UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Módulo 6:

Respuesta a Incidentes y Análisis Forense Digital

Sesión 1:

Fundamentos de respuesta a incidentes de seguridad

OBJETIVO DE LA SESIÓN:

Comprender qué es un incidente de seguridad, identificar las etapas del ciclo de respuesta, y aprender a documentar adecuadamente una respuesta inicial.

¿Qué es un incidente de seguridad?

Un incidente de seguridad de la información es cualquier evento que compromete la confidencialidad, integridad o disponibilidad de la información.

Ejemplos comunes:

Acceso no autorizado a un sistema
Pérdida de información confidencial
Infección por malware
Uso indebido de credenciales

Tipos de incidentes

Tipo de incidente	Ejemplo
Acceso no autorizado	Hackeo de correo electrónico
Malware	Ransomware en red empresarial
Pérdida de información	Extracción de datos por USB
Negación de servicio (DoS)	Ataque que colapsa un sitio web

¿Qué es NIST 800-61?

La Publicación Especial 800-61 del Instituto Nacional de Estándares y Tecnología (NIST) proporciona directrices integrales diseñadas para ayudar a las organizaciones a desarrollar capacidades efectivas de respuesta a incidentes.

Objetivo:
Responder de forma rápida, organizada y efectiva para minimizar el impacto de incidentes.

Ventajas de seguir NIST 800-61

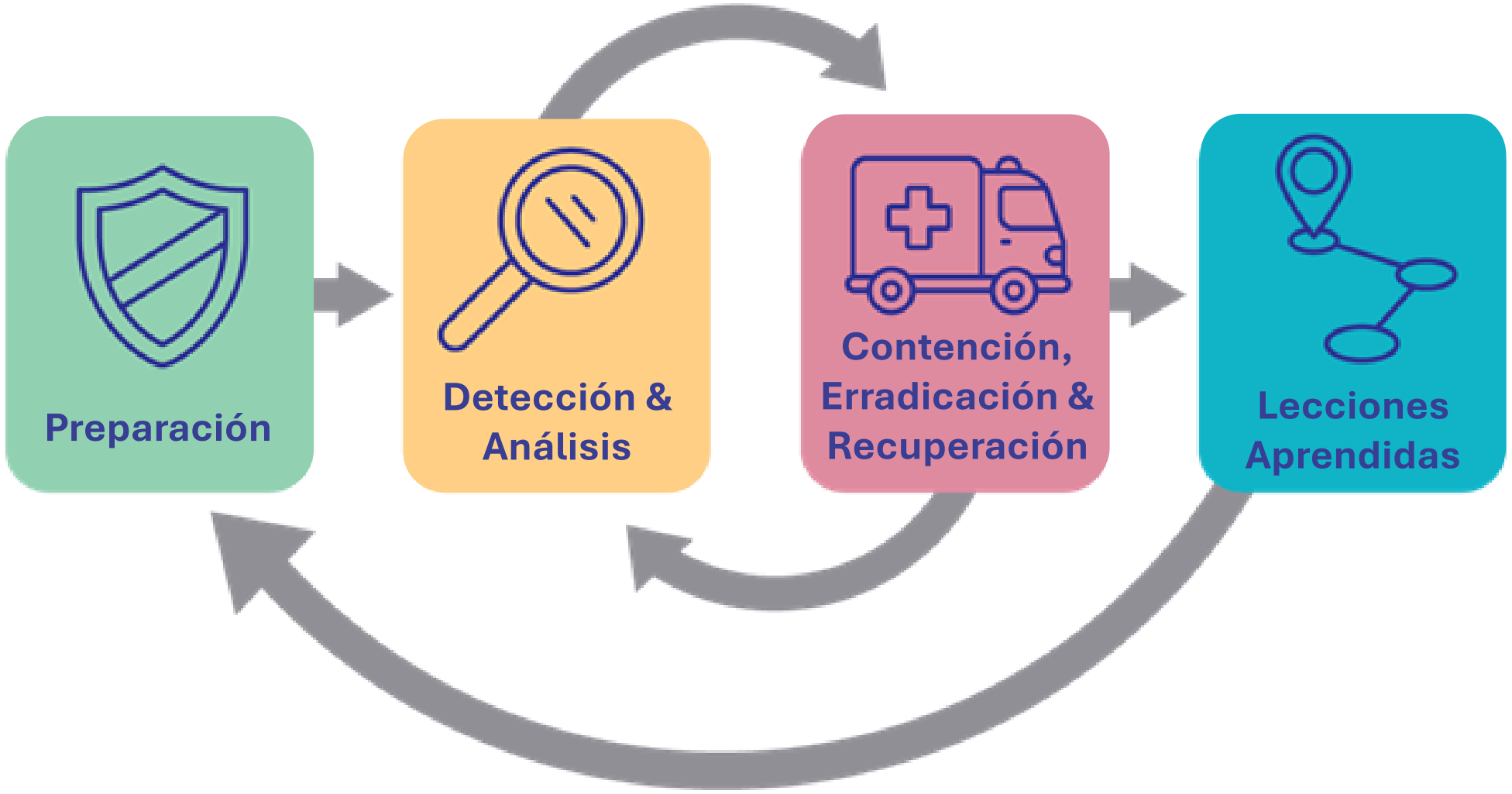
- Proporciona un marco estructurado que pueden adaptar organizaciones grandes o pequeñas.
- Reduce el tiempo de respuesta y las pérdidas económicas.
- Establece roles claros (equipo de respuesta a incidentes, gestión, comunicación).
- Fomenta la mejora continua en la ciberseguridad.
- Facilita la coordinación con autoridades y cumplimiento normativo.

