## Actividad de Evaluación: Elaboración de un Informe de Incidente

**Introducción para el Alumnado:**

Vuestra misión es actuar como analistas de un Equipo de Respuesta a Incidentes (CSIRT). A continuación, se presenta un escenario detallado de un ciberataque. Debéis analizar toda la información proporcionada, estructurar vuestros hallazgos y decisiones utilizando la plantilla de informe de incidentes, y completarla basándoos en un framework reconocido como **NIST SP 800-61** o **SANS PICERL**.

El objetivo es evaluar vuestra capacidad para analizar, documentar y gestionar un incidente de seguridad de principio a fin.

---

## Plantilla de Informe de Incidente (Para rellenar)

**(Basada en las fases del framework NIST SP 800-61)**

**INFORME DE INCIDENTE DE SEGURIDAD**

| | | |
|---|---|---|
| **ID del Incidente:** | **INC-20250725-001** | **Fecha de Detección: 25/07/2025 08:15 AM CEST** |
| **Estado:** | **Cerrado** | **Prioridad: Crítica** |
| **Reportado por:** | **Administradora de Sistemas (Usuario interno)** | **Analista Asignado: Ivana Sánchez con ID 0013** |

### 1. Resumen Ejecutivo

**El 25 de julio de 2025, se detectó un incidente de seguridad en la empresa Gestoría Integral Global que resultó en el cifrado de datos críticos en el servidor de aplicaciones (SRV-APP-01) debido a un ataque de ransomware. La amenaza se originó por un acceso no autorizado a través de RDP, explotando credenciales débiles de una cuenta de administrador local. El impacto principal fue la pérdida de disponibilidad de los datos y servicios alojados en SRV-APP-01. El incidente ha sido contenido, erradicado y los sistemas se encuentran en proceso de recuperación/restaurados en un plazo de aproximadamente 6 horas desde la detección.**

## 2. Detección y Análisis

- **2.1. Vector de Ataque:** *¿Cómo entró la amenaza?*

  **El vector de ataque principal fue el Escritorio Remoto (RDP) expuesto a Internet. El atacante utilizó un ataque de fuerza bruta contra el puerto RDP del servidor de aplicaciones (SRV-APP-01).**

- **2.2. Indicadores de Compromiso (IoCs):** *Listado de evidencias técnicas.*
  - **Credenciales comprometidas:** Cuenta `admin_local` con contraseña débil.
  - **Actividad RDP anómala:** Intentos de fuerza bruta y posterior inicio de sesión exitoso desde una IP externa desconocida.
  - **Desactivación de servicios de seguridad:** Antivirus y otros servicios de seguridad deshabilitados en SRV-APP-01.
  - **Ejecución de ransomware:** Presencia y ejecución de software de cifrado.
  - **Archivos cifrados:** Disco C: y unidades de datos del servidor cifradas.
  - **Nota de rescate:** Aparición de una nota de rescate en el escritorio del servidor.
  - **Fallo de autenticación RDP:** Las credenciales legítimas de la administradora de sistemas fueron rechazadas.

- **2.3. Alcance e Impacto:** *¿Qué sistemas y datos están afectados? ¿Cuál es el impacto en el negocio?*

  - **Sistemas afectados:** Principalmente el servidor de aplicaciones **SRV-APP-01**.
  - **Datos afectados:** Todos los datos y el sistema operativo en el disco C: y las unidades de datos de SRV-APP-01 fueron cifrados por el ransomware. Esto incluye aplicaciones críticas y la información que gestionan.
  - **Impacto en el negocio:**
    - **Pérdida de disponibilidad:** Interrupción total de los servicios y aplicaciones alojados en SRV-APP-01.
    - **Pérdida de productividad:** Los empleados de la gestoría no pudieron acceder a las aplicaciones esenciales para sus operaciones diarias.
    - **Posible pérdida de datos:** Riesgo de pérdida permanente de datos si la recuperación no es exitosa o si los backups no están actualizados/disponibles.
    - **Daño reputacional:** Potencial impacto en la confianza de los clientes debido a la interrupción del servicio y la posible afectación de sus datos.

