Desarrollo de un Sistema Básico de

Gestión de Seguridad de la

Información (SGSI) para una Organización Pública:

# 4 GEEKS

Fecha: 06/02/2025

Presentado por: Jesús Castaño Martínez

Fuente de información principal:

## https://4geeks.com/

La empresa seleccionada para este proyecto es 4geeks dedicada a la formación, por las siguientes razones:

* Manejo de datos sensibles: Datos personales y operativos.
* Cumplimiento regulatorio: GDPR (Reglamento General de Protección de Datos), NIS (Reglamento de Seguridad de Redes y Sistemas de Información) y otros estándares específicos de salud.

Definición del Alcance del Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI de 4 Geeks tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información crítica de salud, cumpliendo con los requisitos regulatorios como GDPR y NIS y estableciendo un marco estructurado para proteger los activos de información críticos. Se enfoca en mitigar riesgos, garantizar el cumplimiento y promover la seguridad en toda la organización. El alcance abarca todos los activos digitales, sistemas de información y procesos relacionados con el manejo de datos de pacientes y operativos.

El SGSI cubrirá los siguientes aspectos:

1. Activos de información:

* Computadoras y dispositivos: Equipos utilizados por el personal administrativo y clínico.
* Servidores y bases de datos: Infraestructura de TI que almacena y procesa información de pacientes y datos operativos.
* Aplicaciones y sistemas: Portales digitales, sistemas de registro electrónico de alumnos.
* Datos sensibles: Información de alumnos.

2. Clasificación de activos por importancia:

* Crítico: Servidor de aplicaciones, bases de datos.
* Alto: Sistemas de diagnóstico, redes locales.
* Medio: Equipos de oficina, sistemas de respaldo.

3. Ubicaciones físicas incluidas:

* Centros de datos nacionales y regionales.
* Oficinas administrativas.

4. Áreas de acceso restringido:

* Salas de servidores.
* Áreas de almacenamiento de datos confidenciales.

5. Redes y entornos incluidos:

* Redes internas de 4 GEEKS.
* Infraestructura en la nube utilizada para aplicaciones y almacenamiento. - Máquinas virtuales que alojan sistemas de información.

6. Sistemas y tipos de datos bajo control del SGSI:

* Sistemas de gestión de alumnos.
* Datos personales - Registros financieros y operativos.

7. Partes interesadas clave y sus responsabilidades:

* Equipo de TI: Responsable de la implementación técnica de controles de seguridad, monitoreo continuo y respuesta a incidentes.
* Gestores de datos y de seguridad: Aseguran el cumplimiento de las políticas de privacidad, evaluación de riesgos y actualización del SGSI.
* Personal administrativo y docente: Usuarios finales que manejan información sensible.
* Dirección: Revisión y aprobación de políticas.

Metas y objetivos del SGSI:

* Garantizar la protección de datos sensibles contra accesos no autorizados.
* Reducir la probabilidad e impacto de incidentes de seguridad.
* Cumplir con las normativas aplicables, como GDPR y NIS.
* Fomentar una cultura de seguridad de la información entre el personal.

Limitaciones y exclusiones:

* Redes Wi-Fi públicas no gestionadas por 4 GEEKS.
* Equipos legados desconectados de la red principal.

Evaluación de Riesgos para 4 Geeks Academy

1. Lista de activos identificados:

Hardware:

* + Servidor de aplicaciones.
  + Computadoras de escritorio y portátiles.
  + Equipos de almacenamiento en red (NAS).
  + Dispositivos de red (routers, switches).
  + Equipos móviles (tabletas, teléfonos inteligentes).

Software:

* + Sistemas de gestión de Alumnos.
  + Campus virtual.
  + Bases de datos (MySql).
  + Sistemas operativos (Linux).
  + Soluciones de seguridad (antivirus, firewalls).

Datos:

* + Información personal de empleados. - Informes financieros y operativos.

Personal:

* + Equipo de TI.
  + Personal administrativo. - Profesores y alumnos.

