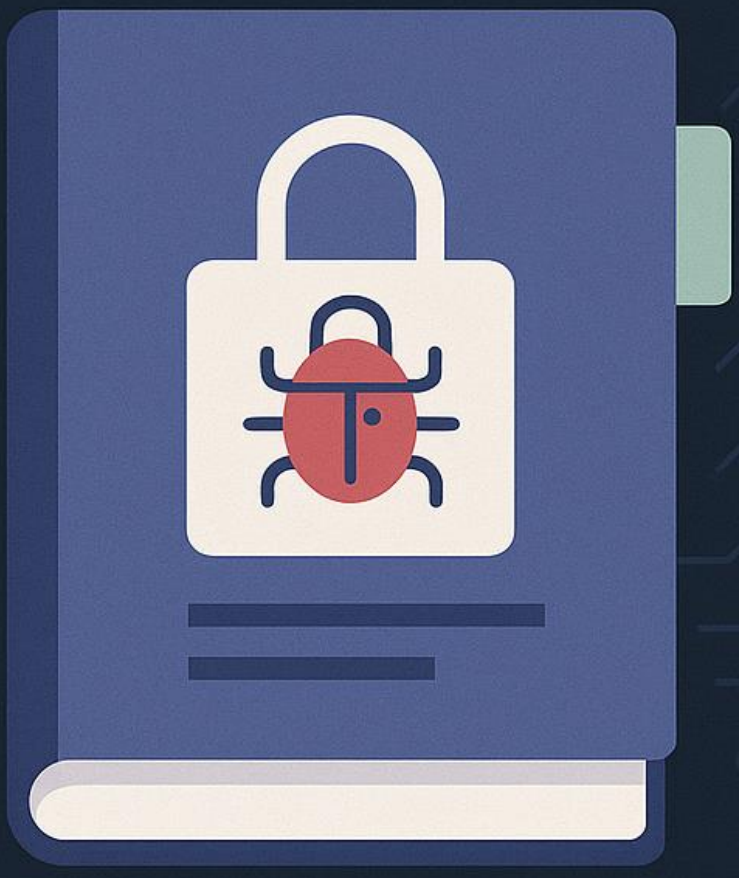
PLAN DE RESPUESTA A INCIDENTE DE RANSOMWARE

BASADO EN NIST



TECHCO

Contenido

Síntesis Ejecutiva

La empresa **TechCo**, dedicada a ofrecer servicios en la nube y al tratamiento de datos confidenciales, ha sido víctima de un incidente de seguridad de tipo *ransomware*, derivado de una campaña de *phishing* dirigida a uno de sus empleados. Este ataque comprometió de forma crítica la disponibilidad, confidencialidad e integridad de los sistemas centrales, incluyendo servidores de archivos, bases de datos de clientes y entornos de respaldo, paralizando temporalmente las operaciones empresariales.

El presente documento constituye un **Plan Formal de Respuesta a Incidentes de Ransomware**, desarrollado en base al **Marco de Ciberseguridad del NIST (National Institute of Standards and Technology)**, que establece cinco funciones clave: **Identificación, Protección, Detección, Respuesta y Recuperación**. A través de este marco, se propone una estrategia integral que abarca desde la evaluación y clasificación de activos críticos, hasta la planificación de escenarios de recuperación, garantizando una mayor resiliencia operativa ante amenazas futuras.

El análisis realizado revela deficiencias estructurales significativas, como la ausencia de segmentación de red, la falta de políticas preventivas de concienciación sobre amenazas internas y externas, la carencia de mecanismos de monitoreo en tiempo real y una inadecuada arquitectura de respaldo, factores que favorecieron la propagación del malware y agravaron el impacto del incidente.

Este plan no solo busca remediar la situación actual, sino también establecer una cultura organizacional orientada a la ciberresiliencia. Para ello, se establecen medidas técnicas, organizativas y procedimentales destinadas a minimizar la superficie de ataque, acortar los tiempos de detección y respuesta, y asegurar la continuidad del negocio ante contingencias similares.

