FASE 3: PLAN DE RESPUESTA A INCIDENTES Y SGSI (ISO 27001)

1. PLAN DE RESPUESTA A INCIDENTES (Basado en NIST SP 800-61)

El plan sigue las cuatro fases del ciclo de vida de respuesta a incidentes establecido por el NIST SP 800-61: Preparación, Detección y Análisis, Contención/Erradicación/Recuperación, y Actividades Post-Incidente .

1.1 Preparación

Objetivo: Establecer las capacidades y recursos necesarios antes de que ocurra un incidente .

Acción	Descripción	Responsable	Basado en el caso
Equipo de respuesta (CSIRT)	Formar un equipo con roles definidos: coordinador, analista forense, comunicaciones, soporte técnico .	Dirección de TI	El caso mostró que no había un equipo definido; las acciones las realizó un solo usuario sin supervisión.
Inventario de activos	Mantener actualizado un inventario de hardware, software y datos críticos .	Administradores	No se tenía claro qué servicios eran críticos (FTP se instaló sin justificación).

Backups de sistemas críticos	Realizar copias de seguridad periódicas y almacenarlas en ubicaciones externas .	Administradores	No se mencionan backups en los logs; la recuperación dependería de reinstalaciones manuales.
Centralización de logs	Establecer un sistema de logging centralizado (rsyslog, SIEM) para preservar evidencias .	Área de ciberseguridad	Los logs estaban solo en el sistema local; si el atacante los borraba, se perdían.
Actualizaciones y parches	Aplicar parches de seguridad críticos en un máximo de 48 horas .	Administradores	El sistema estaba actualizado, pero las configuraciones inseguras fueron el problema real.
Política de contraseñas	Establecer requisitos de complejidad y rotación de contraseñas .	CISO	El caso evidenció que se usaron contraseñas (posiblemente débiles) para acceder como root.

1.2 Detección y Análisis

Objetivo: Identificar y confirmar incidentes, así como determinar su alcance e impacto .

Fuente de detección	Descripción	Aplicación al caso

Análisis de logs	Revisar logs de autenticación, servicios y aplicaciones .	Los logs de `sudo` y `sshd` fueron clave para detectar la instalación de servicios y la conexión root.
Monitoreo de integridad	Detectar cambios en archivos críticos (`/etc/ssh/sshd_config`) .	Se detectó la modificación de `sshd_config` para habilitar `PermitRootLogin`.
Alertas de nuevos servicios	Notificar cuando se instalan o activan servicios (FTP, SSH) .	La instalación de `vsftpd` y `openssh-server` debería haber generado alertas.
Cambios en permisos	Monitorear cambios masivos de permisos (`chmod 777`) .	El comando `chmod -R 777 /var/www/html` es una bandera roja evidente.

Procedimiento de análisis para casos similares:

1. Recolectar evidencias inmediatas: Logs de `journalctl`, historial de bash (`~/.bash_history`), y configuración de servicios .
2. Identificar la línea de tiempo: Ordenar eventos por fecha/hora para reconstruir la secuencia de acciones .
3. Determinar el alcance: Revisar qué otros sistemas pudieron verse afectados (ej. si se usaron las mismas credenciales).
4. Clasificar la gravedad: Usar matriz de impacto (funcional, información, recuperabilidad) .

Matriz de priorización:

Nivel	Descripción	Ejemplo
Alto	Compromiso de root, exposición de datos críticos	Conexión root por SSH, permisos 777 en wp-config.php
Medio	Servicios inseguros pero sin evidencia de abuso	FTP anónimo habilitado
Bajo	Malas prácticas sin impacto inmediato	Historial de comandos sin limpiar

1.3 Contención, Erradicación y Recuperación

1.3.1 Contención

Objetivo: Detener la propagación del ataque y limitar el daño .

Acción	Descripción	Tiempo estimado
Aislar el sistema	Desconectar de la red el servidor comprometido .	Inmediato
Bloquear IP maliciosa	Agregar regla en firewall para bloquear `192.168.0.134` .	5 minutos
Deshabilitar servicios innecesarios	Detener FTP si no es requerido: `sudo systemctl stop vsftpd`	5 minutos

Cambiar contraseñas	Rotar contraseñas de root y del usuario `debian` .	10 minutos
Revocar claves SSH	Eliminar claves autorizadas sospechosas .	5 minutos

1.3.2 Erradicación

Objetivo: Eliminar completamente la amenaza del sistema .