1. Potenciales amenazas identificadas:

Hardware:

* + Acceso no autorizado a servidores.
  + Robo o pérdida de dispositivos portátiles. - Fallos técnicos o averías.

Software:

* + Malware y ransomware.
  + Vulnerabilidades en aplicaciones desactualizadas. - Configuraciones incorrectas de sistemas.

Datos:

* + Violaciones de datos sensibles.
  + Pérdida de datos por falta de copias de seguridad.
  + Exposición de datos debido a errores humanos.

Personal:

* + Errores operativos por falta de capacitación.
  + Amenazas internas (empleados descontentos). - Phishing y ataques de ingeniería social.

1. Vulnerabilidades y explotación potencial:

|  |  |  |
| --- | --- | --- |
| Activo | Vulnerabilidad | Explotación Potencial |
| Servidores | Sistemas desactualizados | Acceso no autorizado, violación de datos. |
| Bases de datos | Falta de cifrado en reposo | Robo de datos sensibles por atacantes externos. |
| Dispositivos móviles | Contraseñas débiles | Acceso no autorizado a datos corporativos. |
| Personal | Falta de capacitación en seguridad | Clicks en enlaces de phishing, comprometiendo sistemas. |

1. Evaluación de Riesgos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Riesgo Identificado | Probabilidad | Impacto | Calificación  Riesgo | del |
| Acceso no autorizado a servidores | Alta | Crítico | Alto |  |
| Malware en aplicaciones | Media | Alto | Alto |  |
| Robo de dispositivos móviles | Media | Medio | Medio |  |
| Violaciones de datos por errores humanos | Alta | Alto | Alto |  |
| Phishing dirigido al personal | Alta | Alto | Alto |  |

1. Priorización de Riesgos:
   1. Acceso no autorizado a servidores.
   2. Violaciones de datos por errores humanos.
   3. Phishing dirigido al personal.
   4. Malware en aplicaciones.
   5. Robo de dispositivos móviles.

La evaluación de riesgos para 4 GEEKS identifica riesgos significativos que requieren atención inmediata, particularmente aquellos relacionados con el acceso no autorizado, phishing y errores humanos. Estos riesgos serán priorizados para la implementación de controles de seguridad adecuados, como autenticación multifactor, capacitación en seguridad y actualizaciones regulares de sistemas.

Selección de controles de seguridad apropiados para mitigar los riesgos identificados

Dado que hemos priorizado ciertos riesgos en la etapa anterior, vamos a asociar controles de seguridad relevantes para cada uno de ellos. Algunos controles que podríamos implementar para cada riesgo priorizado son los siguientes:

* + 1. Acceso no autorizado a servidores
* Autenticación multifactor (MFA)
* Implementar MFA para acceder a servidores críticos o aplicaciones sensibles. Esto ayuda a reducir el riesgo de acceso no autorizado, ya que requiere más de una forma de verificación (por ejemplo, contraseña y código enviado a un dispositivo móvil).
* Control de acceso basado en roles (RBAC)
* Asegurar que solo los usuarios autorizados puedan acceder a datos o sistemas críticos. Asignar roles específicos y asegurarse de que los usuarios solo tengan acceso a lo que necesitan para realizar su trabajo.
* Cifrado de datos en tránsito y reposo
* Cifrar los datos tanto cuando están en tránsito (al ser enviados a través de redes) como cuando están almacenados en servidores. Esto protege la información incluso si los atacantes logran acceder a los servidores.
* Auditoría y monitoreo
* Implementar un sistema de auditoría para registrar y monitorear los accesos a los servidores. Esto ayuda a detectar cualquier actividad sospechosa en tiempo real y tomar medidas correctivas rápidamente.

