SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Plan Director de Seguridad - Fase 3
Hospital General de Madrid

Autor: Arturo Martín-Vegue
Fecha: 6 de enero de 2026

CONFIDENCIAL

Índice

1. Introducción y Visión General

1.1. Propósito del Manual

Este manual describe el Sistema de Gestión de Seguridad de la Información (SGSI) del Hospital General, diseñado para proteger la confidencialidad, integridad y disponibilidad de los datos de pacientes y sistemas críticos, cumpliendo con estándares internacionales (ISO 27001) y normativas de salud.

1.2. Compromiso del Liderazgo

La Alta Dirección del Hospital manifiesta su compromiso total con el SGSI mediante:

1. **Asignación de Recursos:** Garantizar el presupuesto necesario para tecnología y formación.
2. **Mejora Continua:** Revisar semestralmente el desempeño de la seguridad.
3. **Cultura de Seguridad:** Liderar con el ejemplo, promoviendo que la seguridad de la información es responsabilidad de todos, desde el celador hasta el Director Médico.

---

2. Definición del Alcance

2.1. Inventario de Activos

Para definir el perímetro de seguridad, se han identificado los siguientes activos principales:

- **Hardware**: Servidores de almacenamiento de datos, servidores para SIEM (Security Information and Event Manager), máquinas de resonancia magnética (IoT médico), ordenadores de personal médico y administrativo, equipos de blue team.
- **Software**: Sistemas operativos **Windows** para ordenadores de personal médico y administrativo y servidores **Linux** para el almacenaje de datos, software de gestión hospitalaria, herramientas de seguridad (EDR, SIEM) y software de control de maquinaria médica.
- **Datos**: Historiales clínicos de pacientes, datos de filiación (Seguridad Social, DNI, teléfonos), información del personal sanitario e información de infraestructura TI.

2.2. Declaración de Alcance

El alcance del SGSI aplica a todos los servicios clínicos, administrativos y de seguridad del Hospital General de Madrid.

Específicamente, el sistema se centrará en proteger la integridad y confidencialidad de los activos clasificados como CRÍTICOS:

1. Los **servidores** que alojan los historiales y el sistema de monitoreo (SIEM).
2. El **software** de defensa (EDR) y el control operativo de maquinaria vital.
3. Los **datos sensibles** (historiales médicos y números de la Seguridad Social)

Quedan dentro del alcance todas las ubicaciones físicas de la sede principal donde se procesen estos datos.

2.3. Limites Físicos y Lógicos

- **Ubicaciones Físicas:** El alcance cubre el edificio principal del Hospital. Se destaca la inclusión del **Centro de Procesamiento de Datos (CPD)** propio, ubicado físicamente en el sótano para mayor control de los datos críticos.
- **Áreas Restringidas:** Se aplica una política de control de acceso estricto. Todo el recinto se considera restringido (Quirófanos, consultas, laboratorios, sala de servidores/CPD), salvo las zonas públicas designadas explícitamente (recepciones, salas de espera, aseos).
- **Redes y Nube:** La infraestructura es híbrida.
  - Red Interna (LAN) gestionada localmente.
  - Extensión de la nube mediante AWS (Amazon Web Services) para servicios de soporte y redundancia, bajo estrictos acuerdos de nivel de servicio de seguridad.

2.4. Partes Interesadas y Responsabilidades

Para el correcto funcionamiento del SGSI, se definen los siguientes roles y responsabilidades:

- **Alta Dirección (Gerencia)**
  - Aprobar la Política de Seguridad y asignar el presupuesto necesario.
  - Garantizar la realización de auditorías internas periódicas.
  - Asumir la responsabilidad legal final sobre la protección de datos.
- **Equipo de TI / Seguridad (Blue Team)**
  - Monitoreo activo de amenazas internas y externas.
  - Configuración segura de equipos y gestión de la encriptación.
  - Respuesta ante incidentes y mantenimiento de sistemas (SIEM, EDR).
- **Personal Médico y Administrativo**
  - Uso correcto de los datos para fines estrictamente laborales.
  - Gestión de credenciales: contraseñas robustas y rotación trimestral.
  - Asistencia obligatoria a cursos de concienciación en seguridad.

2.5. Propósito del SGSI

El objetivo principal de este SGSI es establecer un marco de gestión que garantice la **Confidencialidad, Integridad y Disponibilidad** de la información del Hospital. Específicamente, busca:

1. Asegurar el cumplimiento normativo (RGPD, Esquema Nacional de Seguridad).
2. Proteger la privacidad de los pacientes frente a filtraciones.
3. Garantizar la continuidad de los servicios críticos (Urgencias, Quirófanos) ante ciberataques.

2.6. Limitaciones y Exclusiones

Se excluye del alcance de este SGSI la **Red Wi-Fi pública para invitados**. Dicha red está aislada lógicamente (VLAN separada) de la red corporativa y no tiene acceso a ningún activo crítico del hospital.

