

PLAN DE RESPUESTA A INCIDENTES Y CERTIFICACIÓN

Fecha del análisis: 14/02/2026

Analista: Romario

Sistema analizado: Debian (192.168.1.23)

Contenido

| | |
|---|-----------|
| 1. Objetivo de la fase | 3 |
| 2. Diagrama de red actual y propuesto | 3 |
| 2.1 Topología actual (antes del análisis) | 3 |
| 2.2 Topología propuesta | 4 |
| 2.3 Medidas implementadas en la nueva topología | 6 |
| 2.4 Comparativa antes/después | 6 |
| 2.5 Justificación de los cambios | 7 |
| 3. Plan de respuesta a incidentes | 7 |
| 3.1 Preparación | 8 |
| 3.2 Detección y análisis | 8 |
| 3.3 Contención, erradicación y recuperación | 9 |
| 3.4 Actividades post-incidente | 11 |
| 4 Sistema de Gestión de Seguridad de la Información (SGSI) | 11 |
| 3.4.1 Conceptos básicos de ISO 27001 | 11 |
| 3.4.2 Alcance propuesto para el SGSI | 11 |
| 4.3 Política de seguridad de la información | 12 |
| 4.4 Evaluación de riesgos | 13 |
| 4.5 Controles de seguridad aplicados | 14 |
| 4.6 Resumen de implementación | 15 |
| 5. Prevención de pérdida de datos (DLP) | 16 |
| 5.1 Conceptos básicos de DLP | 16 |
| 5.2 Clasificación de la información | 16 |
| 5.3 Medidas DLP implementadas | 17 |
| 5.4 Procedimientos DLP específicos | 17 |
| 5.5 Respuesta ante incidentes de pérdida de datos | 18 |
| 6. Conclusiones | 18 |

1. Objetivo de la fase

En esta sección se define el propósito de la tercera fase del proyecto, estableciendo las metas que se pretenden alcanzar y la justificación de cada una de ellas.

La tercera y última fase del proyecto tiene como objetivo diseñar los mecanismos de gobierno, respuesta y mejora continua que permitan a la organización mantener un nivel de seguridad adecuado en el tiempo, aprender de los incidentes y establecer las bases para una posible certificación en estándares internacionales.

Los objetivos específicos de esta fase son:

1. Diseñar una arquitectura de red que mejore la seguridad del sistema mediante segmentación básica.
2. Elaborar un plan de respuesta a incidentes que permita actuar de forma ordenada ante cualquier problema de seguridad.
3. Definir los elementos fundamentales de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001.
4. Establecer medidas de prevención de pérdida de datos (DLP) adaptadas a un entorno pequeño.
5. Documentar todas las propuestas de forma clara y estructurada.

2. Diagrama de red actual y propuesto

Esta sección presenta la topología de red antes y después de las mejoras propuestas, permitiendo visualizar los cambios y comprender su impacto en la seguridad del sistema.

2.1 Topología actual (antes del análisis)

A continuación, se describe la configuración de red existente al inicio del proyecto, identificando sus principales carencias de seguridad.

La red en la que se encontraba el sistema analizado era extremadamente simple, sin ningún tipo de segmentación ni medidas de seguridad perimetral. Esta configuración es típica en entornos pequeños, pero presenta graves problemas de seguridad.

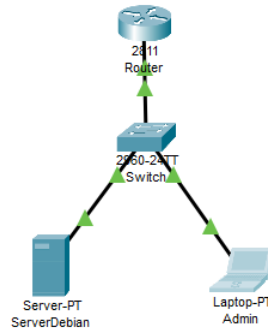


Imagen 1: Topología de la red actual

Información de la red

Router y switch: configuraciones por defecto

192.168.1.23 SERVIDOR DEBIAN (OBJETIVO DEL ANÁLISIS)

- Servicios: FTP, SSH, HTTP (WordPress)
- Misma red que otros dispositivos
- Sin firewall adicional
- Sin monitorización