Normativa aplicable:

* + - * Control ISO/IEC 27001: A.9 Control de acceso. Este control establece que se deben definir procedimientos y criterios para gestionar el acceso a la información, incluyendo autenticación multifactor (MFA) y control de privilegios.
      * Control NIST: AC-1 (Access Control Policy and Procedures). NIST recomienda establecer políticas y procedimientos de control de acceso a los sistemas de información, con controles estrictos sobre el acceso basado en el rol y la autenticación fuerte.
      * Control CIS: CIS Control 4 (Controlled Use of Administrative Privileges). Requiere que el acceso a privilegios administrativos sea restringido y monitoreado de manera rigurosa.
      * Regulación GDPR: El acceso no autorizado a datos personales es una violación del principio de Confidencialidad del GDPR, que exige la implementación de controles de acceso adecuados y la protección de datos personales.

* + 1. Violaciones de datos por errores humanos
* Capacitación en ciberseguridad para empleados
* Ofrecer formación regular sobre cómo manejar información sensible, reconocer correos electrónicos de phishing, y las mejores prácticas para proteger la confidencialidad de los datos.
* Gestión de contraseñas
* Implementar políticas de contraseñas seguras que requieran complejidad (por ejemplo, mínimo de caracteres, uso de mayúsculas y números) y rotación periódica de contraseñas.
* Herramientas de prevención de pérdida de datos (DLP)
* Implementar software de DLP para evitar que datos sensibles sean enviados por error fuera de la red de 4 Geeks Academy, ya sea por correo electrónico o a través de otros canales.

Normativa aplicable:

* + - Control ISO/IEC 27001: A.7 Conciencia y formación en seguridad. Este control subraya la importancia de la capacitación y concienciación del personal en cuanto a la seguridad de la información, para reducir el riesgo de errores humanos.
    - Control NIST: AT-2 (Security Awareness Training). NIST enfatiza la necesidad de proporcionar formación periódica en seguridad a todos los empleados, con especial atención en la protección de datos sensibles.
    - Control CIS: CIS Control 17 (Security Awareness and Skills Training). CIS recomienda la implementación de programas de formación continua para que el personal esté actualizado sobre las mejores prácticas de seguridad.
    - Regulación GDPR: El GDPR exige que las organizaciones implementen controles adecuados para evitar la exposición no intencionada de datos personales, lo que se logra mediante la formación adecuada del personal.
    1. Riesgo: Phishing dirigido al personal

Filtro de correos electrónicos y detección de phishing: Utilizar soluciones de filtrado de correos electrónicos para bloquear mensajes de phishing conocidos y entrenar a los empleados para identificar posibles correos maliciosos, mediante campañas periódicas de simulación de phishing para sensibilizar al personal sobre las técnicas de ingeniería social.

Esto ayudará a que los empleados estén mejor preparados para reconocer intentos de fraude.

Normativa aplicable:

* + - * Control ISO/IEC 27001: A.13 Comunicaciones y operaciones de seguridad. Este control establece que deben implementarse controles de seguridad para proteger las comunicaciones y prevenir ataques de ingeniería social, como el phishing.
      * Control NIST: IR-4 (Incident Handling). NIST sugiere la implementación de políticas para detectar y mitigar ataques de phishing, como la creación de un proceso claro de respuesta ante incidentes.
      * Control CIS: CIS Control 17 (Security Awareness and Skills Training). CIS también recomienda entrenar al personal para identificar intentos de phishing y proporcionarles herramientas para reportar dichos incidentes.
      * Regulación NIS: La Directiva NIS exige que las organizaciones implementen controles de seguridad para protegerse contra amenazas externas, incluyendo el phishing.
    1. Malware en aplicaciones
    - Soluciones antivirus y antimalware
    - Instalar software antivirus y antimalware en todos los dispositivos que manejen información sensible, incluyendo servidores y dispositivos móviles.
    - Actualizaciones regulares de software y parches
    - Asegurar que todos los sistemas operativos, aplicaciones y bases de datos estén actualizados con los últimos parches de seguridad para reducir las vulnerabilidades explotables.
    - Sandboxing para aplicaciones críticas
    - Implementar entornos controlados (sandboxing) para ejecutar aplicaciones de alto riesgo, como aquellas que manejan datos de pacientes, para evitar que el malware se propague.

