Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) Básico

NYC Health + Hospitals

Paso 1: Selección de la Organización Pública

Para este proyecto, seleccioné NYC Health + Hospitals, un sistema público de salud que maneja una cantidad significativa de datos sensibles, particularmente información de pacientes. Esta organización es compleja, con múltiples centros de atención y hospitales, lo que la convierte en un buen candidato para implementar un SGSI que garantice la protección adecuada de la información.

Justificación:

- NYC Health + Hospitals gestiona datos de salud altamente sensibles (HIPAA).

- La organización dispone de informes anuales y documentación pública sobre sus políticas de privacidad y estrategias de TI, lo que facilita la evaluación.

- La organización tiene múltiples centros físicos y redes que requieren controles tanto físicos como técnicos.

Paso 2: Definición del Alcance del SGSI

Alcance del SGSI

Organización: NYC Health + Hospitals

Propósito del SGSI: El SGSI tiene como objetivo establecer un marco formal para gestionar los riesgos de seguridad de la información y proteger los datos de salud de los pacientes, la infraestructura de TI, y la red de hospitales de NYC Health + Hospitals. Se asegurará que la información confidencial de los pacientes esté protegida contra accesos no autorizados, violaciones de datos, y otros riesgos que comprometan la confidencialidad, integridad y disponibilidad.

El SGSI cubrirá la protección de los datos de salud de los pacientes y la infraestructura tecnológica en todas las instalaciones de NYC Health + Hospitals. Se aplicará a todos los sistemas que almacenan, procesan o transmiten información de salud protegida (PHI), incluyendo servidores, bases de datos, redes, y dispositivos de los empleados.

Activos a proteger:

- Datos de pacientes (historias clínicas electrónicas, datos personales).

- Equipos de TI (servidores, bases de datos, estaciones de trabajo).

- Redes (redes internas, VPN, sistemas de comunicación).

- Software crítico (sistemas de administración de hospitales, aplicaciones de salud).

Límites físicos:

- Centros de salud y hospitales bajo el control de NYC Health + Hospitals.

- Áreas de acceso restringido como salas de servidores y laboratorios clínicos.

Límites virtuales:

- Redes internas y en la nube utilizadas para el almacenamiento y transmisión de datos.

- Sistemas conectados a bases de datos que contienen PHI.

Partes interesadas:

- Equipo de TI.

- Dirección y gerencia hospitalaria.

- Personal médico.

- Pacientes.

Paso 3: Evaluación de Riesgos

Evaluación de Riesgos

1. Identificación de activos:

- **Hardware:** Servidores, estaciones de trabajo, dispositivos móviles, dispositivos médicos conectados.
- **Software:** Sistemas de gestión de historias clínicas (HCE), aplicaciones de facturación médica, sistemas de comunicación interna.
- **Datos:** Historias clínicas electrónicas (HCE), datos de identificación de pacientes, resultados de exámenes y diagnósticos, datos financieros de pacientes.
- **Personal:** Doctores, enfermeros, equipo administrativo, equipo de TI, consultores de ciberseguridad externos.

2. Amenazas identificadas:

- Acceso no autorizado a las historias clínicas de los pacientes.
- Malware, ransomware y otros ataques de software malicioso.
- Pérdida de dispositivos móviles que contienen datos sensibles.
- Violación de datos personales debido a errores humanos (e.g., envío incorrecto de información a terceros no autorizados).
- Ataques de denegación de servicio (DoS) que podrían afectar la disponibilidad de los sistemas de salud.

3. Vulnerabilidades identificadas:

- Sistemas sin actualizaciones de seguridad.
- Uso de contraseñas débiles o compartidas.
- Falta de autenticación multifactor (MFA) en algunos sistemas.
- Dispositivos móviles sin cifrado que contienen datos de pacientes.
- Red interna con segmentación insuficiente que permite el acceso no restringido a datos sensibles.

Evaluación de probabilidad e impacto:

- Alta probabilidad: acceso no autorizado debido a credenciales comprometidas.