## 3. Contención, Erradicación y Recuperación

- **3.1. Estrategia de Contención:** *Medidas inmediatas tomadas para aislar la amenaza.*
  - **Medida inmediata:** Tras la confirmación visual de la nota de rescate, se procedió a la **desconexión inmediata de SRV-APP-01 de la red (física o lógica)** a las **08:25 AM CEST** para evitar cualquier propagación adicional del ransomware o exfiltración de datos.

- **Bloqueo de IP/Credenciales:** Se bloquearon las IPs de origen del ataque en el firewall perimetral y se deshabilitó la cuenta admin_local a las **08:35 AM CEST**

- **3.2. Plan de Erradicación:** *Pasos para eliminar completamente la amenaza de los sistemas.*

  - **Identificación y eliminación del ransomware:** A partir de las 08:45 AM CEST, se inició un análisis forense del SRV-APP-01 para identificar el tipo de ransomware, su persistencia y eliminar cualquier rastro.
  - **Limpieza de sistemas:** Formateo completo del SRV-APP-01 para asegurar la eliminación total de la amenaza, comenzando a las 09:30 AM CEST.
  - **Parcheo y endurecimiento:** Aplicación de todos los parches de seguridad pendientes en el sistema operativo y las aplicaciones, y endurecimiento de la configuración de RDP (cambio de puerto, uso de VPN para acceso externo, etc.).
  - **Revisión de credenciales:** Auditoría de todas las cuentas de administrador local y de dominio para identificar y fortalecer contraseñas débiles o sin MFA.

- **3.3. Plan de Recuperación:** *Procedimiento para restaurar los sistemas y datos a su estado normal.*

  - **Restauración de backups:** A partir de las **10:00 AM CEST**, se inició la restauración de SRV-APP-01 desde la última copia de seguridad limpia y validada (anterior a las 02:30 AM del 25/07/2025).
  - **Verificación de integridad:** Una vez restaurado, se realizó una verificación exhaustiva de la integridad de los datos y la configuración del sistema a las **12:00 PM CEST**.
  - **Pruebas de funcionalidad:** Se llevaron a cabo pruebas de funcionalidad de todas las aplicaciones y servicios en SRV-APP-01 para asegurar su correcto funcionamiento, finalizando a las **14:00 PM CEST**.
  - **Monitoreo intensivo:** Se implementó un monitoreo adicional en SRV-APP-01 y otros sistemas críticos durante un periodo post-recuperación, a partir de las **14:00 PM CEST**.

**4. Actividad Post-Incidente (Lecciones Aprendidas)**

- **4.1. Causa Raíz:** *Análisis final de por qué el ataque tuvo éxito.*
  La causa raíz principal del incidente fue la **exposición directa del puerto RDP a Internet combinada con una contraseña débil** en una cuenta de administrador local y la **ausencia de Autenticación Multifactor (MFA)**. Esto permitió al atacante obtener acceso inicial al servidor y, posteriormente, desplegar el ransomware sin impedimentos significativos por parte de los servicios de seguridad deshabilitados.
- **4.2. Mejoras y Recomendaciones:** *Acciones a implementar para evitar futuros incidentes.*

**Mejoras en Protección:**

- **Deshabilitar RDP directo a Internet:** Configurar el acceso RDP solo a través de una VPN o un bastion host.
- **Implementar MFA:** Establecer MFA obligatorio para todas las cuentas de acceso remoto y privilegiadas.
- **Políticas de contraseñas robustas:** Forzar contraseñas complejas y rotación periódica para todas las cuentas, especialmente las de administrador.
- **Gestión de vulnerabilidades:** Implementar un programa de escaneo y parcheo proactivo para todos los sistemas expuestos y críticos.
- **Endurecimiento de sistemas:** Revisar y aplicar configuraciones de seguridad recomendadas (CIS Benchmarks) a todos los servidores.

**Mejoras en Detección:**

- **Monitoreo de logs RDP:** Implementar alertas en el SIEM para intentos fallidos de RDP, inicios de sesión inusuales (fuera de horario, desde IPs desconocidas) y cambios en la configuración de seguridad del sistema (ej. desactivación de antivirus).
- **Solución EDR:** Desplegar una solución de Detección y Respuesta de Endpoints (EDR) en todos los servidores para detectar y responder a actividades maliciosas como la desactivación de servicios de seguridad o la ejecución de ransomware.