Normativa aplicable:

* + - Control ISO/IEC 27001: A.12 Operaciones de seguridad. Este control cubre la implementación de medidas para detectar y prevenir malware, como el uso de software antivirus actualizado.
    - Control NIST: SI-3 (Malicious Code Protection). NIST recomienda utilizar soluciones de software para la detección de malware y establecer políticas para la actualización continua de las firmas de virus.
    - Control CIS: CIS Control 8 (Malware Defenses). Este control enfatiza la implementación de herramientas para detectar, prevenir y responder a incidentes de malware.
    - Regulación NIS: La Directiva NIS requiere que las organizaciones implementen medidas para proteger los sistemas de información contra incidentes de seguridad, como malware y otras amenazas cibernéticas.

* + 1. Robo de dispositivos móviles
  + Cifrado de dispositivos móviles

Asegurar que todos los dispositivos móviles utilizados por el personal estén cifrados para proteger los datos en caso de pérdida o robo.

* + Gestión de dispositivos móviles (MDM)

Implementar una solución MDM para gestionar de manera centralizada los dispositivos móviles, incluyendo la capacidad de borrar remotamente los datos si un dispositivo se pierde o es robado.

* + Políticas de uso de dispositivos móviles (BYOD)

Establecer políticas claras sobre el uso de dispositivos personales para acceder a información de 4 Geeks Academy, y asegurarse de que cumplan con los requisitos de seguridad.

Normativa aplicable:

* + - Control ISO/IEC 27001: A.11 Seguridad física y del entorno. Este control establece la necesidad de proteger los dispositivos móviles mediante encriptación y políticas de gestión de dispositivos móviles (MDM).
    - Control NIST: AC-19 (Access Control for Mobile Devices). NIST sugiere la implementación de controles de acceso estrictos para dispositivos móviles, como el uso de contraseñas robustas y el cifrado de datos.
    - Control CIS: CIS Control 3 (Data Protection). CIS recomienda implementar cifrado para proteger los datos en dispositivos móviles y limitar su uso a personas autorizadas.
    - Regulación GDPR: El GDPR exige que los datos personales sean protegidos en tránsito y en reposo, lo que implica el uso de cifrado en dispositivos móviles.

Documentación y plan de implementación de los controles seleccionados

A continuación, es importante documentar cada uno de los controles seleccionados, incluyendo la forma en que se mitigarán los riesgos, los responsables de implementarlos y los recursos necesarios, así como elaborar un plan de implementación que detalle cronogramas y recursos necesarios para la implementación de controles:

Control 1: Autenticación Multifactor (MFA)

Riesgo Mitigado: Acceso no autorizado a servidores

|  |  |
| --- | --- |
| Elemento | Detalle |
| Cronograma de  Implementación | 3 meses |
| Responsable de  Implementación | Equipo de TI |
| Recursos Necesarios | Herramientas MFA (ej. Google Authenticator, Microsoft Authenticator), personal de TI para implementación. |
| Dependencias | * Necesidad de actualización de las plataformas existentes (si es necesario). * Capacitación del personal sobre el uso de MFA. |
| Monitoreo y Evaluación | * Realizar auditorías mensuales de acceso. * Medir la tasa de autenticación fallida y errores. |

Control 2: Control de Acceso Basado en Roles (RBAC)

Riesgo Mitigado: Acceso no autorizado a sistemas críticos

|  |  |
| --- | --- |
| Elemento | Detalle |
| Cronograma de  Implementación | 2 meses |
| Responsable de  Implementación | Equipo de TI, administradores de sistemas y bases de datos |
| Recursos Necesarios | Herramientas de gestión de accesos, software de gestión de identidades y accesos (IAM). |
| Dependencias | - Revisión de los roles y permisos existentes en los sistemas. |
| Monitoreo y Evaluación | * Revisión mensual de las políticas de acceso. * Auditorías trimestrales de acceso a sistemas críticos. |

