2025

FASE 3

PLAN DE RESPUESTA DE INCIDENTES Y CERTIFICACIÓN

EMMANUEL IZAGUIRRE RUIZ

Plan de respuesta a incidentes (PRI) basado en NIST

Introducción

Este documento describe el plan de respuesta a incidentes para proteger los sistemas críticos de la organización, que se basa en el marco del NIST 800-61 y tiene como objetivo minimizar el impacto de incidentes de seguridad.

ROLES Y RESPONSABILIDADES

- **Equipo de Respuesta a Incidentes (CSIRT):** Responsable de la detección, análisis y mitigación de incidentes.
- **Administrador de Sistemas:** Asegura la disponibilidad y configuración segura de los servidores.
- **Encargado de Seguridad:** Define políticas y estrategias de prevención.

Fases del Plan de Respuesta a Incidentes

Implementación de herramientas de monitoreo (SIEM, IDS/IPS).

Recolección y almacenamiento de logs desde múltiples fuentes (firewalls, servidores, endpoints, etc.).
Correlación de eventos para detectar patrones de ataque.
Generación de alertas sobre actividades sospechosas.
Análisis forense para investigar incidentes de seguridad.
Cumplimiento normativo (ISO 27001, NIST, PCI-DSS, etc.).

Herramientas SIEM populares

- **Splunk** (uno de los más usados, pero costoso).
- **IBM QRadar** (potente en correlación de eventos).
- **Elastic Security (ELK Stack)** (open-source).
- **AlienVault USM (de AT&T)**.
- **Microsoft Sentinel** (nativo de Azure).

IDS/IPS (Intrusion Detection/Prevention System)

Los sistemas **IDS (Sistema de Detección de Intrusos)** y **IPS (Sistema de Prevención de Intrusos)** analizan el tráfico de red para identificar y bloquear amenazas en tiempo real.

Diferencias clave:

- **IDS (Intrusion Detection System):** Solo detecta ataques y genera alertas, pero no los bloquea.
- **IPS (Intrusion Prevention System):** Detecta y bloquea automáticamente amenazas.

Funciones principales

Monitoreo del tráfico de red en busca de ataques (DDoS, malware, exploits).
Uso de firmas y heurística para detectar amenazas conocidas y desconocidas.
Bloqueo automático de ataques (solo en IPS).
Integración con SIEM para mejorar la detección de amenazas.

- **Herramientas IDS/IPS populares**

  - **Snort** (open-source y muy utilizado).
  - **Suricata** (similar a Snort, pero más avanzado).
  - **Zeek (Bro)** (fuerte en análisis de tráfico).
  - **Cisco Firepower** (solución comercial con integración en firewalls).
  - **Palo Alto Networks** (firewall con IPS avanzado).

Contención: Aislamiento de sistemas comprometidos

El objetivo es evitar la propagación del ataque y minimizar el daño.

Acciones clave:

- Desconectar los sistemas comprometidos de la red (aislamiento lógico o físico).
- Bloquear direcciones IP sospechosas en firewalls y routers.
- Deshabilitar cuentas de usuario comprometidas.
- Redirigir tráfico malicioso usando reglas en IDS/IPS.
- Implementar soluciones de segmentación de red para contener la amenaza.

Erradicación: Eliminación de malware y puertas traseras

Después de contener la amenaza, es necesario **limpiar los sistemas** para evitar futuras reinfecciones.

Acciones clave:

- Realizar un análisis forense para identificar el vector de ataque.
- Eliminar malware, rootkits y cualquier software malicioso detectado.
- Revocar accesos no autorizados y cambiar credenciales comprometidas.
- Aplicar parches y actualizar sistemas para corregir vulnerabilidades explotadas.
- Eliminar configuraciones maliciosas (como scripts persistentes o reglas en firewalls).

Consideraciones:

- Verificar que no haya **persistencia** del atacante en el sistema.
- Usar herramientas como **ESET, Malwarebytes, ClamAV** para análisis y eliminación de malware.
- Revisión manual de logs para identificar posibles **backdoors**.

Recuperación: Restauración de sistemas desde backups seguros

El objetivo es restaurar los sistemas afectados y devolverlos a un estado seguro.

Acciones clave:

- Restaurar desde **copias de seguridad confiables** (preferiblemente almacenadas offline).
- Reinstalar sistemas comprometidos si es necesario.
- Verificar integridad de los archivos y la infraestructura después de la restauración.
- Implementar medidas adicionales para evitar futuros ataques (ejemplo: Zero Trust, segmentación de red).
- Monitorear el sistema restaurado para detectar posibles reinfecciones o actividad sospechosa.