Su correcta implementación permitirá a TechCo **fortalecer su postura de ciberseguridad**, cumplir con los requisitos normativos aplicables (como el RGPD o marcos ISO/IEC 27001), y preservar la confianza de sus clientes, partners y partes interesadas. La creación de un equipo de respuesta a incidentes (CSIRT), la implementación de herramientas SIEM y EDR, así como la integración de prácticas de mejora continua, serán pilares fundamentales para la transformación de su modelo de seguridad.

1. Identificación

La fase de **Identificación** tiene como objetivo reconocer y clasificar los activos más críticos de TechCo, evaluar las vulnerabilidades que facilitaron la intrusión y determinar el nivel de riesgo asociado al incidente. Esta etapa es esencial para priorizar acciones de contención y establecer medidas defensivas adecuadas.

1.1 Infraestructura y Recursos Críticos Comprometidos

Durante el incidente se vieron comprometidos los siguientes activos:

- **Servidor de archivos central**: contenía documentos operativos clave y datos estructurados utilizados en procesos diarios. Su indisponibilidad detuvo tareas administrativas y afectó la eficiencia global de la empresa.
- **Base de datos de clientes**: alojaba información personal y financiera sensible, cuyo cifrado no solo afectó la operativa, sino que generó un riesgo elevado de incumplimiento normativo (p. ej., RGPD).
- **Sistemas de respaldo internos**: se encontraban alojados dentro de la misma red, sin aislamiento ni políticas de acceso diferenciadas, lo que permitió su cifrado por parte del ransomware.
- **Infraestructura de red interna**: su arquitectura plana y carente de segmentación facilitó la propagación lateral del malware a través de múltiples sistemas.

1.2 Análisis de Vulnerabilidades y Riesgos

El ataque puso de manifiesto diversas debilidades estructurales y de gestión:

- **Vulnerabilidad frente a ingeniería social**: el éxito del phishing inicial refleja una baja preparación del personal ante amenazas comunes.
- **Ausencia de segmentación de red**: permitió la expansión incontrolada del ransomware desde el equipo infectado hasta servidores centrales y entornos de backup.
- **Carencia de monitoreo proactivo**: no se contaba con sistemas SIEM o alertas basadas en comportamiento que permitieran detectar actividad sospechosa en fases tempranas.
- **Acceso no controlado a backups**: los respaldos eran accesibles desde los mismos segmentos de red, lo que comprometió su función como última línea de defensa.

1.3 Evaluación de Riesgos

A partir de la clasificación de activos y su grado de exposición, se establece la siguiente jerarquía de riesgo:

- **Riesgo Crítico**: Base de datos de clientes y backups internos.
- **Riesgo Alto**: Servidores de archivos y sistemas administrativos.
- **Riesgo Moderado**: Equipos de usuario final no infectados pero con acceso a red compartida.

Este análisis sirve como base para priorizar acciones de respuesta y fortalecer los controles preventivos.

2. Medidas de Protección Proactiva

La función de **Protección** se centra en implementar controles preventivos que reduzcan la probabilidad de que un incidente de ciberseguridad tenga lugar o se propague. Esta sección detalla las medidas que TechCo debería haber adoptado para evitar o mitigar el impacto del ataque.

2.1 Controles Técnicos y Arquitectónicos Recomendados

- **Segmentación de red por zonas de seguridad** (zona de usuarios, producción, administración y backup), con reglas estrictas de comunicación interzonal.
- **Autenticación multifactor (MFA)** en todos los accesos remotos, interfaces administrativas y servicios críticos.
- **Política de contraseñas robustas**, combinando requisitos de longitud, complejidad y rotación periódica.
- **Control de acceso basado en el principio de mínimo privilegio (PoLP)**, especialmente en servidores compartidos o con datos sensibles.
- **Copias de seguridad automatizadas, cifradas y almacenadas fuera de línea (offline)** o en entornos inmutables (*immutable backups*), con pruebas periódicas de restauración.

2.2 Capacitación del Personal y Cultura de Ciberseguridad

- **Programas de concienciación continua** sobre ciberseguridad, con énfasis en amenazas por correo electrónico y navegación insegura.
- **Simulaciones periódicas de ataques de phishing** para evaluar y reforzar el comportamiento seguro de los empleados.