Ciclo de Respuesta a Incidentes (NIST 800-61)

La gestión efectiva de incidentes no es solo reaccionar cuando algo ocurre. Es un proceso estructurado y continuo que se compone de cuatro fases fundamentales:

1. Preparación
2. Detección y análisis
3. Contención, erradicación y recuperación
4. Lecciones aprendidas

Ciclo de Respuesta a Incidentes (NIST 800-61)



Ciclo de Respuesta a Incidentes (NIST 800-61)

1. Preparación

Esta fase ocurre **antes** de que ocurra un incidente. Su objetivo es **fortalecer la capacidad organizacional** para responder de forma rápida y efectiva.

Componentes clave

- **Políticas y procedimientos de respuesta a incidentes:** Documentos oficiales que indican cómo actuar.
- **Equipo de respuesta a incidentes (CSIRT o IRT):** Personal capacitado y con roles claros.
- **Herramientas tecnológicas:** Firewalls, sistemas de detección de intrusos (IDS/IPS), antivirus, sistemas de monitoreo, etc.
- **Simulacros y ejercicios:** Prácticas periódicas para evaluar la preparación.
- **Capacitación del personal:** Todos los empleados deben conocer cómo identificar y reportar incidentes.

Ejemplo práctico:

Una universidad establece un protocolo donde si un estudiante detecta un intento de phishing, debe reportarlo al área de TI usando un formulario específico. Se capacita al personal con simulacros de correos falsos.

Ciclo de Respuesta a Incidentes (NIST 800-61)

2. Detección y análisis

Aquí comienza la **acción directa** cuando se detecta un posible incidente.

Actividades esenciales

- **Identificación de señales:** Logs del sistema, alertas del antivirus, reportes de usuarios, etc.
- **Correlación de eventos:** Analizar múltiples señales para confirmar si realmente es un incidente.
- **Clasificación del incidente:** Determinar tipo, gravedad, alcance y activos afectados.
- **Notificación interna:** Informar a los responsables adecuados.
- **Documentación:** Registrar todo desde el primer momento.

Ejemplo práctico:

Se detecta una actividad anómala en la red en horarios inusuales. Al investigar los logs, el equipo identifica conexiones remotas desde un país no habitual y acceso a archivos sensibles. Se confirma que hubo un acceso no autorizado.

Ciclo de Respuesta a Incidentes (NIST 800-61)

3. Contención, erradicación y recuperación

El objetivo es limitar el daño, eliminar la amenaza y volver a la normalidad.

Contención

- Aislar los sistemas afectados (por ejemplo, desconectarlos de la red).
- Redireccionar tráfico o bloquear accesos.
- Implementar reglas temporales en el firewall.

