Plan de Respuesta a Incidentes y Marco de SGSI (ISO 27001)

Índice (Tabla de Contenido)

Introducción

El objetivo de este documento es establecer un marco de seguridad proactivo después de un incidente crítico. Detalla un **Plan de Respuesta a Incidentes (PRI)** basado en la guía NIST SP 800-61 y establece las bases para implementar un **Sistema de Gestión de Seguridad de la Información (SGSI)** conforme a la norma ISO 27001.

1. Plan de Respuesta a Incidentes (PRI) - Guía NIST SP 800-61

Este plan describe los procedimientos que la organización seguirá para gestionar un ataque similar al acceso no autorizado por SSH y la escalada de privilegios a root.

Etapa A: Preparación

Antes de que ocurra un incidente:

Acción	Propósito
Documentación	Mantener listas de contactos de emergencia, diagramas de red y procedimientos de *hardening* actualizados.
Monitoreo	Implementar un Sistema de Información y Gestión de Eventos de Seguridad (SIEM) y configurar alertas para inicios de sesión fallidos o actividades de escalada de privilegios (uso de sudo).
Copias de Seguridad	Realizar respaldos automáticos y probados de datos críticos (BBDD de WordPress, archivos de configuración) con regularidad.

Etapa B: Detección y Análisis

Una vez detectada la actividad anómala (ej., un inicio de sesión SSH no reconocido o un cambio de permisos):

Acción	Propósito
Detección	Identificar la hora, el origen (IP) y el vector de ataque (puerto 22) mediante el análisis de logs (/var/log/auth.log y logs de Apache).
Análisis	Determinar el alcance del compromiso: ¿Se accedió solo al usuario debian? ¿Se escalaron privilegios a root? ¿Se instaló *malware* o *backdoors*?

Etapa C: Contención, Erradicación y Recuperación (El Corazón de la Respuesta)

Contención (Aislamiento inmediato)

El objetivo es detener el ataque antes de que cause más daño.

- **Aislamiento de Red:** Ejecutar temporalmente la regla de *firewall* más restrictiva, cerrando todo acceso externo (incluyendo el puerto 80) para aislar el servidor.
  - *Acción Rápida:* iptables -P INPUT DROP
- **Contención SSH:** Deshabilitar inmediatamente la autenticación por contraseña si se sospecha de *brute force*, o cambiar la contraseña del usuario comprometido (passwd debian).

Erradicación (Limpieza del Sistema)

Eliminar la causa raíz y cualquier herramienta dejada por el atacante.

- **Eliminación del Vector:** Cambiar todas las contraseñas comprometidas (SSH, bases de datos, WordPress).
- **Limpieza de Backdoors:** Revisar los archivos de persistencia comunes (/etc/crontab, archivos de inicio de usuario, .bashrc, claves SSH en /root/.ssh/authorized_keys) y eliminar cualquier clave o código malicioso.
- **Auditoría de Logs:** Verificar que no haya otros usuarios o servicios comprometidos.

Recuperación (Restauración del Servicio)

Restaurar la funcionalidad normal, asegurando que el sistema sea seguro.

- **Restauración:** Si el compromiso es severo, restaurar el sistema operativo y la aplicación (WordPress) desde la **última copia de seguridad segura** antes del incidente.
- **Hardening Final:** Aplicar las reglas de iptables desarrolladas en la Fase 2 para el endurecimiento y auditoría de permisos de archivos sensibles (ej., wp-config.php).
  - **Reglas de Firewall Aplicadas:**

```
# Limpia todas las reglas existentes y las cadenas personalizadas
iptables -F
iptables -X
# Establece la política por defecto en DROP para tráfico entrante (Cierra todo)
iptables -P INPUT DROP
# Permite el tráfico de conexiones ya establecidas y relacionadas
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Permite el tráfico en la interfaz de loopback (lo)
iptables -A INPUT -i lo -j ACCEPT
# Abre solo el puerto 80 (HTTP) para el servicio web de WordPress
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
# Hacer las reglas permanentes (se debe usar un servicio como iptables-persistent para persistencia)
```

Etapa D: Actividades Post-Incidente

Cerrar el ciclo de respuesta para mejorar la seguridad futura.