Consideraciones:

- Los backups deben ser **pruebas de que no contienen malware** antes de restaurar.
- Validar accesos y permisos para evitar una nueva intrusión.
- Documentar todo el proceso como parte del **Plan de Respuesta a Incidentes**.
- **Sistema de Gestión de Seguridad de la Información (SGSI) - Basado en ISO 27001**

El **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en **ISO/IEC 27001** es un conjunto de políticas y procedimientos para gestionar de forma segura los activos de información dentro de una organización. Esta norma internacional establece los requisitos para implementar un **SGSI** efectivo y garantizar que la seguridad de la información se mantenga de manera continua.

¿Qué es ISO/IEC 27001?

La **ISO/IEC 27001** es una norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar de manera continua un **SGSI** dentro del contexto de los riesgos de seguridad de la información de la organización. Asegura que los procesos de seguridad sean gestionados de manera sistemática.

Objetivos del SGSI según ISO 27001

1. **Confidencialidad**: Asegurar que la información solo sea accesible por personas autorizadas.
2. **Integridad**: Garantizar que la información sea precisa y completa, y que no se altere sin autorización.
3. **Disponibilidad**: Asegurar que la información esté disponible cuando se necesite.
4. **olítica de seguridad de la información**:
   Documento que establece la dirección y el enfoque para gestionar la seguridad de la información.
5. **Evaluación de riesgos**:
   Identificación, análisis y evaluación de los riesgos que afectan a la confidencialidad, integridad y disponibilidad de la información. Se realiza para determinar las medidas de control necesarias.
6. **Control de acceso**:
   Definir quién puede acceder a qué información y bajo qué condiciones.
7. **Gestión de incidentes de seguridad de la información**:
   Establecer procedimientos para identificar, gestionar y responder a incidentes de seguridad.
8. **Cumplimiento normativo y legal**:
   Asegurarse de que el SGSI cumpla con leyes y regulaciones pertinentes, como GDPR, PCI-DSS, etc.

9. **Control de comunicaciones y operaciones**:
   Asegurar que los procesos de transmisión y almacenamiento de datos sean seguros y estén protegidos.
10. **Gestión de la continuidad del negocio**:
    Preparar planes para la recuperación ante desastres y la continuidad de las operaciones en caso de incidentes.
11. **Mejora continua**:
    Realizar auditorías internas y revisiones periódicas para asegurar que el SGSI evolucione y mejore constantemente.

Fases de implementación de un SGSI basado en ISO 27001 COMO SI FUERA NUESTRA EMPRESA

1. Planificación:
   - Definir los objetivos y el alcance del SGSI.
   - Establecer una política de seguridad de la información.
   - Identificar los activos de información y su valor para la organización.
2. Identificación de riesgos:
   - Realizar un análisis de riesgos para identificar amenazas y vulnerabilidades.
   - Evaluar el impacto y la probabilidad de los riesgos.
3. Implementación de controles:
   - Elegir e implementar controles de seguridad de acuerdo con los resultados del análisis de riesgos (por ejemplo, cifrado de datos, políticas de contraseñas, etc.).
4. Monitoreo y revisión:
   - Supervisar el desempeño del SGSI para asegurarse de que los controles estén funcionando correctamente.

    - Realizar auditorías y revisiones internas periódicas.
5. Mejora continua:
    - Evaluar y ajustar el SGSI para asegurar su efectividad y adaptabilidad a nuevos riesgos y amenazas.

Beneficios de implementar un SGSI basado en ISO 27001

- **Gestión de riesgos de seguridad**: Permite identificar, evaluar y mitigar riesgos relacionados con la seguridad de la información.
- **Cumplimiento de regulaciones**: Asegura el cumplimiento con normativas y regulaciones internacionales, lo que es crucial para evitar sanciones.
- **Confianza en clientes y socios**: La certificación ISO 27001 muestra el compromiso con la seguridad de la información, aumentando la confianza de los clientes.
- **Mejora continua**: El proceso de revisión y mejora garantiza que el SGSI evolucione y se adapte a nuevas amenazas.
- **Protección de la reputación**: Evita incidentes que puedan dañar la imagen de la empresa, como filtraciones de datos o ataques cibernéticos.