- Impacto alto: compromiso de datos de pacientes puede llevar a multas por incumplimiento de HIPAA y pérdida de reputación.

Priorización de riesgos:

1. Riesgo alto: accesos no autorizados y vulnerabilidades en sistemas críticos.

2. Riesgo medio: malware y ransomware.

3. Riesgo bajo: desastres naturales (pero con impacto alto).

Evaluación de riesgos (ejemplos):

Riesgo	**Probabilidad**	**Impacto**	**Nivel de riesgo**
Acceso no autorizado a HCE	Alta	Alto	Alto
Ataques de ransomware	Media	Alto	Alto
Pérdida de dispositivos móviles	Media	Medio	Medio
Violación de datos personales	Baja	Alto	Medio
Ataques DoS	Baja	Alto	Medio

Paso 4: Selección de Controles

Controles seleccionados:

1. Autenticación multifactor para todos los sistemas que manejan datos de pacientes.

2. Cifrado de datos en tránsito y en reposo, especialmente para PHI.

3. Firewalls y sistemas de detección de intrusos (IDS) para proteger las redes hospitalarias.

4. Actualización regular de sistemas y parches de seguridad automáticos.

5. Capacitación continua del personal sobre seguridad de la información y el uso adecuado de dispositivos.

<Normas de referencia: ISO/IEC 27001, NIST>

Lista de Controles (basado en NIST)

Basados en el **NIST SP 800-53**, los controles de seguridad que se seleccionarán para mitigar los riesgos incluyen:

Control de Acceso (AC):

- **AC-2: Control de cuentas de usuario:** Implementar revisiones periódicas de las cuentas de usuario y limitar el acceso basado en roles.
- **AC-17: Acceso remoto:** Asegurar que las conexiones remotas se realicen a través de VPN cifrada y MFA.

Control de Identificación y Autenticación (IA):

- **IA-2: Autenticación multifactor:** Requerir autenticación multifactor para todo acceso a los sistemas que contengan datos de salud sensibles.
- **IA-5: Gestión de contraseñas:** Establecer políticas de contraseñas fuertes y su rotación periódica.

Control de Protección de la Información (SC):

- **SC-13: Cifrado de datos en reposo:** Implementar cifrado para toda la información almacenada en los sistemas.
- **SC-28: Protección de la información sensible:** Asegurarse de que todos los datos sensibles estén cifrados tanto en tránsito como en reposo.

Control de Auditoría y Monitoreo (AU):

- **AU-2: Auditoría de eventos:** Monitorear y auditar el acceso a sistemas y registros médicos para detectar cualquier actividad sospechosa.

- **AU-6: Análisis de auditorías:** Revisar periódicamente los registros de auditoría para identificar patrones inusuales de acceso.

Control de Respuesta a Incidentes (IR):

- **IR-4: Respuesta a incidentes:** Implementar un plan formal para la respuesta a incidentes, que incluya notificación, análisis, contención y recuperación.
- **IR-6: Informe de incidentes:** Establecer procedimientos para informar incidentes de seguridad a las partes interesadas en un plazo determinado.

Control de Capacitación y Concienciación (AT):

- **AT-2: Capacitación de seguridad:** Proporcionar capacitación continua sobre seguridad de la información a todos los empleados, incluidos los riesgos de phishing y manejo seguro de información.

Control de Recuperación de Contingencias (CP):

- **CP-9: Copias de seguridad de la información:** Realizar copias de seguridad diarias de los datos críticos y verificar su restauración periódica.

Lista de Controles Basados en ISO/IEC 27001

A.5: Políticas de Seguridad de la Información

- **A.5.1.1 Política de Seguridad de la Información:** Se debe establecer y mantener una política documentada de seguridad de la información que refleje el compromiso de la organización con la seguridad y protección de datos sensibles, como las historias clínicas de los pacientes.