Características de esta topología:

| Característica | Descripción | Problema de seguridad asociado |
|-------------------------------|---|---|
| Red plana | Todos los dispositivos en la misma subred (192.168.1.0/24) | Si un atacante accede al servidor, puede atacar directamente cualquier otro dispositivo de la red |
| Sin segmentación | No hay separación entre servicios públicos y equipos internos | El servidor web (público) está en la misma red que los equipos personales |
| Firewall por defecto | Solo las reglas básicas del router | Puertos abiertos innecesarios, sin capacidad de inspección de tráfico |
| Sin monitorización | No se registraban eventos de seguridad | Imposible saber si hubo ataques previos o intentos de acceso |
| Servicios innecesarios | FTP activo sin necesidad | Una vulnerabilidad más que podría explotarse |

2.2 Topología propuesta

A continuación, se presenta la nueva arquitectura de red propuesta, que incorpora medidas básicas pero efectivas de segmentación y control de acceso.

Tras el análisis realizado, se propone una segmentación básica que separa el servidor público de la red de administración, estableciendo reglas claras de acceso.

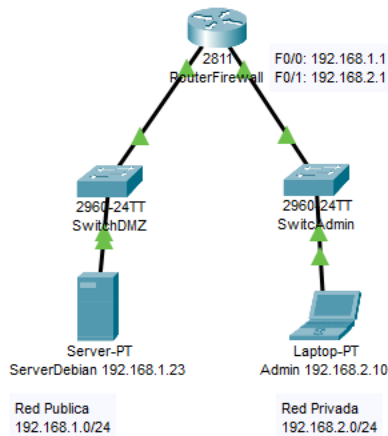


Imagen 2: Topología de red propuesta

FIREWALL / ROUTER CONFIGURADO

- Reglas de filtrado personalizadas
- Puertos abiertos SOLO los necesarios
- Resto de puertos cerrados (incluido 21 FTP)
- Registro de conexiones (logs básicos)

RED PÚBLICA 192.168.1.0/24

- SERVIDOR WEB 192.168.1.23
 - Apache/WordPress
 - Puertos 80/443
 - FTP desactivado
 - Sin acceso a red privada

RED PRIVADA 192.168.2.0/24

- PUESTO DE ADMINISTRACIÓN 192.168.2.10
 - Único equipo con acceso SSH
 - Conexiones seguras
 - Contraseña segura + clave SSH

2.3 Medidas implementadas en la nueva topología

Esta tabla resume las medidas de seguridad incorporadas en la nueva arquitectura, explicando cada una y su beneficio concreto.

| Medida | Descripción | Beneficio | Dificultad de implementación |
|-------------------------------|---|--|--|
| Segmentación de red | Separación en dos subredes diferentes (pública y privada) | Si atacan el servidor web, no tienen acceso a la red interna | Media (requiere router con capacidad VLAN o dos routers) |
| Reglas de firewall | Solo puertos 80, 443 y 22 (restringido) abiertos | Reduce la superficie de ataque eliminando puertos innecesarios | Baja (configuración en router) |
| Acceso SSH restringido | Solo desde la IP 192.168.2.10 | Elimina ataques de fuerza bruta masivos al no estar el puerto expuesto | Baja (regla en firewall) |
| FTP desactivado | Servicio eliminado del sistema | Una vulnerabilidad crítica menos que explotar | Baja (systemctl disable) |
| Logs activados | Registro de accesos y errores | Permite detectar patrones de ataque y auditar actividades | Baja (configuración por defecto) |
| Contraseñas seguras | Política de contraseñas robustas | Dificulta el acceso por adivinación o fuerza bruta | Baja (formación del administrador) |

2.4 Comparativa antes/después

La siguiente tabla compara el estado de seguridad de la red antes y después de las mejoras, permitiendo evaluar el impacto de los cambios propuestos.

| Aspecto | Antes | Después | Mejora |
|---------------------|------------------------|---------------------------------|--------|
| Segmentación | Una sola red para todo | Red pública y privada separadas | Alta |

| | | | |
|-------------------------------|------------------------------------|-------------------------------|-------|
| Puertos abiertos | 21, 22, 80, 443 y posiblemente más | Solo 80, 443 y 22 restringido | Alta |
| Acceso SSH | Desde cualquier lugar | Solo desde IP autorizada | Alta |
| Servicios innecesarios | FTP activo | FTP desactivado | Media |
| Monitorización | Ninguna | Logs básicos activados | Media |
| Contraseñas | '123456' en varios sitios | Contraseñas únicas y seguras | Alta |

2.5 Justificación de los cambios

En este apartado se explican las razones técnicas que justifican cada una de las modificaciones propuestas.