Acción	Descripción	Verificación
Revertir cambios maliciosos	Restaurar configuraciones originales: `PermitRootLogin no` en `/etc/ssh/sshd_config` .	`grep PermitRootLogin /etc/ssh/sshd_config`
Corregir permisos	Restablecer permisos seguros: `chmod -R 755 /var/www/html` y `chmod 600 wp-config.php`	`ls -la /var/www/html/wp-config.php`
Eliminar servicios no autorizados	Desinstalar vsftpd si no es necesario: `sudo apt remove vsftpd`	`systemctl status vsftpd`
Actualizar software	Aplicar parches de seguridad pendientes .	`apt update && apt upgrade -y`

1.3.3 Recuperación

Objetivo: Restaurar la operación normal del sistema de forma segura .

Acción	Descripción	Comprobación
Restaurar desde backup	Si hay daños mayores, restaurar desde copia limpia .	Verificar integridad del backup
Reconectar a la red	Una vez seguro, volver a conectar el sistema .	Monitorear tráfico
Monitoreo intensivo	Durante 48 horas, revisar logs en busca de reincidencias .	`journalctl -f`
Comunicar a usuarios	Informar sobre la restauración del servicio	Correo / Intranet

1.4 Actividades Post-Incidente

Objetivo: Mejorar el plan y prevenir futuros incidentes .

Acción	Descripción	Responsable
Reunión post-mortem	Analizar qué ocurrió, qué se hizo bien y qué se puede mejorar .	CSIRT + Dirección
Documentar lecciones aprendidas	Responder: ¿Qué información se necesitó antes? ¿Qué acciones fueron incorrectas? ¿Cómo prevenir?	Analista forense

Actualizar políticas	Reforzar políticas de contraseñas, accesos y actualizaciones .	CISO
Mejorar detección	Crear nuevas reglas de alerta para `chmod 777`, instalación de servicios, etc.	Área de ciberseguridad
Capacitación	Entrenar al personal en las lecciones aprendidas .	RRHH / TI

---

2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI - ISO 27001)

2.1 Alcance del SGSI

El SGSI cubre los activos críticos identificados en el análisis forense:

Activo	Descripción	Propietario	Riesgo identificado
Servidor Debian	Servidor web, base de datos, FTP, SSH	Administrador de sistemas	Configuraciones inseguras, acceso root
Aplicación WordPress	Sitio web corporativo	Equipo de desarrollo	Permisos 777 en wp-config.php

Base de datos MariaDB	Datos de usuarios y contenidos	DBA	Credenciales en texto plano en wp-config.php
Credenciales de acceso	Usuarios y contraseñas del sistema	CISO	Contraseñas débiles, root login habilitado
Logs del sistema	Registros de actividad	Área de ciberseguridad	No centralizados, riesgo de pérdida

2.2 Análisis de Riesgos (ISO 27005)

Basado en el incidente analizado, se identifican los siguientes riesgos :

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Riesgo	Tratamiento
Servidor	Acceso no autorizado	Contraseñas débiles	Alto	Alta	Crítico	Mitigar (política de contraseñas)
SSH	Acceso root	Root login habilitado	Alto	Alta	Crítico	Mitigar (deshabilitar)
FTP	Exfiltración de datos	Instalado sin necesidad	Medio	Media	Medio	Eliminar si no es necesario
WordPress	Modificación de sitio	Permisos 777 en archivos sensibles	Alto	Media	Alto	Mitigar (permisos 600/755)

Logs	Pérdida de evidencia	No centralizados	Medio	Media	Medio	Mitigar (logs remotos)
Configuración	Cambios no autorizados	Falta de control de cambios	Alto	Media	Alto	Implementar auditoría

2.3 Políticas de Seguridad

2.3.1 Política de Control de Accesos

- Principio de mínimo privilegio: Los usuarios solo tendrán los permisos necesarios para su función.
- Autenticación multifactor (MFA): Obligatoria para accesos administrativos (root, sudo).
- Revisión periódica de accesos: Cada 3 meses se revisarán y auditarán los permisos de todos los usuarios.
- Deshabilitar root login por SSH: Prohibido el acceso directo como root; usar `sudo` con usuarios regulares.

2.3.2 Política de Contraseñas

- Longitud mínima: 12 caracteres.
- Complejidad: mayúsculas, minúsculas, números y símbolos.
- Cambio obligatorio cada 90 días.
- Prohibido reutilizar las últimas 5 contraseñas.
- Almacenamiento con hash seguro (SHA-256 o superior).

