# Plan de recuperación en caso de incidencia

## 1. Objetivos y alcance

### Objetivo general:

Restablecer lo antes posible los servicios afectados (WordPress, FTP, SSH, bases de datos) en un estado seguro y consistente, minimizando tiempo de inactividad y pérdida de datos.

### Alcance:

– Servidor Debian con Apache, MariaDB, vsftpd y WordPress.

– Directorios web.

– Cuentas y permisos de sistema y base de datos.

– Políticas de contraseñas y acceso remoto.

## 2. Funciones y actividades

### 1.- Identificar:

- Monitorizar logs de sistemas, aplicaciones y redes.
- Detectar anomalías (SUDO, escaneos).
- Clasificar la severidad del incidente (alto, medio, bajo).

### 2.- Contener:

- Aislar inmediatamente el servidor/servicio comprometido (corte de red, ACLs, desconectar físicamente de la red).
- Implementar bloqueos temporales (fail2ban, firewall).

- Guardar evidencia (volcado de RAM, procesos activos, conexiones de red, usuarios conectados, copia del disco duro, logs).

### 3.- Erradicar:

- Eliminar malware, procesos o usuarios maliciosos detectados.
- Eliminar y modificar credenciales comprometidas.
- Aplicar parches, actualizaciones y correcciones de configuración.

### 4.- Recuperar:

- Restaurar sistemas desde backups limpios.
- Validar integridad y funcionalidad.
- Reabrir servicios controlados y monitorizar comportamiento constantemente.

# 3. Flujo de respuesta ante un ataque similar

### Detección y alerta

- Un usuario sin privilegios intenta ejecutar comandos sudo y los logs de Apache muestran acceso a /wp-content/uploads.
- El SIEM detecta las actividad anómalas y lanza una alerta.

### Identificación y clasificación

- Evaluar el alcance: ¿qué servicios se vieron comprometidos? ¿se vieron comprometidos archivos o usuarios? ¿se vieron involucrados varios servidores o equipos? ¿qué redes o subredes están involucradas? ¿hubo escalación de privilegios (ya sea lateral o vertical)? ¿hubo ejecución de código? ¿se instalaron nuevos servicios o se crearon nuevos archivos?
- Clasificar el riesgo de acuerdo a la respuestas anteriores en las siguientes categorías:
    - Crítico.
    - Alto.
    - Medio.
    - Bajo.

## Contención rápida

- Desconectar interfaces no críticas.
- Aplicar reglas firewall que bloqueen el tráfico externo.
- Desactivar temporalmente FTP y SSH.

## Recolección de evidencia

- Hacer volcado de información para el análisis forense (discos duros), extraer datos RAM, procesos activos, conexiones de red, usuarios conectados.
- Copiar archivos modificados.

## Erradicación

- Eliminar usuarios maliciosos creados o comprometidos.
- Limpiar shells PHP.
- Desactivar indexación.
- Aplicar parches y actualizar wordPress y apache.

## Recuperación

- Restaurar base de datos con respaldo pre-incidente.
- Restablecer archivos web desde backup limpio.
- Rehabilitar servicios: Apache, MySQL, SSH, vsftpd, etc.

# 4. Prevención y control de recurrencia de indcidentes

| Vector de Ataque | Medida Preventiva |
|---|---|
| **Escalación vía sudo** | – Revisar /etc/sudoers, dar privilegios mínimos a los usuarios.<br>– Auditar comandos sudo con alertas automatizadas. |
| **Contraseñas débiles** | – Políticas de contraseñas con más de 12 caracteres con validate_password (MySQL) y pwquality.conf (sistema). |
| **Indexación web** | – Desactivar options -Indexes en Apache. |
| **Escaneos automatizados** | – Implementar WAF y reglas contra usuarios maliciosos. |

# 5. Mecanismos de protección de datos

### Respaldos periódicos

- **Base de datos**: mysqldump diario.
- **Archivos de aplicación**: copia diaria.
- **Almacenamiento Off-site**: nube o dispositivo de almacenamiento externo cifrado.

### Cifrado de datos sensibles

- **Datos en reposo**: discos duros de respaldo cifrados.
- **Datos en tránsito**: SFTP en lugar de FTP, SSH en lugar de Telnet.

### Controles de acceso

- **SSH**: autenticación por llave pública, bloqueo de root, 2FA.
- **FTP**: acceso a usuarios explícitos con TLS.

- **MySQL**: usuarios con privilegios mínimos, cifrado de conexiones (SSL).