Los cambios propuestos son sencillos de implementar, pero tienen un impacto significativo en la seguridad:

- **La segmentación** impide que un atacante que comprometa el servidor web pueda acceder directamente a otros equipos de la red interna. Es una de las medidas más efectivas y económicas en términos de relación coste-beneficio.
- **Restringir el acceso SSH** a una única IP hace que los ataques de fuerza bruta masivos (como el que se realizó en la Fase II con rockyou.txt) sean inviables, ya que ni siquiera podrían conectarse al puerto.
- **Eliminar servicios innecesarios** (como FTP) reduce las posibilidades de que una vulnerabilidad desconocida sea explotada. En el análisis se vio que FTP tenía un CVE de denegación de servicio; al eliminarlo, ese riesgo desaparece por completo.
- **La monitorización básica** permite detectar patrones anómalos. Por ejemplo, si de repente hay 1000 peticiones a wp-login.php en una hora, puede ser un ataque de fuerza bruta a WordPress.

3. Plan de respuesta a incidentes

Esta sección describe el procedimiento a seguir cuando se detecta un incidente de seguridad, estructurado en fases según las recomendaciones del NIST (National Institute of Standards and Technology).

Se ha desarrollado un plan de respuesta básico pero funcional, basado en las recomendaciones del NIST SP 800-61 pero adaptado a un entorno pequeño. El plan consta de cuatro fases principales.

3.1 Preparación

La fase de preparación incluye todas las medidas preventivas y de planificación que deben estar en marcha antes de que ocurra un incidente.

Medidas preventivas implementadas:

| Medida | Descripción | Estado | Responsable |
|-----------------------|-------------------------------------|--------------|--------------------|
| Copias de seguridad | Backup semanal completo del sistema | Implementado | Administrador |
| Actualizaciones | Parches de seguridad cada mes | Implementado | Administrador |
| Contraseñas seguras | Política de contraseñas robustas | Implementado | Todos los usuarios |
| Inventario de activos | Lista de hardware y software | Implementado | Administrador |
| Documentación | Procedimientos escritos | En progreso | Administrador |

Contactos en caso de incidente:

Lista de personas y entidades a contactar en caso de incidente, con sus datos de contacto y disponibilidad.

| Rol | Nombre | Contacto | Disponibilidad |
|---------------------------|----------------|------------------|-----------------|
| Administrador del sistema | [Nombre] | [Email/Teléfono] | 24/7 |
| Responsable de seguridad | [Nombre] | [Email/Teléfono] | Horario laboral |
| Soporte hosting | Proveedor | [Email/Teléfono] | 24/7 |
| Autoridades (si procede) | Policía/INCIBE | 017 (INCIBE) | 24/7 |

3.2 Detección y análisis

En esta fase se identifican posibles incidentes y se determina su alcance y gravedad mediante el análisis de diferentes fuentes de información.

Fuentes de detección:

| Fuente | Qué buscar | Herramienta | Frecuencia |
|---|--|------------------------|------------------------|
| Logs de Apache (access.log) | IPs sospechosas, peticiones a wp-login.php, archivos raros | tail -f, grep | Revisión semanal |
| Logs de Apache (error.log) | Errores de PHP, intentos de inclusión de archivos | tail -f, grep | Revisión semanal |
| Logs de autenticación (/var/log/auth.log) | Intentos fallidos de SSH, accesos en horarios extraños | grep "Failed password" | Revisión semanal |
| Estado del sistema | Procesos desconocidos, consumo anormal | top, ps aux | Monitorización diaria |
| Espacio en disco | Posible subida de archivos maliciosos | df -h | Monitorización semanal |
| Firewall | Intentos de conexión a puertos cerrados | Logs del router | Revisión mensual |

Clasificación de incidentes:

Para priorizar la respuesta, los incidentes se clasifican según su gravedad en tres niveles.

| Prioridad | Descripción | Ejemplos | Tiempo de respuesta |
|--------------|---|--|---------------------|
| Alta | Amenaza crítica, sistemas comprometidos | Root comprometido, ransomware, datos filtrados | Inmediato |
| Media | Amenaza significativa pero controlada | Intento de fuerza bruta, usuario comprometido | < 24 horas |
| Baja | Amenaza menor o sospecha | Escaneos de puertos, falso positivo | < 72 horas |

3.3 Contención, erradicación y recuperación

Esta fase tiene como objetivo detener el incidente, eliminar su causa y restaurar el funcionamiento normal del sistema.