2.3.3 Política de Actualizaciones y Parches

- Las actualizaciones de seguridad se aplicarán en un máximo de 7 días.
- Parches críticos (ej. vulnerabilidades con CVSS > 7) se aplicarán en 24-48 horas.
- Se mantendrá un inventario de software con versiones y fechas de actualización.
- Pruebas en entorno de staging antes de aplicar a producción.

2.3.4 Política de Configuración Segura (Hardening)

- SSH: `PermitRootLogin no`, `PasswordAuthentication no` (usar claves), puerto personalizable.
- FTP: Deshabilitado por defecto; si es necesario, usar SFTP y acceso autenticado.
- Apache: Deshabilitar directory listing (`Options -Indexes`), ocultar versión (`ServerTokens Prod`).
- WordPress: Permisos 755 para directorios, 644 para archivos, 600 para `wp-config.php`.
- MySQL: Solo conexiones locales, eliminar usuarios anónimos, contraseñas fuertes.

2.3.5 Política de Respuesta a Incidentes

- Todo incidente debe ser reportado al CSIRT en menos de 1 hora.
- Se seguirá el plan basado en NIST SP 800-61 (sección 1 de este documento).
- Se elaborará un informe final en un plazo de 7 días tras la resolución.

2.4 Planes de Acción para Protección de Información Crítica

Medida	Descripción	Plazo	Responsable	Indicador de éxito
Backups periódicos	Copias de seguridad diarias con retención de 30 días, almacenadas en ubicación externa .	Inmediato	Administradores	Restauración exitosa verificada mensualmente
Centralización de logs	Enviar logs a servidor remoto (rsyslog + SIEM) .	1 mes	Área de ciberseguridad	Logs accesibles tras caída del servidor
Monitoreo de cambios críticos	Alertar sobre `chmod 777`, edición de `sshd_config`, instalación de servicios .	2 meses	Área de ciberseguridad	Alertas generadas y revisadas
Hardening de servidores	Aplicar guías CIS a todos los servidores nuevos y existentes .	3 meses	Administradores	Checklist de hardening completado

Auditorías trimestrales	Revisar configuraciones, usuarios y permisos .	Trimestral	Auditor interno	Informe de auditoría sin hallazgos críticos
Capacitación anual	Entrenar al personal en seguridad y políticas .	Anual	RRHH / TI	100% del personal capacitado

2.5 Mejora Continua (Ciclo PDCA)

El SGSI se revisará y mejorará siguiendo el ciclo Planificar-Hacer-Verificar-Actuar (PDCA) :

Fase	Actividades	Frecuencia	Evidencia
Planificar	Análisis de riesgos, definición de políticas y objetivos	Anual	Documento de análisis de riesgos
Hacer	Implementación de controles y medidas de seguridad	Continuo	Registros de configuración, logs
Verificar	Auditorías internas, revisión de incidentes, métricas de cumplimiento	Semestral	Informes de auditoría
Actuar	Acciones correctivas y mejora de políticas	Anual	Plan de mejora continua

3. RELACIÓN CON EL CASO ANALIZADO

Las acciones del usuario `debian` el 8 de octubre de 2024 evidencian la necesidad de este SGSI:

Acción del caso	Política/Control que lo habría prevenido
`sudo apt install vsftpd`	Política de control de cambios y aprobación de nuevos servicios
`sudo nano /etc/ssh/sshd_config` (habilitar root)	Monitoreo de integridad de archivos críticos + política de hardening
`sudo chmod -R 777 /var/www/html`	Monitoreo de cambios masivos de permisos + política de permisos mínimos
Conexión root por SSH desde IP externa	Deshabilitar root login + MFA + monitoreo de accesos
Falta de logs centralizados	Centralización de logs para preservar evidencia

---

4. CONCLUSIÓN DE LA FASE 3

El plan de respuesta a incidentes basado en NIST SP 800-61 y el SGSI alineado con ISO 27001 permitirán a 4Geeks Academy:

- Detectar tempranamente actividades anómalas como las realizadas por el usuario `debian`.
- Responder de forma organizada con roles claros y procedimientos definidos .
- Contener y erradicar incidentes minimizando el impacto .
- Preservar evidencias mediante logs centralizados y backups .
- Mejorar continuamente la postura de seguridad mediante lecciones aprendidas .
- Cumplir con estándares que facilitan auditorías y certificaciones .