

Plan de Recuperación de Incidentes



Nombre: Gerardo Ernesto Aguilar López

Garantía de continuidad de los servicios críticos

1. Introducción

Este Plan de Recuperación de Incidentes tiene como finalidad garantizar la continuidad de los servicios críticos de la organización ante un incidente de seguridad, fallo técnico o compromiso del sistema. El plan se basa en el análisis previo realizado sobre el servidor Debian GNU/Linux, en el cual se identificaron riesgos de seguridad y se aplicaron medidas correctivas.

El enfoque adoptado combina buenas prácticas de la industria en gestión de incidentes, tomando como referencia el marco **NIST SP 800-61**, junto con los principios de un **Sistema de Gestión de Seguridad de la Información (SGSI)** conforme a la norma **ISO/IEC 27001**, incorporando además medidas orientadas a la **Prevención de Pérdida de Datos (DLP)**.

2. Objetivos del plan de recuperación

Los principales objetivos de este plan son:

- Restablecer los servicios críticos en el menor tiempo posible.
- Minimizar el impacto operativo y de seguridad tras un incidente.
- Proteger la información sensible y los activos del sistema.
- Evitar la repetición de incidentes similares en el futuro.
- Garantizar una recuperación controlada y documentada.

3. Identificación de servicios críticos

A partir del análisis del sistema, se identificaron los siguientes servicios como críticos para la operación:

- **Servidor web (Apache)**: servicio esencial para la disponibilidad de la aplicación web.
- **Base de datos (MariaDB/MySQL)**: almacena información sensible necesaria para el funcionamiento del sistema.
- **Acceso remoto (SSH)**: utilizado para la administración y recuperación del servidor.
- **Sistema de archivos y configuraciones críticas**: especialmente archivos de configuración del servidor web y la base de datos.

La indisponibilidad o compromiso de cualquiera de estos componentes afecta directamente a la continuidad del servicio.

4. Marco de respuesta a incidentes (NIST SP 800-61)

El proceso de recuperación se estructura siguiendo estas fases.

1 Identificación

- Detección de comportamientos anómalos mediante revisión de logs.
- Identificación de servicios afectados.
- Análisis de alertas generadas por herramientas de seguridad.
- Confirmación del alcance del incidente.

2 Contención

- Aislamiento del servicio o componente comprometido.
- Bloqueo temporal de accesos sospechosos.
- Restricción del tráfico mediante firewall.
- Cambio preventivo de credenciales si es necesario.

El objetivo de esta fase es evitar que el incidente se propague o empeore.

3 Erradicación

- Eliminación de configuraciones inseguras.
- Desinstalación o desactivación de servicios innecesarios.
- Corrección de permisos en archivos sensibles.
- Eliminación de posibles backdoors o procesos no autorizados.

4 Recuperación

- Restauración de los servicios críticos desde un estado seguro.
- Verificación de la integridad del sistema tras la recuperación.
- Reinicio controlado de servicios.
- Monitorización intensiva tras la puesta en producción.

5 Lecciones aprendidas

- Documentación del incidente y de las acciones realizadas.
- Evaluación de la efectividad del plan de recuperación.
- Actualización de controles y procedimientos de seguridad.
- Mejora continua del sistema y del plan.

5. Recuperación por servicio crítico

1 Servidor web (Apache)

- Verificar la configuración del servidor web.
- Restaurar archivos desde copias de seguridad confiables si fuese necesario.
- Confirmar que no se permite el listado de directorios.
- Revisar permisos de archivos y carpetas del sitio.
- Validar el correcto funcionamiento del servicio tras la recuperación.

2 Base de datos (MariaDB/MySQL)

- Verificar la disponibilidad e integridad de la base de datos.
- Restaurar respaldos en caso de corrupción o pérdida de datos.
- Cambiar credenciales si existe sospecha de acceso no autorizado.
- Confirmar que el servicio solo esté accesible localmente.

3 Acceso remoto (SSH)

- Revisar los registros de autenticación.
- Limitar el acceso remoto a usuarios autorizados.
- Evitar accesos directos como root.
- Aplicar políticas de contraseñas seguras o autenticación reforzada.

6. Copias de seguridad y restauración

Las copias de seguridad son un elemento clave del plan de recuperación:

- Realizar respaldos periódicos de la base de datos y archivos del sitio web.
- Verificar la integridad de los respaldos.
- Almacenar copias en ubicaciones separadas.
- Restaurar únicamente desde copias verificadas como seguras.

7. Prevención de Pérdida de Datos (DLP)

Como parte del plan de recuperación y del SGSI, se incorporan medidas básicas de **Prevención de Pérdida de Datos (DLP)**, orientadas a proteger la información sensible frente a accesos no autorizados o fugas accidentales.

Estas medidas incluyen:

- Restricción de permisos en archivos que contienen información crítica.
- Control de accesos a la base de datos.
- Segmentación de servicios para reducir la exposición de datos.
- Uso de firewall para limitar la comunicación innecesaria.
- Monitorización de accesos mediante análisis de logs.

Estas acciones permiten reducir el riesgo de fuga de información durante y después de un incidente.

8. Integración con un SGSI (ISO/IEC 27001)

El plan de recuperación forma parte de un enfoque más amplio de gestión de la seguridad de la información basado en ISO/IEC 27001, que contempla:

- Identificación y gestión de riesgos.
- Definición de políticas de seguridad.
- Aplicación de controles técnicos y organizativos.

- Evaluación periódica de la seguridad.
- Mejora continua del sistema.

9. Validación posterior a la recuperación

Una vez finalizado el proceso de recuperación:

- Se validará el estado de los servicios críticos.
- Se revisarán logs recientes para detectar anomalías.
- Se realizará un escaneo básico del sistema.
- Se confirmará que no existan servicios innecesarios activos.

10. Comunicación y documentación

Tras cada incidente:

- Se documentará el evento y las acciones realizadas.
- Se informará a los responsables técnicos.
- Se actualizará el plan de recuperación si es necesario.
- Se conservará la documentación para futuras auditorías.

11. Mejora continua

El plan de recuperación debe revisarse de forma periódica y tras cada incidente relevante, adaptándose a nuevas amenazas, cambios en la infraestructura y lecciones aprendidas, garantizando así la continuidad y seguridad del sistema a largo plazo.

12. Conclusión

La aplicación de este Plan de Recuperación de Incidentes permite a la organización responder de forma estructurada y eficaz ante incidentes de seguridad, garantizando la continuidad de los servicios críticos, protegiendo la información sensible y reforzando la postura de seguridad del sistema mediante buenas prácticas alineadas con NIST, ISO 27001 y principios básicos de DLP.