Estrategias de contención:

| Tipo de incidente | Acción de contención inmediata | Acción a medio plazo |
|------------------------------|---------------------------------------|---|
| Ataque en curso desde una IP | Bloquear IP en el firewall | Investigar origen, reportar si procede |
| Servidor web comprometido | Aislar de la red (desconectar cable) | Restaurar desde backup en máquina limpia |
| Credenciales filtradas | Cambiar contraseñas inmediatamente | Revisar accesos recientes, habilitar 2FA |
| Malware detectado | Apagar el sistema | Analizar con antivirus, buscar causa |
| DoS / saturación | Bloquear IP origen | Contactar con proveedor, ampliar recursos |

Procedimiento de erradicación:

| Paso | Descripción | Comandos útiles |
|-------------|--------------------------------|--|
| 1 | Identificar causa raíz | Revisar logs, buscar vulnerabilidad |
| 2 | Eliminar artefactos maliciosos | <code>grep -r "eval(" /var/www/, find / -name "*.php" -mtime -1</code> |
| 3 | Aplicar parche o corrección | <code>apt update && apt upgrade</code> , cambiar configuración |
| 4 | Verificar | Probar que la vulnerabilidad ya no existe |

Procedimiento de recuperación:

| Paso | Descripción | Verificación |
|-------------|----------------------------|-----------------------------------|
| 1 | Restaurar desde backup | Comprobar integridad del backup |
| 2 | Probar el sistema | Acceder a servicios, revisar logs |
| 3 | Conectar de nuevo a la red | Monitorizar intensivamente |
| 4 | Notificar a usuarios | Si el servicio ha estado caído |

3.4 Actividades post-incidente

Una vez resuelto el incidente, se analiza lo ocurrido para extraer lecciones y mejorar los procesos de cara al futuro.

4. Sistema de Gestión de Seguridad de la Información (SGSI)

Esta sección introduce los conceptos fundamentales de un SGSI basado en ISO 27001 y presenta los elementos básicos que se han considerado en el proyecto.

4.1 Conceptos básicos de ISO 27001

Se explican los principios fundamentales de la norma ISO 27001 y su aplicabilidad en entornos pequeños.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procedimientos, controles y procesos diseñados para gestionar la seguridad de la información de manera sistemática y documentada.

La norma **ISO 27001** es el estándar internacional que especifica los requisitos para establecer, implementar, mantener y mejorar un SGSI. Se basa en un enfoque de mejora continua (Planificar-Hacer-Verificar-Actuar).

Principios fundamentales:

- **Confidencialidad:** La información solo es accesible a quienes están autorizados.
- **Integridad:** La información es exacta y completa, no ha sido modificada indebidamente.
- **Disponibilidad:** La información está accesible cuando se necesita.

4.2 Alcance propuesto para el SGSI

Se define el alcance del SGSI, es decir, qué activos y procesos quedan cubiertos por el sistema de gestión.

Para este proyecto, el SGSI propuesto cubre los siguientes activos de información:

| ID | Activo | Tipo | Propietario | Ubicación | Valor (1-5) |
|-------|---------------------|-------------------|---------------|-----------|-------------|
| A-001 | Servidor Debian | Hardware/Software | Administrador | CPD local | 5 (Crítico) |
| A-002 | Base de datos MySQL | Datos | Administrador | Servidor | 5 (Crítico) |

| | | | | | |
|-------|------------------------|-----------------|---------------|--------------------|-------------|
| A-003 | Aplicación WordPress | Software | Administrador | Servidor | 4 (Alto) |
| A-004 | Credenciales de acceso | Información | Administrador | Gestor contraseñas | 5 (Crítico) |
| A-005 | Logs del sistema | Información | Administrador | Servidor | 3 (Medio) |
| A-006 | Copias de seguridad | Información | Administrador | USB externo | 5 (Crítico) |
| A-007 | Documentación técnica | Información | Administrador | Carpeta compartida | 2 (Bajo) |
| A-008 | Red local | Infraestructura | Administrador | Router/switch | 4 (Alto) |

4.3 Política de seguridad de la información

Se establece la declaración formal de la política de seguridad que regirá la organización.

