Plan Respuesta a Incidentes(PRI)

Francisco Félix Rodríguez Pellicer

Índice

1. Introducción

Este documento se describe el Plan de Respuesta a Incidentes (PRI) basado en el NIST y su integración dentro de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001. Además, se incorporan políticas y controles de Prevención de Pérdida de Datos (DLP) para mitigar el riesgo de fuga de información.

2. Objetivos

- Establecer un proceso eficaz para la gestión de incidentes de seguridad.

- Garantizar la continuidad del negocio y la integridad de la información.

- Prevenir y mitigar fugas de datos mediante políticas de Prevencion de perdida de datos DLP.

- Cumplir con los requisitos de la norma ISO 27001.

3. Alcance

Este plan se aplica a toda la infraestructura tecnológica, sistemas de información, personal y procesos relacionados con el tratamiento de información confidencial dentro de la organización.

4. Ciclo de Vida del Plan de Respuesta a Incidentes (NIST)

4.1. Preparación

- Formación del Equipo de Respuesta a Incidentes (CSIRT).

- Establecimiento de roles y responsabilidades.

- Herramientas de monitoreo y detección (IDS/IPS, SIEM).

- Simulacros regulares.

4.2. Detección y Análisis

- Identificación temprana de indicadores de compromiso (IoC).

- Clasificación de incidentes (fuga de datos, malware, DoS, etc.).

- Recopilación de evidencias digitales.

4.3. Contención, Erradicación y Recuperación

- Contención: Inmediata y a largo plazo (aislamiento de sistemas).

- Erradicación: Eliminación de malware, vulnerabilidades.

- Recuperación: Restauración de servicios seguros.

4.4. Actividades Post-Incidente

- Análisis forense y lecciones aprendidas.

- Actualización de procedimientos y controles.

- Informe a dirección y partes interesadas.

5. Sistema de Gestión de Seguridad de la Información (SGSI)

5.1. Contexto de la Organización

Identificación de activos críticos, partes interesadas, requisitos legales y riesgos de seguridad.

5.2. Política de Seguridad

Definición del compromiso organizacional con la seguridad de la información y el cumplimiento de ISO 27001.

5.3. Análisis de Riesgos

Evaluación y tratamiento del riesgo siguiendo la metodología ISO 27005 o similar.

6. Prevención de Pérdida de Datos (DLP)

6.1. Políticas de DLP

- Clasificación de la información.

- Restricciones de copia, envío y almacenamiento externo de datos sensibles.

- Reglas para transferencias por correo, USB o nube.

6.2. Herramientas de DLP

- Soluciones DLP a nivel de endpoint, red y nube.

- Integración con SIEM para correlación de eventos.

6.3. Medidas complementarias

- Cifrado de información confidencial.

- Control de acceso basado en el principio de mínimo privilegio.

- Capacitación continua al personal sobre fugas de datos.

7. Mejora Continua

El SGSI y el PRI deben someterse a una mejora continua basada en el ciclo PDCA (Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar)):

- Plan: Evaluación de riesgos y planificación de controles.

- Do: Implementación del SGSI y políticas DLP.

- Check: Auditorías internas y revisión de incidentes.

- Act: Corrección y mejora de procesos.

8. Roles y Responsabilidades

- CISO: Lidera el SGSI y el PRI.

- CSIRT: Detecta, responde y documenta incidentes.

- Usuarios: Reportan incidentes y cumplen con políticas.

9. Conclusión

Este plan proporciona un enfoque estructurado para gestionar incidentes de seguridad de forma eficaz y reducir los riesgos relacionados con la fuga de datos, alineando los procesos de seguridad con las mejores prácticas internacionales.