# PROYECTO SGSI HOSPITALES PUBLICOS

# Imagen de la pantalla de un videojuego El contenido generado por IA puede ser incorrecto.

Proyecto SGSI para Hospitales Públicos

# Índice

1. Introducción
2. Definición del Alcance del SGSI
3. Inventario y Clasificación de Activos
4. Evaluación de Riesgos
5. Selección de Controles
6. Documentación de Políticas y Procedimientos de Seguridad
7. Preparación del Manual del SGSI
8. Revisión y Presentación del SGSI

# 1. Introducción

El presente documento detalla el proyecto de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en hospitales públicos. Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información sensible, asegurando el cumplimiento normativo y la continuidad de los servicios médicos.

# 2. Definición del Alcance del SGSI

## Ubicaciones físicas incluidas

* Oficinas administrativas
* Salas de consulta y hospitalización
* Sala de servidores (acceso restringido)
* Laboratorio de investigación (acceso restringido)
* Centro de datos externo (si aplica)
* Áreas de almacenamiento de copias de seguridad

## Redes y entornos incluidos

* Red interna del hospital
* VPN para acceso remoto seguro
* Entornos en la nube utilizados para almacenamiento o aplicaciones
* Máquinas virtuales en servidores internos

## Sistemas y tipos de datos bajo el SGSI

* Sistemas de gestión hospitalaria (HIS)
* Bases de datos de pacientes
* Sistemas de correo electrónico institucional
* Aplicaciones administrativas y de recursos humanos
* Datos personales, médicos y administrativos

## Partes interesadas clave y responsabilidades

|  |  |
| --- | --- |
| Parte interesada | Responsabilidad principal |
| Equipo de TI | Implementación y mantenimiento de controles técnicos, monitoreo y respuesta a incidentes. |
| Dirección del hospital | Aprobación de políticas, asignación de recursos. |
| Personal médico | Uso seguro de sistemas y protección de datos de pacientes. |
| Personal administrativo | Manejo seguro de información administrativa. |
| Proveedores externos | Cumplimiento de políticas de seguridad en servicios tercerizados. |

## Propósito, metas y objetivos del SGSI

* Propósito: Proteger la confidencialidad, integridad y disponibilidad de la información del hospital público.
* Metas:
* Prevenir accesos no autorizados.
* Garantizar la continuidad de los servicios médicos.
* Cumplir con normativas legales y regulatorias.

Objetivos:

Implementar controles de acceso.

Realizar copias de seguridad periódicas.

Capacitar al personal en buenas prácticas de seguridad.

# 3. Inventario y Clasificación de Activos

|  |  |  |
| --- | --- | --- |
| Activo | Clasificación | Descripción/Importancia |
| Servidores de bases de datos | Crítico | Almacenan historiales médicos y datos personales de pacientes. |
| Computadoras de personal | Alto | Acceso a sistemas clínicos y administrativos. |
| Sistemas de gestión hospitalaria (HIS) | Crítico | Gestionan la atención médica y operaciones. |
| Información de pacientes | Crítico | Datos personales y médicos sensibles. |
| Información administrativa | Medio | Datos de gestión interna y recursos humanos. |

# 4. Evaluación de Riesgos

## Amenazas y vulnerabilidades

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Activo | Amenaza | Vulnerabilidad | Probabilidad | Impacto | Riesgo |
| Servidores de bases de datos | Acceso no autorizado | Contraseñas débiles | Alta | Alta | Alto |
| Computadoras de personal | Malware | Falta de antivirus actualizado | Media | Alta | Alto |
| Sistemas HIS | Ataque DoS | Falta de firewall/limitación | Media | Alta | Alto |
| Información de pacientes | Fuga de datos | Falta de cifrado | Baja | Muy alta | Alto |
| Copias de seguridad | Pérdida de datos | Almacenamiento inseguro | Media | Alta | Alto |

# 5. Selección de Controles

## Controles seleccionados y su documentación

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Riesgo identificado | Control seleccionado | Descripción / Mitigación | Responsable | Cronograma / Recursos |
| Acceso no autorizado a bases de datos | Control de acceso basado en roles (RBAC) | Solo personal autorizado puede acceder a datos sensibles. | Equipo de TI | 1 mes / Software de gestión |
| Fuga de información de pacientes | Cifrado de datos en reposo y en tránsito | Datos cifrados en bases de datos y durante la transmisión. | Equipo de TI | 2 meses / Licencias de cifrado |
| Ataques DoS a sistemas críticos | Firewall y limitación de conexiones | Filtrado de tráfico y límites de conexiones simultáneas. | Equipo de TI | 1 mes / Firewall físico |
| Pérdida de copias de seguridad | Copias de seguridad automáticas y externas | Backups regulares y almacenamiento fuera del sitio. | TI / Soporte | 2 semanas / Almacenamiento |
| Malware en computadoras de personal | Antivirus actualizado y control de USB | Protección contra malware y restricción de dispositivos. | TI / Usuarios | 2 semanas / Licencias AV |

# 6. Documentación de Políticas y Procedimientos

* Política de Seguridad de la Información
* Gestión de accesos
* Gestión de incidentes
* Capacitación y concienciación
* Revisión y actualización

6.1 Implementación de controles técnicos adicionales

Además de las políticas establecidas, se recomienda evaluar e implementar controles técnicos como la segmentación de redes, el uso de listas blancas para aplicaciones y un sistema de monitoreo continuo. Estas medidas pueden mejorar aún más la prevención y detección de incidentes dentro del marco de seguridad.

6.2 Evaluación periódica de cumplimiento

Es esencial realizar auditorías internas regulares para verificar que las políticas y procedimientos establecidos están siendo correctamente aplicados. Estas evaluaciones deben enfocarse en identificar áreas de mejora y garantizar que todos los controles estén alineados con los estándares internacionales vigentes.

6.3 Programas de simulación de incidentes

Para fortalecer la gestión de incidentes, se sugiere desarrollar simulaciones o ejercicios que permitan a los usuarios y al equipo de TI practicar respuestas ante posibles amenazas. Esto no solo mejora la preparación, sino también incrementa la capacidad de reacción frente a eventos reales.

# 7. Preparación del Manual del SGSI

7.1 Estructura y contenido del manual

El manual del SGSI debe incluir una descripción detallada del alcance del sistema, políticas de seguridad, procedimientos operativos, roles y responsabilidades, así como los controles implementados para mitigar riesgos específicos. Además, debe estar redactado de manera clara y organizada, facilitando su comprensión y aplicación por todas las personas involucradas.

7.2 Inclusión de métricas y KPIs

Es importante incorporar indicadores clave de desempeño (KPIs) y métricas específicas en el manual para evaluar la efectividad del SGSI. Estos indicadores pueden incluir tiempos de respuesta a incidentes, niveles de cumplimiento de políticas, y estadísticas sobre la reducción de riesgos, entre otros.

7.3 Aseguramiento del mantenimiento continuo

El manual debe incluir un apartado dedicado al proceso de mantenimiento continuo del SGSI, detallando cómo se realizarán las revisiones periódicas, las actualizaciones de los procedimientos, y la gestión de cualquier cambio tecnológico o normativo que pueda impactar la seguridad de la organización.

Estructura del manual, políticas clave, roles y responsabilidades, entre otros aspectos.

# 8. Revisión y Presentación del SGSI

* Verificar alineación del alcance, riesgos, controles y políticas.
* Preparar presentación para dirección y partes interesadas.
* Destacar logros y áreas de mejora futura.
* Recoger retroalimentación y ajustar el SGSI.