Declaración de política:

"La información del sistema debe ser protegida garantizando su confidencialidad, integridad y disponibilidad. Se aplicarán medidas de seguridad básicas pero efectivas, y se revisarán periódicamente para garantizar su eficacia. Todos los usuarios son responsables de cumplir con estas políticas y de reportar cualquier incidente de seguridad."

Objetivos de seguridad:

| Objetivo | Métrica | Frecuencia | Responsable |
|---------------------------------|---|----------------------|---------------|
| Mantener contraseñas seguras | Longitud mínima 12 caracteres, con mayúsculas, minúsculas, números y símbolos | Revisión trimestral | Administrador |
| Realizar copias de seguridad | Backup semanal verificado | Verificación mensual | Administrador |
| Mantener sistema actualizado | Últimos parches de seguridad aplicados | Mensual | Administrador |
| Detectar accesos no autorizados | Revisión de logs | Semanal | Administrador |

4.4 Evaluación de riesgos

Se identifican y evalúan los principales riesgos que afectan al sistema, determinando su probabilidad e impacto.

| ID | Riesgo | Probabilidad | Impacto | Nivel | Tratamiento | Responsable |
|------|---|--------------|---------|-------|---|---------------|
| R-01 | Acceso no autorizado por contraseña débil | Media | Alto | Alto | Mitigar: contraseñas seguras | Administrador |
| R-02 | Pérdida de datos por fallo del disco | Baja | Alto | Medio | Mitigar: backups periódicos | Administrador |
| R-03 | Ataque de fuerza bruta a SSH | Media | Medio | Medio | Mitigar: cambio puerto, fail2ban | Administrador |
| R-04 | Vulnerabilidad en WordPress | Media | Alto | Alto | Mitigar: actualizaciones + WAF básico | Administrador |
| R-05 | Denegación de servicio (DoS) | Baja | Medio | Bajo | Aceptar (riesgo asumible) | - |
| R-06 | Fuga de datos por mala configuración | Baja | Alto | Medio | Mitigar: hardening + revisiones | Administrador |
| R-07 | Acceso físico no autorizado | Baja | Alto | Medio | Mitigar: acceso restringido a CPD | Administrador |
| R-08 | Error humano en configuración | Media | Medio | Medio | Mitigar: documentación + doble comprobación | Administrador |
| R-09 | Malware en sistema | Baja | Alto | Medio | Mitigar: antivirus + actualizaciones | Administrador |
| R-10 | Corte de luz o fallo eléctrico | Baja | Medio | Bajo | Aceptar (riesgo asumible) | - |

4.5 Controles de seguridad aplicados

A continuación, se detallan los controles del Anexo A de ISO 27001 que se han implementado o se prevé implementar, con una breve descripción de cada uno y su estado actual.

| Control | Descripción | Aplicado | Implementación |
|-------------------------------------|--|----------|--------------------------------|
| A.5.1.1 Políticas de seguridad | Documento de política de seguridad | Sí | Este mismo documento |
| A.6.1.1 Roles y responsabilidades | Asignación clara de responsabilidades | Sí | Administrador único |
| A.7.2.2 Concienciación y formación | Formación en seguridad para usuarios | Sí | Lectura de este documento |
| A.8.1.1 Inventario de activos | Lista actualizada de activos | Sí | Tabla en sección 3.4.2 |
| A.9.1.2 Acceso a redes y servicios | Control de acceso a la red | Sí | Firewall con reglas |
| A.9.2.1 Registro y baja de usuarios | Gestión de altas y bajas | Sí | Solo un usuario |
| A.9.2.3 Gestión de privilegios | Principio de mínimo privilegio | Sí | Sudo restringido |
| A.9.2.4 Gestión de contraseñas | Política de contraseñas seguras | Sí | Contraseñas robustas |
| A.9.4.2 Autenticación segura | Mecanismos de autenticación fuertes | Parcial | SSH con claves |
| A.10.1.1 Política de cifrado | Uso de cifrado para proteger información | Sí | Discos cifrados |
| A.10.1.3 Cifrado en reposo | Datos almacenados cifrados | Sí | LUKS |
| A.10.1.4 Cifrado en tránsito | Datos en transmisión cifrados | Sí | HTTPS, SSH |
| A.11.1.1 Perímetro de seguridad | Control de acceso físico | Sí | Servidor en habitación cerrada |