Control 3: Capacitación en Ciberseguridad para Empleados Riesgo Mitigado: Violaciones de datos por errores humanos

|  |  |
| --- | --- |
| Elemento | Detalle |
| Cronograma de  Implementación | 1 mes para el desarrollo de los materiales y 2 meses para el entrenamiento inicial. |
| Elemento | Detalle |
| Responsable de  Implementación | Departamento de Recursos Humanos, Equipo de Seguridad de la Información |
| Recursos Necesarios | Plataforma de formación en línea (LMS), materiales de formación (videos, presentaciones), presupuesto para contratación de expertos si es necesario. |
| Dependencias | - Identificación de temas clave para capacitación. - Selección de plataforma de formación. |
| Monitoreo y  Evaluación | - Evaluaciones de conocimiento post-capacitación. - Encuestas de satisfacción de los empleados. |

Control 4: Ejercicios regulares de simulación de phishing para sensibilizar al personal.

Riesgo Mitigado: Phishing dirigido al personal

|  |  |
| --- | --- |
| Elemento | Detalle |
| Cronograma de  Implementación | Iniciar en el primer mes y realizar simulaciones trimestrales a lo largo del año. |
| Responsable de  Implementación | Equipo de TI, Equipo de Seguridad, Departamento de  Recursos Humanos |
| Recursos Necesarios | Herramienta de simulación de phishing (ej. KnowBe4), personal de TI para gestionar las simulaciones. |
| Dependencias | * Evaluación de la disposición del personal a recibir simulaciones. * Establecimiento de un plan de seguimiento postsimulación. |
| Monitoreo y Evaluación | * Análisis de tasas de éxito en simulaciones. * Seguimiento de las correcciones de comportamiento. |

Control 5: Cifrado de Dispositivos Móviles

Riesgo Mitigado: Robo de dispositivos móviles

|  |  |
| --- | --- |
| Elemento | Detalle |
| Cronograma de  Implementación | 2 meses |
| Elemento | Detalle |
| Responsable de  Implementación | Departamento de TI, Equipo de Seguridad |
| Recursos Necesarios | Software de cifrado de dispositivos (ej. BitLocker, FileVault), personal de TI. |
| Dependencias | - Determinar qué dispositivos necesitan cifrado (todos los dispositivos móviles de la organización). |
| Monitoreo y Evaluación | * Revisar que el cifrado se esté aplicando correctamente en todos los dispositivos. * Auditorías anuales para asegurar que todos los dispositivos estén cifrados. |

Control 6: Actualizaciones Regulares de Software y Parches

Riesgo Mitigado: Malware en aplicaciones

|  |  |
| --- | --- |
| Elemento | Detalle |
| Cronograma de  Implementación | Implementación continua (parches regulares cada mes). |
| Responsable de  Implementación | Equipo de TI |
| Recursos Necesarios | Herramientas de gestión de parches, personal de TI para aplicar las actualizaciones. |
| Dependencias | - Revisión de las políticas de actualización de software. - Integración de un sistema de gestión de parches. |
| Monitoreo y Evaluación | - Revisar cada mes si todos los sistemas han recibido las actualizaciones correspondientes. |

Control 7: Sandboxing para Aplicaciones Críticas: Asegurarse de que todos los sistemas estén actualizados con parches de seguridad.

Riesgo Mitigado: Malware en aplicaciones

|  |  |
| --- | --- |
| Elemento | Detalle |
| Cronograma de  Implementación | 3 meses para la implementación y prueba. |
| Elemento | Detalle |
| Responsable de  Implementación | Equipo de TI, Equipo de Seguridad. |
| Recursos Necesarios | Software de sandboxing (ej. Bromium, Cyberbit), servidores y recursos para pruebas. |
| Dependencias | - Evaluación de las aplicaciones críticas para determinar cuáles deben ejecutarse en sandbox. |
| Monitoreo y Evaluación | * Revisión trimestral del funcionamiento de las aplicaciones en sandbox. * Auditorías de seguridad anuales. |

Documentación de Políticas y Procedimientos de Seguridad del 4 Geeks Academy

4 GEEKS se compromete a proteger la confidencialidad, integridad y disponibilidad de la información que maneja, garantizando el cumplimiento de las leyes y regulaciones aplicables, incluidos el GDPR y el Reglamento de Seguridad de Redes y Sistemas de Información (NIS). Esta política define el marco para proteger los activos de información y establecer prácticas de seguridad claras que mitiguen los riesgos y aseguren la continuidad de las operaciones.