A.6: Organización de la Seguridad de la Información

- **A.6.1.1 Roles y responsabilidades de la seguridad de la información:** Definir claramente los roles y responsabilidades de la seguridad, tanto para el equipo de TI, como para el personal médico y administrativo.
- **A.6.2.1 Movilidad de los dispositivos:** Definir una política de uso de dispositivos móviles que incluya requisitos de cifrado y controles de acceso para aquellos que accedan a datos sensibles desde dispositivos móviles.

A.7: Seguridad en Recursos Humanos

- **A.7.2.2 Términos y condiciones de empleo:** Asegurar que todos los empleados, antes de obtener acceso a los sistemas de información sensibles, firmen acuerdos de confidencialidad.

A.8: Gestión de Activos

- **A.8.1.1 Inventario de activos:** Mantener un inventario de todos los activos de información, incluidas las bases de datos de pacientes, servidores, estaciones de trabajo y dispositivos móviles.

- **A.8.2.1 Clasificación de la información:** Clasificar la información según su sensibilidad (por ejemplo, información médica confidencial, información pública).
- **A.8.3.1 Gestión de medios:** Implementar controles para la eliminación segura de medios que contengan información sensible (e.g., discos duros, USBs).

A.9: Control de Acceso

- **A.9.1.1 Política de control de acceso:** Definir una política de control de acceso que regule el acceso basado en roles (RBAC) y asegure que los empleados solo tengan acceso a los datos necesarios para sus funciones.
- **A.9.2.2 Gestión de acceso de usuarios:** Revisar regularmente los permisos de acceso de los usuarios para asegurar que sean consistentes con sus responsabilidades.
- **A.9.4.2 Autenticación segura:** Implementar autenticación multifactor (MFA) para el acceso a sistemas sensibles, como las historias clínicas electrónicas (HCE).

A.10: Criptografía

- **A.10.1.1 Política de uso de controles criptográficos:** Establecer una política para el uso de criptografía, que incluya el cifrado de datos en reposo y en tránsito para las historias clínicas electrónicas y otros datos sensibles.

A.11: Seguridad Física y del Entorno

- **A.11.1.1 Áreas seguras:** Definir zonas de acceso restringido, como salas de servidores y áreas donde se gestionan datos sensibles.
- **A.11.2.1 Protección de equipos:** Implementar medidas de protección física para los equipos, como servidores y dispositivos de almacenamiento, garantizando que estén en ubicaciones seguras y con acceso controlado.

A.12: Seguridad en las Operaciones

- **A.12.3.1 Gestión de copias de seguridad:** Asegurar que se realicen copias de seguridad periódicas de los datos sensibles y que estas se prueben regularmente para verificar su integridad.
- **A.12.4.1 Registro de eventos:** Implementar un sistema de auditoría y monitoreo de los eventos que afecten a los sistemas de información críticos, como los registros de acceso a las HCE.

A.13: Seguridad en las Comunicaciones

- **A.13.1.1 Protección de la información en tránsito:** Cifrar los datos sensibles mientras se transmiten a través de la red, especialmente cuando se trate de información de pacientes.
- **A.13.2.1 Acuerdos de confidencialidad:** Implementar acuerdos de confidencialidad y compartir la información con terceros solo cuando sea necesario y siguiendo estrictos protocolos de seguridad.

A.14: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- **A.14.1.2 Seguridad en el ciclo de vida de desarrollo:** Asegurar que la seguridad esté integrada en todas las fases del desarrollo de sistemas de información, incluyendo las aplicaciones utilizadas para la gestión de historias clínicas.

A.15: Relaciones con Proveedores

- **A.15.1.1 Política de seguridad con proveedores:** Establecer controles de seguridad rigurosos para los proveedores de servicios, asegurando que los contratos incluyan cláusulas de confidencialidad y protección de datos.

A.16: Gestión de Incidentes de Seguridad de la Información

- **A.16.1.1 Responsabilidad de la gestión de incidentes:** Implementar un procedimiento documentado para la gestión de incidentes de seguridad, incluyendo la notificación y resolución rápida de brechas de datos.

