PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

E.S.E HOSPITAL SAN FÉLIX
LA DORADA – CALDAS
"Atención con Sentido Humano"

AREA DE SISTEMAS Y TECNOLOGIA
DE LA INFORMACIÓN

VIGENCIA
2024

NIT. 810.000.913-8
Teléfonos (6) 839 2000 - Línea Gratuita: 018000941888
Dirección: Calle 12 No. 4-20 La Dorada - Caldas - Colombia
www.hospitalsanfelix.gov.co

Introducción

El Hospital San Félix reconoce la importancia crítica de la seguridad y la privacidad de la información en la atención médica moderna. Dado que el hospital opera con información sensible de pacientes y datos administrativos, es imperativo gestionar y mitigar los riesgos de seguridad y privacidad de la información de manera eficaz. Este plan tiene como objetivo establecer un marco sólido para identificar, evaluar y abordar los riesgos de seguridad y privacidad de la información en todas las sedes y operaciones del Hospital San Félix.

Fase 1: Identificación de Riesgos

- Identificación de Activos Críticos: Enumerar todos los activos de información críticos, incluyendo registros médicos electrónicos, datos de pacientes, datos administrativos y recursos tecnológicos.

- Identificación de Amenazas: Identificar las amenazas potenciales a la seguridad y privacidad de la información, como el acceso no autorizado, el robo de datos, el malware y los desastres naturales.

- Identificación de Vulnerabilidades: Evaluar las vulnerabilidades en la infraestructura tecnológica, procedimientos y prácticas de gestión de la información.

Fase 2: Evaluación de Riesgos

- Análisis de Riesgos: Evaluar la probabilidad y el impacto de cada riesgo identificado. Clasificar los riesgos en función de su gravedad y probabilidad.

Fase 3: Tratamiento de Riesgos

- Desarrollo de Estrategias de Mitigación: Diseñar estrategias de mitigación específicas para cada riesgo, teniendo en cuenta su gravedad y probabilidad. Esto podría incluir la implementación de medidas técnicas, políticas y procedimientos.

- Asignación de Responsabilidades: Designar responsables de la implementación de las estrategias de mitigación y definir un cronograma de implementación.

- Implementación de Controles: Implementar los controles y medidas de seguridad, como sistemas de firewall, cifrado de datos y acceso basado en roles.

- Capacitación del Personal: Proporcionar capacitación regular al personal en prácticas seguras de manejo de datos y conciencia de seguridad.

Fase 4: Monitoreo y Revisión Continua

- Monitoreo de Riesgos: Establecer un sistema de monitoreo continuo para evaluar la efectividad de los controles implementados y detectar nuevas amenazas.

- Evaluación Periódica de Riesgos: Realizar revisiones periódicas de la evaluación de riesgos para adaptarse a cambios en la infraestructura, regulaciones y amenazas emergentes.

- Actualización de Políticas y Procedimientos: Ajustar las políticas y procedimientos de seguridad y privacidad de acuerdo con las lecciones aprendidas y los cambios en el entorno de amenazas.

Fase 5: Respuesta a Incidentes

- Plan de Respuesta a Incidentes: Desarrollar un plan de respuesta a incidentes detallado que incluya procedimientos de notificación, manejo de crisis y recuperación.

- Pruebas de Incidentes Simulados: Realizar ejercicios regulares de simulación de incidentes para garantizar la preparación del personal y la eficacia del plan.

Políticas y Procedimientos Claros:

Establecer políticas y procedimientos de seguridad de la información claros y bien documentados. Estas políticas deben abordar aspectos como el acceso, la autenticación, la gestión de contraseñas, el cifrado y la gestión de incidentes.

Gestión de Acceso:

Implementar un sistema de gestión de acceso basado en roles. Esto garantizará que los usuarios solo tengan los privilegios necesarios para realizar sus funciones.

Cifrado[i] de Datos:

Utilizar cifrado para proteger los datos sensibles en reposo[ii], en tránsito [iii]y en dispositivos móviles[iv]. El cifrado es una herramienta esencial para proteger la información de los ataques cibernéticos.

Actualizaciones y Parches[v]:

Mantener actualizados todos los sistemas y aplicaciones con las últimas actualizaciones y parches de seguridad. Esto ayudará a proteger la información de las vulnerabilidades conocidas.