Erradicación

- Eliminar el malware, usuarios maliciosos, puertas traseras.
- Reinstalar sistemas comprometidos o restaurar versiones limpias.

Recuperación

- Verificar que el sistema está limpio y funcional.
- Reincorporar sistemas al entorno productivo.
- Monitorear intensivamente para detectar recurrencias.

Ejemplo práctico:

Un servidor fue infectado con ransomware. Se desconecta de la red, se reinstala desde una imagen segura, se restauran archivos desde backup y se monitoriza por una semana antes de reactivarlo completamente.

Ciclo de Respuesta a Incidentes (NIST 800-61)

4. Lecciones aprendidas (Post-Incident)

Una fase **frecuentemente olvidada** pero esencial para mejorar continuamente.

¿Qué incluye?

- **Revisión del incidente:** ¿Qué pasó? ¿Qué se hizo bien y qué no?
- **Análisis de causas raíz.**
- **Actualización de políticas y controles.**
- **Informes finales para gerencia y áreas responsables.**
- **Capacitación adicional si se detectaron errores humanos.**

Ejemplo práctico:

Luego de un incidente, se descubre que el phishing tuvo éxito porque algunos usuarios no reconocieron el correo falso. La organización decide reforzar la capacitación en detección de ingeniería social y activar el segundo factor de autenticación en todos los sistemas.

Caso de Estudio

Objetivo: aplicar el ciclo de respuesta NIST 800-61 para gestionar el incidente.

Imagina que trabajas en una universidad. Un día, recibes un correo que parece venir del área de Soporte de TI. El mensaje es claro y urgente:

"Tu contraseña va a expirar, actualízala ahora para no perder acceso a tu cuenta".

El correo luce convincente: tiene el logo institucional, la firma de un supuesto administrador y un enlace que lleva a una página casi idéntica al portal de la universidad.

En total, 50 personas reciben este mensaje. La mayoría sospecha y lo ignora, pero 12 usuarios hacen clic y escriben sus credenciales en el sitio falso.

Con esas claves, los atacantes logran entrar al correo institucional y acceder a documentos compartidos. Ahora la universidad enfrenta un incidente serio de seguridad.

Roles en un equipo de respuesta

- Líder del equipo de incidentes (IRT)
- Analista técnico
- Comunicación interna / externa
- Soporte legal / RRHH

Documentación básica de un incidente

- Fecha y hora
- Afectados
- Impacto
- Medidas tomadas
- Evidencias recogidas

Resumen

- **Día 0 08:15**: Llega la campaña de phishing (asunto “Actualización de seguridad”).
- **08:40–10:30**: 12 usuarios entregan credenciales.
- **10:45**: Alertas de login desde IPs inusuales (fuera del país).
- **11:10**: Usuario reporta correo raro enviado “desde su cuenta”.
- **11:30**: Se declara **incidente de seguridad** (phishing con compromiso).
- **11:40–18:00**: Contención (bloqueos, reseteos, revocar sesiones).
- **Día 1**: Erradicación técnica y limpieza de buzones/reglas maliciosas.
- **Día 2**: Recuperación completa; monitoreo reforzado 30 días.
- **Semana 2**: Lecciones aprendidas, actualización de políticas y formación.

Fase 1: Preparación (antes del incidente)

Capacidades existentes

- Políticas: uso aceptable del correo, reporte de incidentes, gestión de contraseñas.
- Equipo: **IRT** con Roles (Líder IR, Analista, Comunicación, soporte legal).
- Herramientas: correo en la nube (con logs), **MFA opcional**, SIEM básico, EDR en PCs.
- Backups: diarios de buzones y repositorios (probados mensualmente).

Brechas detectadas

- Capacitación anti-phishing **no obligatoria**.
- MFA **no forzado** para todo el personal.
- Procedimientos desactualizados para “phishing masivo + robo de credenciales”.

Entregables de la fase

- Políticas y procedimientos vigentes, catastro de activos, contactos de emergencia, plantillas de comunicación.

Fase 2: Detección y Análisis (qué pasó)

Señales/Indicadores de compromiso (IoCs)

- Dominios/URLs maliciosas:
  - it-soporte-univ[.]secure-login[.]site/login
- IPs de acceso anómalas:
  - 185.XX.34.10; 37.XX.120.87 (geolocalizadas fuera del país).
- Cabeceras del correo: **spoofing** de display name, dominio parecido al oficial.