- **Inclusión obligatoria de formación en ciberseguridad en los procesos de onboarding y reciclaje profesional** del personal.
- **Evaluaciones de madurez organizacional en ciberseguridad**, utilizando frameworks como NIST CSF o CMMI Cybermaturity.

2.3 Marco Normativo y Procedimientos Documentados

- **Política integral de ciberseguridad**, alineada con ISO/IEC 27001, que defina roles, procedimientos y controles técnicos.
- **Política de gestión de incidentes**, con flujos de trabajo definidos, criterios de escalado y mecanismos de notificación interna y externa.
- **Procedimientos documentados de backup y recuperación**, incluyendo roles responsables, tiempos de restauración objetivo (RTO) y punto de recuperación objetivo (RPO).

3. Detección

La función de **Detección** busca identificar eventos de seguridad con la mayor antelación posible, permitiendo activar medidas de contención antes de que un incidente escale o se propague. Esta fase requiere soluciones tecnológicas robustas, reglas de correlación bien definidas y procesos automatizados de escalado.

3.1 Tecnologías de Supervisión e Inteligencia de Amenazas

(antes: Métodos y Herramientas de Detección)

Para mejorar su capacidad de detección, TechCo debe integrar una arquitectura de vigilancia continua basada en las siguientes herramientas:

- **SIEM (Security Information and Event Management)**: permite la recopilación, correlación y análisis centralizado de logs de múltiples sistemas. Recomendado el uso de soluciones como *Wazuh, Splunk, LogPoint o Elastic Stack*.
- **EDR (Endpoint Detection and Response)**: agentes en equipos y servidores que detectan comportamientos anómalos, acceso a procesos sospechosos, ejecución de scripts maliciosos o cambios no autorizados en el sistema.
- **FIM (File Integrity Monitoring)**: seguimiento continuo de la integridad de archivos y configuraciones críticas del sistema.

- **Threat Intelligence Feeds**: integración con fuentes de indicadores de compromiso (IoC) y listas negras actualizadas para bloquear IPs, dominios o hashes conocidos.

3.2 Alarmas Automatizadas y Umbrales de Respuesta Inmediata

(antes: Alertas Tempranas y Respuesta Inmediata)

Los mecanismos de alerta deben estar definidos por políticas que incluyan:

- **Activación de alertas** ante creación masiva de archivos cifrados, picos inusuales en uso de CPU/disco o cambios en permisos de red.
- **Sistemas de detección de patrones** (como Beaconing, Lateral Movement o uso de Powershell no autorizado).
- **Umbrales definidos** que diferencien entre eventos informativos, advertencias y alertas críticas, priorizando respuestas automatizadas en los últimos.
- **Alertas por correo, consola o canales internos seguros**, permitiendo al CSIRT actuar de inmediato.

3.3 Proceso de Escalado y Clasificación de Incidentes

(antes: Procedimiento de Escalado)

Una vez detectado un evento potencialmente malicioso, el procedimiento de escalado debe contemplar:

- **Clasificación del incidente**: tipificación basada en categoría (malware, acceso no autorizado, ransomware...), impacto y urgencia.
- **Registro automático en plataforma ITSM**: todos los eventos críticos deben generar un ticket con traza temporal y responsable asignado.
- **Activación del protocolo de respuesta**: si se confirma un ataque, se activa el plan con los niveles de respuesta establecidos.
- **Notificación estructurada** al Responsable de Seguridad (CISO), líder del CSIRT y equipo de comunicaciones internas.

4. Respuesta

Una respuesta eficaz ante un ataque de ransomware requiere rapidez, coordinación y procedimientos definidos que permitan contener la amenaza, minimizar el impacto y preservar la evidencia. Esta fase debe ejecutarse con

precisión quirúrgica, garantizando que cada actor involucrado actúe conforme a un plan previamente establecido.