- **Lecciones Aprendidas:** Documentar qué falló (ej., credenciales débiles, falta de monitoreo) y qué se puede mejorar.
- **Revisión del SGSI:** Actualizar las políticas y el análisis de riesgos basados en la experiencia del ataque.

2. Plan de Recuperación de Servicios Críticos

Detalle de los procedimientos para restablecer la operatividad de los dos servicios principales tras el incidente.

Servicio Crítico A: Acceso SSH (Administración)

Procedimiento	Detalle
1. Verificación de Integridad	Comprobar que el dominio SSH (sshd) no haya sido modificado por el atacante.
2. Restablecimiento de Credenciales	Restablecer las contraseñas del sistema (incluyendo root y usuarios administrativos) con credenciales de alta complejidad.
3. Implementación de Clave Pública	Configurar SSH para que *solo* permita la autenticación con clave pública para los administradores, deshabilitando la autenticación por contraseña (PasswordAuthentication no) para prevenir futuros ataques de fuerza bruta.

Servicio Crítico B: Servidor Web Apache/WordPress (Negocio)

Procedimiento	Detalle
1. Restauración de la Aplicación	Restaurar la base de datos y los archivos de WordPress desde una copia de seguridad limpia y validada (especialmente el directorio de *uploads* y el archivo wp-config.php).
2. Escaneo de Integridad	Utilizar herramientas de escaneo de integridad de archivos para detectar

	malware o *webshells* ocultas en el código de WordPress.
3. Activación del Firewall	Habilitar el puerto 80/TCP en iptables **solo después** de haber asegurado el servidor y cambiado todas las credenciales internas de WordPress.

3. Mecanismos de Protección de Datos y Controles de Acceso

3.1. Respaldo (Backup) de Datos

Se implementará una política de respaldo siguiendo la regla 3-2-1:

- **Frecuencia:** Copia de seguridad diaria de la base de datos y semanal de la imagen completa del servidor.
- **Almacenamiento (3-2-1): 3** copias de datos, en **2** tipos de medios diferentes, con **1** copia almacenada fuera del sitio (*off-site*).
- **Pruebas:** Se realizarán pruebas trimestrales de restauración para asegurar la integridad de las copias.

3.2. Cifrado de Datos Sensibles

Dato a Cifrar	Riesgo Mitigado	Método Sugerido
Contraseñas de la Base de Datos	Exposición de credenciales de conexión si wp-config.php es accedido.	Restringir permisos de wp-config.php a chmod 600.
Tráfico SSH	Ataques *Man-in-the-Middle* para robar credenciales.	El cifrado nativo de SSH (Protocolo 2) ya mitiga este riesgo, pero la clave pública debe protegerse con *passphrase*.

3.3. Controles de Acceso Estrictos (Principio de Mínimo Privilegio)

- **Usuarios del Sistema:** Se eliminarán los permisos de sudo para cualquier usuario que no sea esencial para la administración del sistema (como el usuario debian).
- **Permisos de Archivos:** Se revisarán periódicamente los permisos de los archivos de

configuración críticos, asegurando que solo el usuario propietario (generalmente root o el usuario del servicio como www-data) tenga acceso de lectura y escritura.

4. SGSI (ISO 27001)

Para cumplir con los requisitos de la **ISO 27001** (Estándar internacional para establecer, implementar, mantener y mejorar un **Sistema de Gestión de Seguridad de la Información**

$$SGSI$$
), la organización debe formalizar los siguientes puntos, basándose en el incidente ocurrido.