Análisis

Clasificación: Phishing → Compromiso de cuenta (Account Takeover).
Severidad: Alta (12 cuentas, potencial acceso a docs sensibles).
Alcance: Buzones, unidades compartidas, riesgo de robo de información

Tareas clave

Correlacionar logs de correo, SIEM y geolocalización.
Identificar **todas las cuentas** con inicio de sesión desde IoCs.
Verificar creación de reenvíos/alias/reglas sospechosas.
Determinar datos tocados/exfiltrados (descargas inusuales).

Fase 3: Contención (cortar el daño rápido)

Contención inmediata (0–4 h)

- Deshabilitar **12 cuentas** comprometidas y forzar **cambio de contraseña** global.
- Revocar **tokens/sesiones** activos en la nube.
- Bloquear **dominios/URLs/IPs IoC** en el proxy/firewall y lista de seguridad del correo.
- Eliminar el **correo malicioso** en todas las bandejas (search & purge).
- Mensaje a la comunidad: **no hacer clic**, reportar si recibieron/accionaron.

Contención a corto plazo (4–24 h)

- Forzar **MFA** en todas las cuentas con riesgo alto.
- Aislar endpoints sospechosos con EDR para revisión.
- Bloquear **creación de reenvíos externos** temporalmente.
- Limitar compartir externos en unidades críticas.

Criterios de éxito

- Sin nuevos logins desde IoCs.
- Todas las contraseñas rotadas.
- Correos maliciosos erradicados.

Fase 3: Erradicación (quitar la causa)

Acciones

- Eliminar **reglas de buzón** maliciosas y reenvíos.
- Revisar y revocar **consentimientos OAuth** sospechosos (apps de terceros).
- Reconfigurar SPF/DKIM/DMARC si hay debilidades.
- Parchear sistemas/outlook/plug-ins; endurecer políticas de acceso.
- Revisión de endpoints: no hay malware persistente.

Verificación

- Auditoría de cambios por usuario.
- Validación de que no quedan rutas de acceso (tokens, apps, claves guardadas).

Entregables

- Lista de cambios revertidos, reporte de IoCs neutralizados.

Fase 3: Recuperación (volver a la normalidad)

Pasos

- Rehabilitar cuentas con **MFA** habilitado y políticas de contraseña robusta.
- Restaurar **configuración legítima** de buzones/unidades.
- Monitoreo intensivo 30 días (alertas de geolocalización, reglas, descargas masivas).
- Comunicación final a usuarios con **buenas prácticas** y canal de reporte.

Criterios de cierre

- 0 alertas críticas en periodo de observación.
- Validación de que no hubo **exfiltración** significativa (o gestionada).

Entregables

- Acta de **vuelta a la operación**, lista de verificación de recuperación.

Fase 4: Lecciones Aprendidas (mejora continua)

1. ¿Por qué cayeron? → Correo convincente + falta de entrenamiento.
2. ¿Por qué hubo compromiso? → **MFA no obligatorio**.
3. ¿Por qué se propagó? → Reglas de buzón y tokens no monitoreados.
4. ¿Por qué no se detectó antes? → Detecciones de geolocalización “suaves”.
5. ¿Cómo evitarlo? → **MFA + simulacros + detecciones fuertes + actualizaciones**.

Plan de mejora

- MFA **obligatorio** para toda la comunidad.
- Simulacros de phishing trimestrales y capacitación obligatoria.
- Reglas de detección: “imposible travel”, nuevas reglas de buzón, picos de descarga.
- Actualizar y probar **runbooks** (procedimiento) “Phishing + Compromiso de cuenta”.
- Revisar postura SPF/DKIM/DMARC; bloquear reenvíos externos por defecto.

Ejercicio 2: Análisis de un caso real de incidente

En enero de 2023, una clínica privada en América Latina fue atacada por un ransomware. Todos los archivos clínicos fueron cifrados. La clínica no contaba con respaldo actualizado y no tenía plan de respuesta a incidentes. El área TI tardó 48 horas en detectar la causa. Se intentó recuperar el sistema sin ayuda externa. Finalmente, se recurrió a pagar el rescate a un grupo anónimo. El incidente afectó la atención de pacientes durante 5 días y fue difundido por medios locales.