4.1 Activación del Protocolo de Emergencia

(antes: Activación del Plan de Respuesta)

La activación de la respuesta debe seguir una lógica secuencial basada en la confirmación técnica del incidente. Las fases clave incluyen:

- **Validación del incidente**: confirmación técnica por parte del equipo de seguridad, identificando la presencia activa del ransomware.
- **Declaración formal del incidente** por parte del CISO o responsable de seguridad.
- **Activación del CSIRT (Computer Security Incident Response Team)** con roles ya asignados y recursos preparados.
- **Ejecución inmediata de medidas de contención**, como la desconexión de nodos afectados, segmentación de tráfico y revocación de credenciales comprometidas.

4.2 Acciones Inmediatas de Contención y Preservación

(antes: Pasos Inmediatos de Respuesta)

En las primeras horas tras la detección, se deben aplicar medidas priorizadas para evitar la expansión del daño y preservar la evidencia:

- **Aislamiento de sistemas infectados**: desconexión física o lógica de equipos de red para evitar propagación lateral.
- **Recolección de artefactos digitales**: imágenes forenses, dumps de memoria, logs de red, y copias de archivos cifrados.
- **Revisión exhaustiva de logs**: correlación de eventos en el SIEM para reconstruir la línea temporal del ataque.
- **Bloqueo de cuentas comprometidas y revocación de accesos**, especialmente credenciales con privilegios elevados.

4.3 Estructura de Roles y Responsabilidades

(antes: Roles y Responsabilidades)

La respuesta debe estar liderada por un equipo multidisciplinar con funciones claramente definidas:

Rol	Responsabilidad Principal
Coordinador del CSIRT	Dirección estratégica de la respuesta y toma de decisiones.
Analista de Seguridad	Contención técnica, análisis forense y evaluación del daño.
Responsable Legal y Compliance	Gestión de implicaciones legales y regulatorias (ej. RGPD).
Encargado de Comunicación	Control del flujo de información interna y externa.
Soporte TI	Apoyo en tareas técnicas de red, servidores y backups.

4.4 Plan de Comunicación de Crisis

(antes: Gestión de la Comunicación)

Una comunicación clara, transparente y controlada es esencial durante la gestión del incidente:

- **Canales de comunicación internos cifrados** (VPN, herramientas seguras como Signal o Element).
- **Informes ejecutivos periódicos** a la dirección con evaluación del impacto, medidas adoptadas y siguientes pasos.
- **Mensajes a empleados** para evitar el uso de sistemas comprometidos y mantener una única línea de información.
- **Notificación a terceros relevantes** (clientes, proveedores, reguladores) de acuerdo con el marco normativo vigente.

5. Recuperación

La fase de **Recuperación** está orientada a restablecer la operatividad de los sistemas afectados, garantizando la integridad de los datos y asegurando que no persista ningún vector de amenaza en el entorno restaurado. Esta etapa debe ejecutarse bajo un enfoque controlado, priorizando servicios críticos y evaluando constantemente los riesgos residuales.

5.1 Validación de Respaldos y Restauración Controlada

(antes: Restauración de Sistemas y Datos)

Una vez contenida la amenaza y asegurada la infraestructura, se procede a la recuperación del entorno digital:

- **Análisis forense de los backups** para descartar alteraciones o presencia de código malicioso.
- **Restauración progresiva por niveles de criticidad**, comenzando con sistemas clave (servidores de autenticación, bases de datos, ERPs...).
- **Implementación de entornos de staging** previos al pase a producción, con pruebas de funcionalidad, integridad y rendimiento.
- **Registro detallado de cada proceso de restauración**, garantizando trazabilidad y control de cambios.

5.2 Plan de Continuidad del Negocio durante la Recuperación

(antes: Continuidad del Negocio)

Mientras se realiza la restauración tecnológica, deben activarse medidas de contingencia para asegurar que las operaciones clave de la empresa continúen:

- **Uso de procedimientos manuales documentados** para tareas críticas que no dependan de los sistemas comprometidos.
- **Redireccionamiento temporal de servicios** (por ejemplo, migración de correo a un entorno seguro alternativo).
- **Refuerzo del soporte técnico** para empleados y clientes ante posibles limitaciones de servicio.
- **Coordinación constante entre áreas de IT, operaciones, legal y atención al cliente** para mantener alineada la respuesta institucional.

