PLAN DE RECUPERACIÓN ANTE INCIDENTES Y CONTINUIDAD DE SERVICIOS

1. Introducción

Este plan establece las acciones necesarias para recuperar los servicios críticos en caso de un incidente de seguridad en un entorno Debian comprometido, como el analizado en el proyecto final de ciberseguridad. Su propósito es minimizar el impacto en la disponibilidad, integridad y confidencialidad de los activos digitales, garantizando la continuidad operativa de la organización.

2. Servicios Críticos Identificados

- Servidor Web (Apache + WordPress): portal principal de gestión de contenido.
- Base de Datos MySQL: almacena credenciales, configuraciones y contenido del sitio.
- Servicio SSH: acceso administrativo al servidor.
- Servicio de Backups: recuperación ante pérdida de datos.
- Herramientas de monitoreo (Wazuh): vigilancia de seguridad en tiempo real.

3. Estrategia de Recuperación

La estrategia de recuperación se basa en la priorización de servicios, uso de respaldos confiables y documentación precisa para garantizar una restauración ordenada.

3.1 Prioridades de Restauración

1. Restauración del servidor de base de datos.
2. Recuperación del servicio web y configuración de WordPress.
3. Reestablecimiento del acceso administrativo mediante SSH.
4. Verificación del monitoreo y alertas de seguridad.
5. Validación del sistema completo con pruebas funcionales y de seguridad.

3.2 Procedimiento de Recuperación

- Aislar el servidor afectado de la red.
- Validar el incidente mediante revisión de logs y alertas.
- Restaurar desde el backup más reciente (verificado).

- Reaplicar configuraciones de hardening y reglas de firewall.
- Revalidar los accesos y cambiar todas las contraseñas.
- Activar monitoreo post-restauración por 72 horas.
- Documentar el proceso y notificar a las partes interesadas.

4. Medidas de Continuidad

- Implementación de backups automáticos bajo la regla 3-2-1.
- Documentación de procedimientos y configuraciones críticas.
- Replicación del servidor en un entorno de contingencia (staging).
- Pruebas mensuales de restauración para asegurar integridad de respaldos.
- Establecer tiempos máximos de recuperación (RTO) y pérdida aceptable de datos (RPO).

- Después de mitigaciones (SGSI, hardening, monitorización activa): ≥ 90 días estimados

- Antes de mitigaciones: Incidentes cada 15-30 días (por mala configuración, vulnerabilidades sin parches)

4.1 Análisis de Impacto al Negocio y Parametros de Recuperacion

RTO – Recovery Time Objective (Objetivo de Tiempo de Recuperación)

Definición: Tiempo máximo permitido para restaurar un servicio afectado tras un incidente de seguridad.

- **Servicio Web (Apache + WordPress):** 4 horas
- **Base de Datos MySQL:** 2 horas
- **Acceso SSH seguro:** 3 horas
- **Servicio de monitoreo (Wazuh):** 6 horas
- **FTP (en transición a SFTP):** 6 horas (limitado a entornos internos)

Justificación: El impacto crítico de estos servicios sobre la disponibilidad y recuperación de datos requiere tiempos breves de restauración, priorizando el backend y el control administrativo del sistema.

RPO – Recovery Point Objective (Objetivo de Punto de Recuperación)

Definición: Cantidad máxima de datos que pueden perderse, medida en tiempo.

- **Servicio web y base de datos:** No más de 2 horas de pérdida de datos gracias a backups frecuentes.
- **Configuraciones críticas (wp-config.php, SSH, FTP):** Revisión cada 12 horas mediante copias cifradas.
- **Logs de seguridad y auditoría:** Sincronización cada 15 minutos con el SIEM.

Justificación: El entorno requiere respaldos regulares y automatizados siguiendo la política 3-2-1 para garantizar un punto de restauración reciente y consistente.

MTTR – Mean Time to Recovery (Tiempo Medio de Recuperación)

Definición: Tiempo promedio necesario para recuperar completamente un sistema tras una falla.

- **Estimación general para Debian + Apache + MySQL:** 3 horas
- **Escenarios simulados con restauración de backups verificados:** 2h 45m en promedio
- **Recuperación tras detección de rootkits o shells maliciosos:** 4 horas

Justificación: Basado en pruebas controladas durante el ejercicio, incluyendo restauración y endurecimiento post-compromiso.

MTBF – Mean Time Between Failures (Tiempo Medio Entre Fallos)

Definición: Tiempo promedio entre dos incidentes graves o interrupciones del servicio.

- **Antes de mitigaciones:** Incidentes cada 15-30 días (por mala configuración, vulnerabilidades sin parches)
- **Después de mitigaciones (SGSI, hardening, monitorización activa): ≥ 90 días estimados**

Justificación: El fortalecimiento de políticas de seguridad, junto con Wazuh, hardening de servicios y eliminación de accesos inseguros, reduce significativamente la probabilidad de fallo recurrente.

5. Conclusión

Un plan de recuperación bien definido permite a la organización responder con eficacia ante incidentes graves de seguridad, restaurando la operación de los servicios esenciales sin comprometer los datos ni la confianza de los usuarios. Este plan debe integrarse como parte del SGSI y actualizarse periódicamente mediante simulacros y auditorías técnicas.