Encuentre el texto completo en la plataforma: **Incidente de Ransomware en Clínica Privada**

Ficha de Análisis de Incidente de Seguridad

1. ¿Qué tipo de incidente se presentó?
2. ¿Qué activos fueron comprometidos o afectados?
3. ¿Cuáles fueron los errores cometidos por la organización?
4. ¿Qué acciones se tomaron correctamente?
5. ¿Qué fases del ciclo de respuesta a incidentes están presentes o ausentes en este caso?
6. ¿Qué consecuencias generó el incidente para la clínica?
7. ¿Qué acciones de prevención propondrías para evitar que vuelva a ocurrir?
8. ¿Qué lecciones deja este incidente para otras organizaciones similares?

1. ¿Qué tipo de incidente se presentó?

Un ataque de ransomware. Se secuestro el sistema y se pidió rescate

2. ¿Qué activos fueron comprometidos o afectados?

- Historias clínicas digitales. (Datos)
- Sistema de gestión de pacientes (Datos y software).
- Infraestructura de TI de la clínica (servidores, almacenamiento) (hardware).

3. ¿Cuáles fueron los errores cometidos por la organización?

- No tener copias de seguridad actualizadas.
- No contar con un plan formal de respuesta a incidentes
- Demora excesiva en identificar el ataque (48h).
- Intentar resolver sin apoyo externo especializado.
- Decidir pagar el rescate sin avisar a autoridades.

4. ¿Qué acciones se tomaron correctamente?

- Intentar restaurar los sistemas (aunque de forma manual e improvisada).
- Finalmente restaurar operaciones (aunque pagando rescate).

5. ¿Qué fases del ciclo de respuesta a incidentes están presentes o ausentes?

- Preparación: ausente (no había backups ni plan).
- Detección y análisis: tardía (48h después).
- Contención, erradicación y recuperación: limitada (recuperación parcial tras pago).
- Lecciones aprendidas: ausente, no se menciona.

6. ¿Qué consecuencias generó el incidente para la clínica?

- Pérdida de disponibilidad de sistemas durante 5 días.
- Retraso/reprogramación de procedimientos médicos.
- Riesgo de exposición de datos sensibles.
- Impacto reputacional negativo (medios de comunicación).
- Investigación de la autoridad de salud.
- Costos económicos (rescate, tiempo de inactividad).

7. ¿Qué acciones de prevención propondrías?

- Implementar un sistema de copias de seguridad frecuentes y verificadas.
- Diseñar y probar un plan de respuesta a incidentes (IRP).
- Capacitar al personal en ciberseguridad (phishing, ingeniería social).
- Instalar soluciones de detección temprana.
- Mantener los sistemas y parches de seguridad actualizados.
- Definir protocolos de comunicación con autoridades y proveedores especializados.

8. ¿Qué lecciones deja este incidente para otras organizaciones similares?

- La falta de preparación convierte un incidente grave en una catástrofe.
- Es más barato invertir en prevención que pagar rescates.
- Los sistemas de salud son objetivos críticos para ciberdelincuentes.
- Contar con copias de seguridad, segmentación de redes y entrenamiento del personal puede marcar la diferencia entre recuperarse en horas o paralizarse por días.

¿Hubieran pagado el rescate o no?

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. Burgett, A. (2024, mayo 8). *Practical incident response guidance from NIST SP 800-61. ArmorPoint.* https://armorpoint.com/2024/05/08/a-step-by-step-guide-to-incident-response-practical-guidance-from-nist-sp-800-61/
6. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide : Recommendations of the national institute of standards and technology. National Institute of Standards and Technology.*
7. *NIST Incident Response Life Cycle Explained. (s/f).* Cynomi.com. *Recuperado el 4 de septiembre de 2025, de* https://cynomi.com/nist/nist-incident-response-life-cycle-explained/
8. *Vaishnav, D. (2024, junio 29). NIST SP 800–61 Incident Response Life cycle explained. Medium.* https://medium.com/@divyesh.vaishanv/nist-sp-800-61-incident-response-life-cycle-explained-b7b63372cd3c