4.1. Análisis de Riesgos

Riesgo Identificado	Impacto	Probabilidad	Nivel de Riesgo
Acceso no Autorizado a Root (Vía credenciales débiles y sudo sin restricción)	Pérdida total de la confidencialidad, integridad y disponibilidad del sistema.	Alta (dada la simpleza de la explotación)	**Crítico**
Compromiso de la Red Interna (LAN) (Vía la Topología de Estrella sin DMZ)	El atacante puede **pivotar** del Servidor Web a las PCs de administración o al Servidor SIEM.	Servidor Web a las PCs de administración o al Servidor SIEM.Alta (si no se implementa la DMZ)	**Crítico**
Fuga de Información (C2 Activo) (Vía el canal de Mando y Control y *backdoors*)	Exfiltración de datos sensibles de la base de datos (DB) (como credenciales de clientes), pérdida de propiedad intelectual.	Media (confirmado por conexión UDP saliente)	**Alto**
Pérdida de Integridad del Sitio Web (Vía modificación	Daño a la reputación, inyección de código malicioso a	Media (corregida, pero el riesgo existe si no se mantiene)	**Alto**

remota de `wp-config.php`)	visitantes, pérdida de confianza del cliente.		
Ataque de Denegación de Servicio (DoS/DDoS)	Interrupción del Servicio Web (negocio), indisponibilidad del servicio de administración (SSH).	Media (dada la exposición del servicio HTTP)	**Alto**

4.2. Políticas de Seguridad

Se requiere un conjunto de políticas que cubran el control de acceso lógico, el endurecimiento de sistemas y la seguridad física básica, conforme a los dominios de ISO 27001.

A. Políticas Lógicas y de Sistemas

Política	Detalle de la Medida	Referencia ISO 27001
Política de Contraseñas Robustas	Todos los usuarios deben usar contraseñas de **mínimo 12 caracteres**, incluyendo complejidad (mayúsculas, minúsculas, números, símbolos) y rotación trimestral (90 días).	A.9.2.1
Política de Control de Acceso Remoto (SSH)	El acceso al servidor SSH debe estar restringido a **claves públicas y el uso de un *jump box*** (PC de Administración). La autenticación por contraseña debe ser deshabilitada (PasswordAuthentication no) de forma permanente.	A.9.2.5

Política de Endurecimiento de Sistemas (Hardening)	Se debe aplicar el **Principio de Mínimo Privilegio** a todos los hosts. Esto incluye una política de **Denegación Explícita** en el Firewall e iptables, cerrando todos los puertos excepto los esenciales (80/443, 22 restringido).	A.12.6.2
Política de Copias de Seguridad (Backup)	Se debe asegurar un respaldo automatizado y diario de los datos críticos (Base de Datos y archivos de WordPress). Las copias de seguridad deben ser almacenadas en una **ubicación externa** a la red LAN (según la regla 3-2-1).	A.12.3.1
Política de Auditoría de Privilegios (sudo)	Se prohíbe el uso de comandos como sudo su que permiten la escalada total. Se debe implementar la **restricción por comando** en /etc/sudoers para permitir solo las acciones mínimas necesarias.	A.9.2.3

B. Políticas de Seguridad Física

Política	Detalle de la Medida	Referencia ISO 27001
Política de Acceso Físico al Centro de Datos	El acceso físico al servidor y al Firewall debe estar restringido mediante **control de acceso**	A.11.1.2

	biométrico o por llave, limitando la entrada solo al personal autorizado de TI.	
Política de Protección de Cableado	El cableado de red (tanto el de la LAN interna como el de la DMZ) debe ser protegido contra intercepciones o daños accidentales, utilizando canaletas cerradas y etiquetado claro.	A.11.2.3
Política de Despliegue de Equipos	Los equipos (servidores, Firewall, Switch) deben estar físicamente resguardados en un *rack* con llave y ubicados lejos de áreas de tránsito público para prevenir manipulación no autorizada.	A.11.2.1

4.3. Plan de Acción (Acciones Futuras de Protección)

Acción	Responsable	Prioridad
Implementar Monitoreo Activo (SIEM)	Departamento de TI	Alta
Deshabilitar la autenticación por contraseña en SSH	Administrador de Servidores	Alta
Auditoría de Permisos (chmod/chown)	Administrador de Seguridad	Media
Realizar Pentesting Periódico	Consultor Externo	Media