---

3. Evaluación de Riesgos y Amenazas Detectadas

ID	Activo (Categoría)	Amenaza	Vulnerabilidad	Riesgo	Clasificación
R01	Servidor Historiales	Ransomware	Sistemas desactualizados	9	**CRÍTICO** |
R02	Credenciales Jefe	Phishing	Reutilización de claves	6	**ALTO** |
R03	Centro de Datos (CPD)	Inundación	Ubicación en sótano	3	**MEDIO** |
R04	Servidor Web (Apache)	Intrusión	Permisos 777 / Default	9	**CRÍTICO** |
R05	Servicio FTP	Fuga de Datos	Acceso "Anonymous"	7	**ALTO** |

Nota: El resigo R04 se materializó el **08 de Octubre de 2024** debido a la exposición de credenciales en el archivo `wp-config.php`.

---

4. Plan de Respuesta a Incidentes (NIST SP 800-61)

4.1. Preparación

El Hospital General cuenta con un equipo de seguridad (Blue Team) y herramientas de monitoreo (SIEM) definidas en el SGSI para la detección de amenazas.

4.2. Detección y Análisis

Durante la fase de monitoreo y auditoría, el Equipo de Seguridad (Blue Team) detectó anomalías en el servidor crítico `192.168.122.10`. El análisis forense confirmó el compromiso del activo basándose en las siguientes evidencias técnicas:

- **Detección de Vectores de Entrada:**
  - Se identificó el puerto **21 (FTP)** expuesto sin restricciones, permitiendo el acceso anónimo (`Anonymous Login`) y exponiendo la estructura de directorios.
  - Se detectó el puerto **80 (HTTP)** con configuraciones inseguras de permisos.
- **Evidencias de Compromiso:**
  - **Evaluación de la Integridad de Registros y Trazabilidad:** Se ha validado que el sistema utiliza una arquitectura de registros binarios (**Systemd-Journald**), lo que asegura la persistencia de las evidencias ante intentos de manipulación básica. La lección aprendida es la necesidad de contar con personal capacitado en herramientas de auditoría binaria (`journalctl`) para reducir los tiempos de respuesta ante incidentes.
  - **Permisos Inseguros:** El directorio raíz del servidor web (`/var/www/html`) presentaba permisos `777` (lectura, escritura y ejecución para todos), permitiendo la modificación de archivos críticos.
  - **Credenciales Expuestas:** Se hallaron credenciales por defecto (`123456`) en texto claro dentro del archivo `wp-config.php`, otorgando acceso directo a la base de datos de pacientes.
- **Configuraciones de Riesgo:**
  - El servicio SSH permitía el inicio de sesión directo como `root`, facilitando ataques de fuerza bruta.

4.3. Contención, Erradicación y Recuperación

Tras confirmar los vectores de ataque, se ejecutaron las siguientes acciones correctivas para mitigar el riesgo y restablecer la seguridad del activo:

- **Medidas de Contención (Frenar el ataque):**
  - Se procedió al aislamiento temporal del servicio FTP para detener posibles exfiltraciones de datos en curso.
  - Se revocaron las sesiones activas y se forzó el reinicio de los servicios comprometidos (`vsftpd` y `ssh`).
- **Erradicación (Eliminar la causa raíz):**
  - **Hardening de FTP:** Se modificó el archivo de configuración `/etc/vsftpd.conf`, cambiando la directiva `anonymous_enable=YES` a `NO` para prohibir accesos no autenticados.
  - **Corrección de Permisos Web:** Se ejecutó una normalización recursiva de permisos en `/var/www/html` (755 para directorios, 644 para ficheros) para eliminar la capacidad de escritura pública.
  - **Rotación de Credenciales:** Se modificó la contraseña de base de datos en `wp-config.php`, sustituyendo la clave por defecto (`123456`) por una credencial robusta generada según la política del SGSI.
  - **Blindaje de SSH:** Se deshabilitó el acceso directo de `root` (`PermitRootLogin no`) en `/etc/ssh/sshd_config` para prevenir ataques de fuerza bruta privilegiada.
- **Recuperación (Vuelta a la normalidad):**
  - Se reiniciaron los servicios afectados (`systemctl restart vsftpd`, `ssh`, `apache2`) para aplicar los cambios.
  - **Retesting:** Se realizaron pruebas de conexión manuales y escaneos de verificación, confirmando que el servidor rechaza conexiones anónimas y que los permisos de archivos son seguros.