Firewalls[vi] y Seguridad de Red:

Utilizar firewalls y sistemas de detección de intrusiones para proteger la red interna. Esto ayudará a prevenir los ataques cibernéticos.

Sistemas de Respuesta a Incidentes:

Desarrollar un plan de respuesta a incidentes que detalle los pasos a seguir en caso de una violación de seguridad. Esto ayudará a minimizar el impacto de una violación de seguridad.

Educación y Concienciación:

Capacitar regularmente al personal en prácticas de seguridad de la información y conciencia de seguridad. Esto ayudará a crear una cultura de seguridad en la organización.

Fomentar una cultura de seguridad donde todos los empleados sean responsables de la seguridad de la información.

Respaldo y Recuperación de Datos:

Implementar políticas de respaldo regulares y asegurarnos de que los datos se almacenen de manera segura y se puedan recuperar en caso de pérdida o desastre. Esto ayudará a proteger los datos en caso de un evento disruptivo.

Auditorías y Revisiones de Seguridad:

Realizar auditorías regulares de seguridad de la información para identificar vulnerabilidades y áreas de mejora. Esto ayudará a garantizar que la seguridad de la información sea efectiva.

Cumplimiento Normativo:

Asegurarnos de cumplir con todas las regulaciones y estándares de seguridad de la información aplicables a la atención médica. Esto ayudará a proteger los datos de los pacientes.

Seguridad Física:

Implementar medidas de seguridad física para proteger los activos de información, como el acceso restringido a servidores y centros de datos. Esto ayudará a proteger los datos de los ataques físicos.

Evaluación de Riesgos Continua:

Realizar evaluaciones regulares de riesgos de seguridad de la información para identificar nuevas amenazas y evaluar el estado actual de la seguridad. Esto ayudará a garantizar que la seguridad de la información sea adecuada para el entorno actual.

Colaboración Externa:

Trabajar con proveedores y contratistas externos que cumplan con estándares de seguridad de la información y asegurarnos de que compartan nuestro compromiso con la seguridad de los datos. Esto ayudará a proteger los datos de los ataques provenientes de proveedores externos.

Monitoreo Continuo:

Implementar sistemas de monitoreo continuo para detectar actividad inusual o potencialmente maliciosa en la red. Esto ayudará a prevenir los ataques cibernéticos.

Actualizaciones de Políticas y Entrenamiento:

Mantener actualizadas las políticas de seguridad y brindar entrenamiento recurrente al personal para mantenerlos informados sobre las últimas amenazas y mejores prácticas. Esto ayudará a garantizar que la seguridad de la información sea efectiva a largo plazo.

Conclusiones

Este plan de tratamiento de riesgos de seguridad y privacidad de la información es un compromiso firme del Hospital San Félix para proteger la información sensible y garantizar la confidencialidad, integridad y disponibilidad de los datos. La seguridad de la información es una responsabilidad compartida que requiere la cooperación de todo el personal, desde médicos y enfermeras hasta personal administrativo y técnico. La revisión y actualización periódica de este plan garantizará que el Hospital San Félix continúe brindando atención médica segura y de alta calidad en un entorno cada vez más digitalizado.

Proyecto: Nelson Julián Amaya Giral
Área de Sistemas

[i] Cifrado: Convierte los datos en un formato ilegible que solo puede ser descifrado con una clave.
[ii] En reposo: Los datos en reposo son aquellos que se encuentran almacenados en un dispositivo, como un servidor, una computadora o un disco duro.
iii En tránsito: Los datos en tránsito son aquellos que se están transmitiendo entre dos dispositivos, como cuando se envía un correo electrónico o se accede a una aplicación web.
iv En dispositivos móviles: Los datos en dispositivos móviles son aquellos que se encuentran almacenados en un dispositivo móvil, como un teléfono inteligente o una tableta.
[v] Los parches se utilizan para corregir vulnerabilidades de seguridad. Estas vulnerabilidades pueden ser explotadas por los atacantes para acceder a los sistemas informáticos o robar datos. Los parches suelen ser proporcionados por el fabricante del sistema operativo o el fabricante del software.
[vi] Un firewall es un dispositivo o software que controla el tráfico de red entrante y saliente. Funciona como una especie de filtro, permitiendo el paso del tráfico deseado y bloqueando el tráfico no deseado.