5.3 Validaciones Post-Restauración y Auditoría Técnica

(antes: Verificación Post-Restauración)

Antes de dar por concluida la fase de recuperación, se deben realizar tareas exhaustivas de validación para garantizar que los sistemas están operativos y libres de amenazas:

- **Escaneos completos de seguridad (antimalware, vulnerabilidades, IOC)** en los sistemas restaurados.

- **Comparación con imágenes de referencia** o baselines anteriores para detectar modificaciones no autorizadas.
- **Monitorización intensiva durante las primeras 48-72 horas** tras el restablecimiento total.
- **Evaluación externa opcional** por parte de una entidad independiente para certificar la integridad de la recuperación.

6. Mejora continua

Un plan de respuesta a incidentes no debe quedarse estático. El aprendizaje posterior a un ataque como este es clave para que TechCo evolucione, mejore su preparación y no vuelva a verse igual de expuesta. Esta última etapa es donde se consolidan los errores detectados, se ajustan los procesos y se eleva el nivel de madurez en ciberseguridad de forma realista y sostenible.

6.1 Evaluación Crítica del Desempeño

(antes: Evaluación del Plan de Respuesta)

Tras finalizar la contención y la recuperación, toca sentarse y mirar con lupa lo que se ha hecho:

- ¿Cómo de rápido se detectó el ataque?
- ¿Qué falló y qué se hizo bien?
- ¿Se cumplieron los tiempos de reacción esperados?
- ¿El equipo estaba bien coordinado o hubo puntos de bloqueo?

Estas preguntas deben responderse con datos, comparando los tiempos reales frente a los definidos en el plan, y recogiendo feedback del equipo involucrado. Esta evaluación es clave para que el plan no se convierta en un simple documento de “relleno”.

6.2 Lecciones Aprendidas: Documentar, Compartir, Corregir

(antes: Análisis de Lecciones Aprendidas)

Todo incidente deja huella. Y en este caso, el ransomware ha dejado muchas enseñanzas que no se pueden ignorar. Es necesario:

- Reunir a todos los implicados en una sesión post-mortem.
- Documentar los errores detectados y las soluciones improvisadas que funcionaron (o no).

- Corregir lo que no estaba contemplado en el plan original.
- Compartir estos hallazgos con todo el personal técnico y directivo de forma clara, sin tecnicismos innecesarios.

Este paso, bien hecho, es lo que convierte un incidente en una oportunidad de mejora real.

6.3 Revisión Técnica del Plan y Simulacros

(antes: Actualización del Plan)

Un buen plan no solo se escribe: **se prueba**. La actualización del plan debe ir acompañada de:

- Revisiones periódicas, mínimo semestrales o tras cada incidente relevante.
- Inclusión de nuevas amenazas emergentes, técnicas usadas por actores maliciosos actuales, y lecciones internas.
- **Simulacros realistas**: ejercicios de escritorio y pruebas controladas que pongan al equipo en situaciones límite sin consecuencias reales.
- Incorporación de nuevas herramientas o procesos que se hayan identificado como útiles durante el ataque real.

7. Conclusión

Después de este incidente, queda más que claro que TechCo no puede permitirse volver a estar tan expuesta. El ataque de ransomware ha sido un golpe serio, pero también una oportunidad para hacer las cosas bien, desde la base.

Este plan no es solo una respuesta puntual: es una guía viva que debe acompañar a la empresa a partir de ahora. Se ha diseñado con un enfoque realista, aplicando el marco NIST, pero adaptado a la realidad de una empresa como TechCo, con sus puntos fuertes y sus debilidades. Aquí no hay promesas vacías ni soluciones mágicas: lo que se plantea son medidas concretas, escalables y asumibles.

Implementar todo lo aquí descrito —segmentación, formación, monitorización activa, respuesta estructurada y recuperación real— permitirá a TechCo tener una postura de seguridad más fuerte y una cultura más preparada ante cualquier otro intento de ataque. Además, los procesos de mejora continua asegurarán que no se trata de un documento que se guarda en un cajón, sino de una herramienta viva y útil.

La ciberseguridad no es un estado, es un proceso constante. Y este plan es solo el primer paso para recorrer ese camino con más cabeza, más prevención, y sobre todo, más capacidad de respuesta real ante lo que venga.