4.4. Actividad Post-Incidente (Lecciones Aprendidas)

El análisis del incidente ha revelado carencias en la fase de despliegue y monitoreo que han sido subsanadas. Como parte del ciclo de mejora continua del NIST y del SGSI, se establecen las siguientes acciones estratégicas para evitar la recurrencia:

- **Política de "Hardening" Antes del Despliegue:** Se establece la obligatoriedad de aplicar una lista de verificación de seguridad (checklist) antes de conectar cualquier servidor a la red. Esto incluye la prohibición explícita de credenciales por defecto y configuraciones de servicios "out-of-the-box" (como FTP anónimo).
- **Mejora en la Trazabilidad (Logs):** Dado que la auditoría local de logs binarios puede ser compleja durante un incidente, se establece como acción estratégica la implementación de un **SIEM (Wazuh)**. Esto permitirá centralizar los registros del Journal en un servidor externo e inmutable, facilitando la visualización de alertas en tiempo real sin depender de la consola local del servidor.
- **Revisión de Accesos Privilegiados:** Se refuerza la política de contraseñas, exigiendo rotación trimestral y complejidad robusta para todas las cuentas de servicio y administración de bases de datos.

---

5. Políticas de Prevención de Pérdida de Datos (DLP)

Para garantizar el cumplimiento normativo (RGPD), se han formalizado las siguientes políticas de clasificación y restricción de datos, integrándolas en la operativa diaria del Hospital.

5.1. Clasificación de la Información

Para aplicar controles efectivos, se ha categorizado la información manejada por la organización en tres niveles de sensibilidad:

- **Datos Sensibles (Confidencial):** Información cuya divulgación causaría daños graves (legales, financieros o reputacionales). Incluye:
  - **Historiales Médicos y Diagnósticos** (Datos de categoría especial RGPD).
  - **Identificación Personal (PII):** DNI, Seguridad Social, Teléfonos de pacientes.
  - **Credenciales:** Contraseñas de acceso a sistemas y bases de datos.
- **Datos de Uso Interno:** Información corporativa no pública (procedimientos internos, guías de estilo, organigramas) cuyo impacto de filtración es moderado.
- **Datos Públicos:** Información destinada a la divulgación (Ubicación del hospital, catálogo de servicios, políticas de privacidad).

5.2. Restricción de Medios Extraíbles (USB)

Se ha detectado que el uso de dispositivos de almacenamiento personal representa un vector crítico para la exfiltración de datos (DLP) y la entrada de malware (como en el caso del Ransomware).

Medida Implementada (GPO): Se ha configurado una Directiva de Grupo (GPO) local discriminatoria con las siguientes reglas:

1. **Bloqueo Total:** Se deniega el acceso de **Lectura y Escritura** a cualquier disco extraíble (USB/Disco Duro Externo).
2. **Alcance:** Esta política aplica automáticamente a todos los usuarios del grupo "No Administradores" (personal médico y administrativo).
3. **Excepción:** Solo los administradores de sistemas (IT) tienen permisos para montar unidades externas bajo justificación técnica.

5.3. Política de Robustez de Identidades y Mitigación de Credenciales por Defecto

Se establece como norma de obligado cumplimiento la eliminación de cualquier credencial configurada de fábrica o por defecto en los sistemas antes de su paso a producción. El uso de combinaciones predecibles o de alta frecuencia en diccionarios de ataque (como las detectadas en la fase de auditoría técnica) supone un riesgo crítico que invalida el resto de controles perimetrales.

Directivas Obligatorias:

- **Prohibición de Credenciales "Default" (por defecto):** Queda estrictamente prohibido el despliegue de activos que mantengas las contraseñas configuradas por el fabricante o por scripts de instalación automatizados (ej. `admin/admin`, `debian/123456`).

- **Estándar de Complejidad:** Toda cuenta de sistema o de servicio deberá cumplir con una longitud mínima de 12 caracteres, integrando obligatoriamente mayúsculas, minúsculas, números y caracteres especiales.
- **Hardening de Cuentas del Sistema:** Se deberá realizar un proceso de "endurecimiento" en cada servidor que incluya la desactivación de usuarios genéricos y la personalización de identificadores de acceso para evitar ataques de adivinación de credenciales.
- **Auditoría de Acceso:** Cualquier intento de acceso local o remoto que utilice credenciales consideradas "débiles" según los estándares actuales de ciberseguridad será motivo de bloqueo inmediato del activo y revisión por parte del equipo de seguridad (Blue Team).

---

6. Conclusión

El incidente de seguridad analizado ha servido como catalizador para madurar la postura de ciberseguridad del Hospital General de Madrid.

A través de este proyecto, se ha logrado:

1. **Identificar y remediar** vulnerabilidades críticas (FTP Anónimo, Webshell y Permisos 777) que exponían datos de pacientes.
2. **Formalizar la respuesta** ante incidentes mediante un plan basado en NIST, pasando de una reacción improvisada a un procedimiento estandarizado.
3. **Endurecer (Harden)** la infraestructura preventiva con políticas DLP y controles de acceso estrictos.

El SGSI actualizado no es solo un documento burocrático, sino una herramienta viva que ahora refleja las amenazas reales enfrentadas, garantizando que la organización sea más resiliente ante futuros ataques.