de evidencia**. Esto asegura:
   - **Identificar el Vector de Ataque:** La preservación de la evidencia permite saber cómo actúa el atacante y la forma de entrada en la red.
   - **Alcance:** Determinar el alcance total del daño y si los atacantes exfiltraron datos.
4. **Erradicación (Limpieza y Refuerzo):** La **erradicación inmediata**, en este contexto, se debe enfocar en:
   - **Eliminación de la Causa Principal (ransomware):** Eliminar el ransomware, los archivos maliciosos y cualquier puerta trasera instalada.
   - **Refuerzo inmediato:** Aplicar todos los parches de seguridad, restablecer todas las contraseñas (especialmente de las cuentas comprometidas) y aplicar las medidas de **Protección** que se definieron en el **Plan de Respuesta** antes de volver a conectar los sistemas.

4.2. Roles y Comunicación

La definición de roles dentro de la organización y un **Equipo de Respuesta a Incidentes (IRT)** se recomienda para el correcto manejo de una incidencia como el ataque de ransomware y futuras amenazas, junto con una comunicación precisa y eficaz en la organización.

Roles

Los tres roles esenciales para el **IRT** son:

Rol Clave	Responsabilidad Principal
Líder del Incidente	Dirige la respuesta, toma decisiones críticas (ej. si pagar o no el rescate), coordina la comunicación interna y es el punto de contacto con la gerencia.
Analista Forense / Técnico	Se encarga de la contención, la preservación de evidencia, el análisis de la causa raíz, la erradicación y la reconstrucción técnica de los sistemas.
Coordinador de Comunicación / Legal	Gestiona las comunicaciones externas (clientes, medios, reguladores) e internas. Asegura el cumplimiento de las obligaciones legales de notificación (dada la fuga de datos de clientes).

Comunicación

Comunicación Interna El **Líder del Incidente** debe traducir el impacto técnico en términos de negocio para la Gerencia. Los dos puntos cruciales son:

El Impacto Operacional y Financiero (El Costo del Incidente):

- **Qué comunicar:** El coste cuantificable de la interrupción. Se debe informar qué servicios críticos para el negocio están caídos y el impacto estimado.
- **Perdida de Datos:** La recuperación se realizará a un **Punto de Recuperación Previo al Compromiso (Pre-Compromise State)**.
- **Por qué:** El retroceso garantiza la **erradicación completa** de cualquier *malware* latente o puerta trasera, que podría haber estado activo durante el tiempo de permanencia del atacante.
- **El Beneficio Mayor:** Justificar la pérdida de datos como un **costo necesario** para garantizar una **recuperación limpia** y evitar una catástrofe

futura donde las pérdidas serían incrementadas o mucho peores, como la inutilización permanente de equipos o multas masivas por incumplimiento legal.

El Estado de Contención y Proyección de Tiempo (ETA de Recuperación):

- **Qué comunicar:** La Gerencia necesita saber si el incidente está bajo control y cuándo se espera que termine.

Comunicación Externa El objetivo es cumplir con las obligaciones legales de notificación y gestionar la confianza de los clientes.

Los **tres mensajes clave** que deben incluirse en la comunicación pública son:

1. **Reconocimiento y Transparencia (Qué Sucedió):**
   - **Mensaje:** Confirmar abiertamente que ha ocurrido un incidente de seguridad y especificar **qué tipo de información** fue comprometida (ej. "nombres, direcciones de correo electrónico y números de teléfono"). Es fundamental **no mentir** ni minimizar la escala.
   - **Por qué:** Cumple con el requisito de transparencia y establece una base de confianza, a pesar de la mala noticia.
2. **Acción Correctiva y Contención (Qué Estamos Haciendo):**
   - **Mensaje:** Detallar las medidas que la empresa ha tomado de inmediato (ej. "La amenaza ha sido contenida, hemos reforzado la seguridad y estamos trabajando con expertos forenses externos").
   - **Por qué:** Muestra que la situación está bajo control y que la empresa está actuando de manera responsable.
3. **Orientación y Asistencia al Cliente (Qué Debe Hacer el Cliente):**
   - **Mensaje:** Proporcionar pasos concretos que los clientes deben seguir para protegerse (ej. "Recomendamos cambiar inmediatamente su contraseña y estar atentos a comunicaciones sospechosas"). La empresa debe ofrecer servicios de protección, como **monitoreo de crédito gratuito** (si aplica).
   - **Por qué:** Pone al cliente en primer lugar, le da herramientas para defenderse y mitiga el riesgo de fraude posterior (lo cual reduciría la responsabilidad de la empresa).

5. Recuperación

- En la fase de recuperación es esencial, antes de poner en marcha el sistema, restaurar el backup anterior al **ataque** en un **entorno de prueba o sandbox aislado** y realizar una exploración antivirus completa que garantice que la copia de seguridad está libre de cualquier código malicioso antes de conectarla a la red de la empresa.
- Para complementar la fase de recuperación, se recomienda tener un *backup* aislado o también denominado "*Backup Offline*" que no esté conectado a la red de forma permanente, sino en momentos puntuales para realizar la subida de datos.

Con esto la empresa, TechCo, se asegura un procedimiento seguro y medidas preventivas para el futuro.

6. Mejora Continua

Para asegurar a la empresa una mejora continua y evitar futuras amenazas, se recomienda lo siguiente:

- Evaluar un **Informe Post-Incidente** haciendo especial énfasis en el **tiempo de detección**, el **tiempo de contención** y el **coste total del impacto**.

Para, a continuación, a partir del **Informe Post-Incidente**, generar dos entregables que reúnan lo siguiente:

- **Plan de Acción Correctiva (PAC):** Documento donde cada lección aprendida se convierte en una **tarea específica**, asignada a un **responsable** con una **fecha límite**.
- **Actualización del Plan de Respuesta (IRP):** El documento original del **Plan de Respuesta** a incidentes (el actual) debe ser **revisado**, **modificado** para incluir nuevos procedimientos y finalmente **aprobado** por la Gerencia, convirtiéndolo en política para la empresa.