Fecha: 08 de febrero de 2026
Analista Responsable: Sergio Maturana

PLAN DE RESPUESTA A INCIDENTES Y CERTIFICACIÓN

(SGSI)

Sergio Maturana Mena

1 INTRODUCCIÓN

Tras las fases técnicas de saneamiento y auditoría, la Fase 3 se centra en la gobernanza de la seguridad. El objetivo es establecer un marco estratégico que permita a la organización reaccionar con eficacia ante incidentes y gestionar la seguridad de la información bajo estándares internacionales.

2 PLAN DE RESPUESTA A INCIDENTES (NIST SP 800-61)

Se define un ciclo de vida de respuesta estructurado para minimizar el impacto de futuros ataques:

2.1 Preparación

Inventario: Mantenimiento actualizado de activos (Servidor Debian, Aplicación WordPress).

Seguridad por diseño: Implementación de herramientas de monitoreo como Fail2Ban para bloquear IPs tras varios intentos fallidos de login.

Formación: Capacitación del personal en la identificación de vectores de ataque comunes (Phishing, Fuerza Bruta).

2.2 Detección y Análisis

Monitoreo de Logs: Revisión automatizada de /var/log/apache2/access.log para detectar patrones de enumeración de usuarios.

Indicadores de Compromiso (IoC): Alertas configuradas para detectar picos de tráfico hacia el endpoint /wp-json/wp/v2/users.

2.3 Contención, Erradicación y Recuperación

Contención: Bloqueo inmediato en el Firewall (UFW) de la dirección IP de origen. En caso de compromiso masivo, aislamiento del servidor de la red.

Erradicación: Identificación de la brecha (ej. falta de reglas en .htaccess) y aplicación de parches de seguridad.

Recuperación: Validación de la integridad del sistema y restauración de servicios desde copias de seguridad si se detectó manipulación de archivos.

2.4 Actividad Post-Incidente

Realización de un informe de "Lecciones Aprendidas" para actualizar las políticas de seguridad y evitar la repetición del evento.

3 PROTOCOLO ANTE ATAQUES SIMILARES Y PREVENCIÓN

Para prevenir la recurrencia de ataques de enumeración y fuerza bruta (vistos en la Fase 2), se han establecido los siguientes controles:

Protección de la API: Denegación por defecto a consultas de usuarios no autenticados en WordPress.

MFA (Autenticación de Múltiples Factores): Obligatoriedad de un segundo factor para acceder al panel /wp-admin.

WAF (Web Application Firewall): Implementación de reglas que identifiquen y bloqueen escaneos de herramientas como Hydra o Nmap en tiempo real.

4 MECANISMOS DE PROTECCIÓN DE DATOS

Se documentan los controles implementados para asegurar la tríada de la seguridad (CIA):

- **Respaldos Periódicos**: Implementación de una política de backups automatizados semanales, almacenados en un servidor externo cifrado (Estrategia 3-2-1).
- **Cifrado de Datos**:
  - **En tránsito**: Uso de certificados SSL/TLS para cifrar el tráfico HTTP.
  - **En reposo**: Uso de crypt o herramientas similares para asegurar que las bases de datos no sean legibles en caso de robo físico o lógico del archivo.
- **Controles de Acceso Estrictos**: Aplicación del Principio de Mínimo Privilegio (PoLP). El acceso SSH está limitado únicamente a llaves criptográficas (sin contraseña) y el acceso Root está deshabilitado.

5 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISO 27001)

5.1 Análisis de Riesgos

Activo	**Amenaza**	**Impacto**	**Nivel de Riesgo**	**Plan de Acción**
Servidor Web	Fuerza Bruta	Alto	Crítico	Bloqueo de cuenta y limitación de intentos.
Datos de Usuario	Exfiltración	Muy Alto	Alto	Cifrado y restricción de API.
Configuración	Error Humano	Medio	Bajo	Uso de scripts de despliegue y auditoría.

5.2 Definición de Políticas de Seguridad

- Política de Gestión de Activos: Registro obligatorio de todo software instalado en el servidor Debian.
- Política de Control de Acceso: Revisión trimestral de los usuarios con permisos administrativos.

5.3 Plan de Acción y Mejora Continua

Se establece un ciclo PHVA (Planificar, Hacer, Verificar, Actuar):

- **Verificar**: Realización de escaneos de vulnerabilidades trimestrales.
- **Actuar**: Actualización inmediata de parches de seguridad tras la publicación de CVEs (Vulnerabilidades y Exposiciones Comunes).