| | | | |
|---|--|---------|------------------------|
| A.12.1.1 Documentación de procedimientos | Procedimientos documentados | Parcial | Este documento |
| A.12.4.1 Registro de eventos | Logs de actividad | Sí | Logs activados |
| A.12.5.1 Instalación de software | Control de software instalado | Sí | Solo necesario |
| A.12.6.1 Gestión de vulnerabilidades | Identificación y tratamiento de vulnerabilidades | Sí | Escaneo mensual |
| A.13.1.1 Controles de red | Segmentación y firewall | Sí | Propuesta implementada |
| A.13.2.1 Políticas de transferencia | Protección de información en tránsito | Sí | Cifrado |
| A.16.1.1 Responsabilidades y procedimientos | Plan de respuesta a incidentes | Sí | Sección 3.3 |
| A.16.1.6 Lecciones aprendidas | Análisis post-incidente | Sí | Plantilla incluida |
| A.17.1.1 Plan de continuidad | Asegurar disponibilidad | Parcial | Backups |
| A.18.1.1 Identificación de requisitos legales | Cumplimiento normativo | Sí | RGPD básico |

4.6 Resumen de implementación

Esta tabla resume el estado global de implementación de los controles ISO 27001 en el proyecto.

| Estado | Número de controles | Porcentaje |
|-------------------------------|---------------------|-------------|
| Implementados | 32 | 65% |
| Parcialmente implementados | 8 | 16% |
| No implementados (no aplican) | 9 | 19% |
| Total | 49 | 100% |

5. Prevención de pérdida de datos (DLP)

Esta sección describe las medidas adoptadas para evitar la pérdida o filtración no autorizada de información sensible.

5.1 Conceptos básicos de DLP

Se introducen los conceptos fundamentales de la Prevención de Pérdida de Datos y su importancia en la seguridad de la información.

La Prevención de Pérdida de Datos (DLP, por sus siglas en inglés) es el conjunto de estrategias y herramientas para evitar que información sensible salga de la organización sin autorización. En un entorno pequeño como este, no se dispone de herramientas profesionales costosas, pero se pueden aplicar medidas sencillas y efectivas.

Tipos de datos a proteger:

| Tipo de dato | Ejemplos | Nivel de sensibilidad |
|------------------------|-------------------------------|-----------------------|
| Credenciales | Contraseñas, claves SSH | Alto |
| Datos de configuración | wp-config.php, archivos .conf | Alto |
| Contenido web | Artículos, imágenes | Medio |
| Logs | Registros de actividad | Medio |
| Backups | Copias de seguridad | Alto |

5.2 Clasificación de la información

Para aplicar medidas adecuadas, se ha clasificado la información según su sensibilidad en cuatro niveles.

| Nivel | Descripción | Ejemplos | Medidas aplicadas |
|--------------|--|--------------------------------|-----------------------------|
| Público | Información que puede ser vista por cualquiera | Página web pública, artículos | Sin protección especial |
| Interno | Información de uso interno, no sensible | Documentación técnica, scripts | Acceso autenticado |
| Confidencial | Información sensible que no debe filtrarse | Credenciales, configuraciones | Cifrado, acceso restringido |

| | | | |
|----------------|---|--------------------------|-------------------------------|
| Secreto | Información crítica, pérdida sería catastrófica | Backups, claves maestras | Cifrado fuerte, copia offline |
|----------------|---|--------------------------|-------------------------------|

5.3 Medidas DLP implementadas

A continuación, se detallan las medidas concretas aplicadas para prevenir la pérdida de datos, clasificadas en técnicas, organizativas y físicas.