A.17: Aspectos de Seguridad de la Continuidad del Negocio

- **A.17.1.2 Planificación de la continuidad del negocio:** Establecer planes de contingencia y continuidad del negocio que aseguren que los sistemas críticos de salud puedan seguir operando en caso de una interrupción (por ejemplo, por ataques cibernéticos o desastres naturales).

A.18: Cumplimiento

- **A.18.1.4 Privacidad y protección de datos personales:** Asegurarse de que todos los datos personales se manejen de acuerdo con las regulaciones de privacidad, como la HIPAA en los Estados Unidos.
- **A.18.2.3 Auditoría independiente:** Realizar auditorías periódicas del SGSI para verificar el cumplimiento de las normativas y la efectividad de los controles de seguridad implementados.

Cada control será documentado con detalle, incluyendo la implementación y los responsables de su administración (por ejemplo, el equipo de TI supervisará la autenticación multifactor y el cifrado).

Paso 5: Documentación de Políticas y Procedimientos de Seguridad

Políticas y Procedimientos de Seguridad

Política de Seguridad de la Información:

Esta política establece el compromiso de NYC Health + Hospitals con la protección de la confidencialidad, integridad y disponibilidad de los datos de salud de los pacientes. Todos los empleados deben seguir los procedimientos establecidos para garantizar la seguridad de la información.

Política de Control de Acceso:

El acceso a la información sensible se concederá bajo el principio de menor privilegio. Los permisos de acceso se revisarán periódicamente, y se aplicarán autenticaciones multifactor en sistemas críticos.

Política de Gestión de Incidentes:

Define el proceso para identificar, notificar y responder a incidentes de seguridad de la información. Todos los incidentes deben ser reportados inmediatamente al equipo de seguridad, que será responsable de la investigación y mitigación.

Política de Uso de Dispositivos Móviles:

Los dispositivos móviles que acceden a datos sensibles deben estar protegidos con cifrado y contraseñas robustas. Está prohibido almacenar datos de pacientes en dispositivos móviles no autorizados.

Procedimientos de Copia de Seguridad y Recuperación:

Se realizarán copias de seguridad de los sistemas críticos a diario, y se verificarán mediante pruebas de restauración regulares para garantizar su integridad y disponibilidad.

Procedimientos de Control de Contraseñas:

Las contraseñas deben tener una longitud mínima de 12 caracteres y cumplir con los requisitos de complejidad. Las contraseñas deben cambiarse cada 90 días y no reutilizarse.

Paso 6: Preparar el Manual de SGSI

Manual del SGSI para NYC Health + Hospitals

Capítulo 1: Introducción y Objetivos del SGSI

El SGSI está diseñado para proteger los activos de información de NYC Health + Hospitals. Este sistema garantiza que los datos de salud estén protegidos mediante la aplicación de controles y políticas de seguridad.

Capítulo 2: Alcance del SGSI

El SGSI abarca todas las instalaciones físicas y sistemas tecnológicos utilizados por NYC Health + Hospitals para gestionar la información de los pacientes.

Capítulo 3: Evaluación de Riesgos

El proceso de evaluación de riesgos identifica amenazas, vulnerabilidades y riesgos para los activos de información. Se priorizan los riesgos altos como el acceso no autorizado y los ataques de ransomware.

Capítulo 4: Controles de Seguridad Implementados

Se detallan los controles seleccionados según las normativas NIST, incluyendo el cifrado de datos, autenticación multifactor, y auditorías regulares.

Capítulo 5: Políticas de Seguridad

Este capítulo recoge las políticas clave, como la política de control de acceso, gestión de contraseñas, uso de dispositivos móviles, y copias de seguridad.

Capítulo 6: Respuesta a Incidentes

Describe el procedimiento a seguir en caso de un incidente de seguridad, incluyendo la notificación a las partes interesadas y las medidas correctivas a implementar.

