# Informe de Ciberseguridad según el Marco NIST CSF

**Caso: TechCo bajo Ataque de Ransomware**

---

## 1. <u>Identificación:</u>

**Activos críticos afectados:**

- **Servidor de archivos**: Documentación operativa esencial para el funcionamiento diario.
- **Base de datos de clientes**: Información personal y financiera de carácter sensible.
- **Sistemas de respaldo (backups internos)**: También comprometidos debido a la falta de aislamiento.

**Vulnerabilidades que facilitaron el ataque:**

- Ausencia de segmentación de red que permitió la propagación del ransomware.
- Falta de controles de seguridad en correos electrónicos y detección de phishing.
- Almacenamiento de respaldos en la misma red comprometida.
- Carencia de monitoreo en tiempo real y alertas tempranas.
- Capacitación insuficiente del personal en ciberseguridad.

---

## 2. <u>Protección:</u>

**Medidas preventivas recomendadas:**

- **Segmentación de red** para separar entornos críticos y respaldos.
- **Gestión de identidades y accesos**: Principio de privilegio mínimo y autenticación multifactor (MFA).
- **Protección de respaldos**: Implementar copias externas, cifradas e inmutables, con pruebas periódicas de restauración.
- **Seguridad del correo electrónico**: Filtros antiphishing, bloqueo de archivos sospechosos y sandboxing.
- **Capacitación continua del personal** en concientización sobre phishing y ciberamenazas.
- **Actualización y parches regulares** de sistemas y aplicaciones críticas.
- **Controles de endpoint (EDR/antivirus avanzado)** para prevenir ejecución de ransomware.

---

## 3. Detección:

**Mecanismos de detección propuestos:**

- **SIEM (Security Information and Event Management):** Correlación de eventos y generación de alertas en tiempo real.
- **EDR/NDR (Endpoint/Network Detection and Response):** Identificación de comportamientos anómalos y actividad maliciosa.
- **Alertas de comportamiento de usuario y sistema:** Acceso inusual a grandes volúmenes de archivos.
- **Pruebas periódicas de phishing** y reportes inmediatos de correos sospechosos.
- **Protocolos de alerta temprana** definidos en políticas internas.

---

## 4. Respuesta:

**Plan de acción ante un ataque de ransomware:**

1. **Contención inmediata:** Aislar sistemas afectados de la red para frenar la propagación.

2. **Activación del Comité de Respuesta a Incidentes (CRI):**

    - **CISO / Responsable de Seguridad:** Dirección del proceso.

    - **Equipo de TI:** Contención y análisis técnico.

    - **Área Legal:** Gestión regulatoria y obligaciones legales.

    - **Comunicaciones:** Información clara y transparente a empleados, clientes y medios.

3. **Notificación:** Informar a las autoridades competentes y a clientes afectados según lo requerido por normativas (ej. protección de datos).

4. **Análisis forense digital:** Determinar vector de ataque, alcance e impacto.

5. **Documentación del incidente:** Mantener registros completos para referencia futura.

---

# 5. Recuperación:

**Acciones de recuperación recomendadas:**

- **Restauración de sistemas** a partir de copias de seguridad externas no comprometidas.

- **Validación de integridad** de los datos antes de reincorporar los sistemas a producción.

- **Implementación de planes de continuidad de negocio (BCP) y recuperación ante desastres (DRP)** para mantener servicios críticos durante el proceso.

- **Cambio de credenciales y auditoría de accesos** privilegiados.

- **Reforzamiento de medidas de seguridad** antes de habilitar nuevamente la red completa.

**Mejora continua posterior al incidente:**

- Realización de un **informe post-incidente** con lecciones aprendidas.
- Actualización periódica del plan de respuesta a incidentes.
- Simulacros de ransomware y ejercicios de cibercrisis.
- Refuerzo de la cultura de seguridad en toda la organización.

---

# Conclusión

El ataque de ransomware sufrido por TechCo expuso deficiencias significativas en seguridad de la información, principalmente en segmentación de red, protección de respaldos y concientización del personal. La adopción del marco NIST CSF permite establecer un enfoque sistemático y continuo que fortalezca la capacidad de **identificar, proteger, detectar, responder y recuperar**, garantizando la resiliencia de la organización frente a futuros incidentes.