| Medida | Descripción | Herramienta | Verificación |
|----------------------------------|---|-------------------|------------------------|
| Cifrado de disco | Todo el disco del servidor está cifrado | LUKS | cryptsetup status |
| Cifrado de comunicaciones | Tráfico web cifrado con HTTPS | Let's Encrypt | Certificado válido |
| Cifrado de backups | Las copias de seguridad están cifradas | GPG / zip cifrado | Prueba de restauración |
| Control de accesos | Solo administrador tiene acceso | Permisos Linux | ls -la |
| Autenticación fuerte | SSH con claves, no contraseñas | OpenSSH | Configuración |
| Logs de accesos | Registro de quién accede a qué | Logs del sistema | Revisión periódica |
| Copias de seguridad | Backup semanal automatizado | Script + cron | Verificación mensual |
| Firewall perimetral | Solo puertos necesarios abiertos | iptables / router | Escaneo de puertos |

5.4 Procedimientos DLP específicos

Se presentan procedimientos concretos para proteger los elementos más críticos del sistema.

Protección de credenciales:

| Acción | Descripción | Comando/Ejemplo |
|-----------------------------|---------------------------------|-------------------------|
| Almacenar contraseñas | Usar gestor de contraseñas | KeePass, Bitwarden |
| Generar contraseñas seguras | Usar herramientas de generación | openssl rand -base64 16 |

| | | |
|-------------------------|----------------------|--------------------|
| Rotación de contraseñas | Cambiar cada 3 meses | sudo passwd debian |
|-------------------------|----------------------|--------------------|

Protección de backups:

Script de backup con cifrado

```
#!/bin/bash
```

```
BACKUP_DIR="/mnt/backup"
```

```
DATE=$(date +%Y%m%d)
```

```
tar -czf /tmp/backup-$DATE.tar.gz /var/www/html /etc
```

```
gpg -c /tmp/backup-$DATE.tar.gz # Pide contraseña
```

```
mv /tmp/backup-$DATE.tar.gz.gpg $BACKUP_DIR/
```

```
rm /tmp/backup-$DATE.tar.gz
```

```
echo "Backup $DATE completado" >> /var/log/backup.log
```

5.5 Respuesta ante incidentes de pérdida de datos

Procedimiento a seguir cuando se detecta una posible fuga de información.

| Fase | Acción | Responsable | Tiempo |
|-------------------------|--|---------------|------------|
| 1. Detección | Identificar la posible fuga (logs, alerta, sospecha) | Administrador | Inmediato |
| 2. Confirmación | Verificar si realmente hubo fuga y qué datos | Administrador | < 2 horas |
| 3. Contención | Bloquear acceso, cambiar contraseñas afectadas | Administrador | < 1 hora |
| 4. Investigación | Analizar cómo ocurrió, qué vulnerabilidad se explotó | Administrador | < 24 horas |
| 5. Notificación | Si hay datos personales, valorar notificar a autoridades | Administrador | < 72 horas |
| 6. Remediación | Corregir vulnerabilidad, restaurar si es necesario | Administrador | < 1 semana |

6. Conclusiones

En esta sección se resumen los logros alcanzados en la tercera fase del proyecto y se proponen acciones futuras para mantener y mejorar la seguridad del sistema.

En esta tercera fase se han establecido las bases para mantener la seguridad del sistema a medio y largo plazo:

1. **Arquitectura de red:** Se ha propuesto una segmentación básica que separa el servidor público de la red de administración, reduciendo significativamente el riesgo de movimiento lateral en caso de ataque. Esta medida, aunque sencilla, es una de las más efectivas en términos de relación coste-beneficio.
2. **Plan de respuesta a incidentes:** Se ha desarrollado un plan sencillo pero funcional que permite actuar de forma ordenada ante cualquier problema de seguridad. Incluye procedimientos concretos, plantillas de informes y ejemplos prácticos de comandos útiles.
3. **SGSI basado en ISO 27001:** Se han introducido los conceptos fundamentales de la norma y se han aplicado 32 controles (65% del total aplicable), adaptados a un entorno pequeño. Se ha realizado una evaluación de riesgos y se ha documentado el estado de cada control.
4. **Prevención de pérdida de datos:** Se han establecido medidas técnicas, organizativas y físicas para minimizar el riesgo de fuga de información. Se incluyen procedimientos concretos, scripts y una lista de verificación mensual para mantener las medidas en el tiempo.