**Mejoras en Respuesta y Recuperación:**

- **Pruebas de backups:** Realizar pruebas periódicas y automatizadas de la restauración de copias de seguridad para asegurar su validez y rapidez.
- **Plan de comunicación:** Desarrollar un plan de comunicación de incidentes que incluya plantillas y procedimientos para notificar a la dirección, empleados y, si es necesario, a clientes o autoridades.
- **Simulacros:** Realizar simulacros de incidentes (tabletop exercises) para probar la eficacia del plan de respuesta y la coordinación del equipo.

- **4.3. Cronología de Eventos Clave:** *Resumen de la línea de tiempo del incidente.*

- **02:30 AM:** Atacante inicia ataque de fuerza bruta RDP contra SRV-APP-01.
- **03:15 AM:** Atacante adivina contraseña de `admin_local` y obtiene acceso.
- **03:30 AM:** Atacante desactiva antivirus y servicios de seguridad en SRV-APP-01.
- **04:00 AM:** Atacante ejecuta ransomware, cifrando discos de SRV-APP-01.
- **08:15 AM:** Administradora de sistemas intenta conectar por RDP y es rechazada (detección).
- **08:20 AM:** Administradora accede por consola de hipervisor y confirma nota de rescate (confirmación del incidente).
- **08:25 AM:** Desconexión de SRV-APP-01 de la red (contención).
- **08:35 AM:** Bloqueo de IP de origen y deshabilitación de cuenta `admin_local`.
- **08:45 AM:** Inicio de análisis forense rápido y planificación de erradicación/recuperación.
- **09:30 AM:** Inicio de formateo y reconstrucción de SRV-APP-01.
- **10:00 AM:** Inicio de restauración de SRV-APP-01 desde backup.
- **12:00 PM:** Verificación de integridad de datos y configuración.

- **14:00 PM:** Finalización de pruebas de funcionalidad y servicios operativos (cierre del incidente operativo).

# 5. Conclusiones

**El incidente del 25 de julio de 2025 puso de manifiesto la criticidad de la gestión de accesos remotos y la necesidad de implementar medidas de seguridad robustas en los puntos de exposición a Internet. La rápida actuación del equipo de TI permitió contener y recuperar los sistemas en un tiempo razonable, mitigando un impacto mayor. Sin embargo, las lecciones aprendidas subrayan la importancia de la prevención proactiva, especialmente en lo que respecta a la autenticación y la gestión de vulnerabilidades. La implementación de las recomendaciones propuestas es fundamental para evitar la recurrencia de incidentes similares y fortalecer la resiliencia de la organización frente a ciberataques.**

---

## Escenarios de Incidente

### Variante 4: El Acceso Remoto Comprometido

- **Empresa:** Gestoría Integral Global (Asesoría, 60 empleados).
- **Fecha del Incidente:** Viernes, 25 de julio de 2025.
- **Línea de Tiempo y Eventos:**
    - **02:30 AM:** Un atacante, usando credenciales compradas en la dark web, inicia un ataque de fuerza bruta contra el puerto de Escritorio Remoto (RDP) del servidor de aplicaciones (`SRV-APP-01`), que está expuesto a Internet.
    - **03:15 AM:** El atacante consigue adivinar la contraseña de una cuenta de administrador local (`admin_local`) que tenía una contraseña débil y sin MFA.
    - **03:30 AM:** El atacante accede al servidor, desactiva el antivirus y otros servicios de seguridad.
    - **04:00 AM:** El atacante ejecuta el ransomware, que cifra el disco C: y las unidades de datos del servidor.
    - **08:15 AM:** Como administradora de sistemas, intentas conectar por RDP para el mantenimiento semanal, pero tus credenciales son rechazadas.
    - **08:20 AM:** Accedes a la consola del hipervisor (VMware) y abres la consola de la máquina virtual. El escritorio del servidor muestra una nota de rescate.