Capítulo 7: Concienciación y Capacitación del Personal

El manual detalla las sesiones de capacitación periódicas sobre ciberseguridad y mejores prácticas, con un enfoque en la prevención de ataques de phishing y el manejo de datos sensibles.

Resumen del Enfoque del Sistema de Gestión de Seguridad de la Información (SGSI) para NYC Health + Hospitals

Enfoque General:

El desarrollo del **SGSI** para **NYC Health + Hospitals** tiene como objetivo proteger la información sensible de los pacientes y garantizar el cumplimiento normativo, como la HIPAA. El SGSI sigue un enfoque basado en la **ISO/IEC 27001**, aplicando controles específicos para la identificación, mitigación y gestión de riesgos de seguridad de la información en la organización. Este enfoque incluye la evaluación de riesgos, la implementación de controles, y la creación de políticas y procedimientos para asegurar la confidencialidad, integridad y disponibilidad de los datos.

Hallazgos Clave:

1. **Exposición a Riesgos por Acceso No Autorizado:** Se identificaron vulnerabilidades relacionadas con el acceso no controlado a las bases de datos de pacientes y sistemas médicos críticos. Esto podría derivar en filtraciones de datos sensibles, comprometiendo la privacidad y el cumplimiento normativo.
2. **Amenazas Internas y Externas:** Existe una alta probabilidad de incidentes relacionados con errores humanos (por ejemplo, uso indebido de contraseñas), ataques externos (ciberataques) y amenazas internas (empleados descontentos).
3. **Falta de Políticas Criptográficas Rigurosas:** Si bien se utilizan medidas de seguridad básicas, no se implementa el cifrado en todas las comunicaciones y almacenamiento de datos sensibles.
4. **Carencia de Planes de Continuidad del Negocio:** La organización no cuenta con un plan robusto de continuidad del negocio, lo que representa un riesgo elevado en caso de desastres naturales o interrupciones operativas.

5. **Gestión Deficiente de Proveedores:** Los acuerdos con terceros carecen de cláusulas de seguridad rigurosas, lo que expone a la organización a riesgos derivados de la relación con proveedores que tienen acceso a información sensible.

Recomendaciones:

1. **Implementar Autenticación Multifactor (MFA):** Se debe habilitar MFA para todos los empleados que acceden a sistemas críticos, reduciendo la probabilidad de accesos no autorizados debido a contraseñas comprometidas.
2. **Cifrado de Datos Sensibles:** Implementar el cifrado de datos tanto en tránsito como en reposo, especialmente para las historias clínicas electrónicas y datos personales de los pacientes.
3. **Desarrollar un Plan de Continuidad del Negocio:** Crear un plan integral de continuidad y recuperación ante desastres, asegurando que los servicios críticos sigan operativos durante interrupciones o incidentes.
4. **Fortalecer la Gestión de Proveedores:** Revisar y actualizar los acuerdos con terceros para incluir cláusulas de seguridad de la información que aseguren que los proveedores cumplen con los mismos estándares que la organización.
5. **Capacitación y Concienciación del Personal:** Desarrollar un programa de concienciación y capacitación en seguridad de la información para todos los empleados, promoviendo buenas prácticas de ciberseguridad y minimizando los errores humanos.
6. **Monitoreo y Auditoría Continuos:** Implementar un sistema de auditoría regular para evaluar la efectividad de los controles de seguridad y realizar ajustes conforme a las nuevas amenazas o vulnerabilidades identificadas.

Conclusión:

El **SGSI** diseñado para NYC Health + Hospitals proporcionará una sólida estructura de seguridad de la información, protegiendo los datos sensibles de los pacientes y asegurando el cumplimiento normativo. La implementación de controles más estrictos, como el cifrado, la autenticación multifactor y la gestión de proveedores, mitigará los principales riesgos identificados. Al mismo tiempo, el desarrollo de planes de continuidad y capacitación garantizará la resiliencia de la organización frente a amenazas tanto internas como externas.