Principios de la Política de Seguridad:

* Confidencialidad: Garantizar que la información sensible solo sea accesible para aquellos que tienen autorización legítima.
* Integridad: Asegurar que la información sea precisa, completa y que no haya sido alterada sin autorización.
* Disponibilidad: Asegurar que la información esté disponible para los usuarios autorizados cuando sea necesario.

Alcance:

Esta política aplica a todos los empleados, contratistas y terceros que tengan acceso a la infraestructura de tecnología de la información de 4 GEEKS y a los datos de los alumnos y empleados.

Procedimiento de Gestión de Accesos

1. Concesión de Acceso
   * Nuevo acceso: El acceso a los sistemas y datos será concedido tras la validación de la identidad del usuario, según su rol y responsabilidades. El acceso se debe solicitar mediante el formulario de Solicitudes de Acceso y debe ser aprobado por el gerente responsable.
   * Revisión de acceso: Los accesos serán revisados periódicamente (al menos cada seis meses) para asegurar que solo las personas autorizadas tengan acceso a la información sensible.
2. Modificación de Acceso
   * Cambios de rol: Cuando un usuario cambie de puesto o responsabilidades, su acceso debe ser actualizado según los nuevos requisitos de seguridad. Esto incluye la modificación o eliminación de accesos no necesarios.
3. Revocación de Acceso
   * Desactivación inmediata: El acceso de un usuario será revocado inmediatamente en caso de que termine su relación laboral con la organización o en caso de incidente de seguridad.
   * Revocación programada: La revocación de acceso también ocurrirá cuando un usuario cambie de funciones y ya no requiera acceso a ciertos sistemas o datos.

Política de Contraseñas

1. Requisitos de Complejidad

Las contraseñas deberán cumplir con los siguientes requisitos:

* + Longitud mínima: 12 caracteres.
  + Deben incluir al menos 1 letra mayúscula, 1 letra minúscula, 1 número y 1 carácter especial (ej. @, #, $, %).
  + No pueden ser contraseñas comunes, como "password123" o "123456".
  + Las contraseñas no deben ser reutilizadas entre diferentes sistemas.

1. Frecuencia de Rotación

Las contraseñas deberán ser cambiadas cada 90 días. El sistema alertará al usuario 7 días antes de la caducidad de la contraseña.

1. Almacenamiento y Gestión

Las contraseñas deben almacenarse de manera segura, utilizando tecnologías de cifrado robustas. Los usuarios no deben compartir contraseñas ni almacenarlas en lugares inseguros (por ejemplo, en notas visibles o archivos no cifrados).

Definición de Incidentes de Seguridad

Un incidente de seguridad es cualquier evento que compromete la confidencialidad, integridad o disponibilidad de los activos de información. Esto incluye, pero no se limita a:

Acceso no autorizado a sistemas o datos.

* + Malware detectado en los sistemas o dispositivos.
  + Pérdida de datos sensibles o de carácter personal.
  + Ataques de phishing exitosos que comprometan las credenciales de los usuarios.
  + Desastres físicos (incendios, inundaciones, etc.) que afecten a las instalaciones.

Procedimiento de Respuesta a Incidentes

1. Identificación y Reporte
   * Detección inicial: El personal debe estar capacitado para identificar incidentes de seguridad, como alertas de malware o accesos no autorizados.
   * Reporte inmediato: Cualquier incidente debe ser reportado inmediatamente al equipo de seguridad mediante el sistema de gestión de incidentes.
2. Contención
   * Aislamiento del incidente: Se debe tomar acción para contener el incidente y minimizar su propagación. Esto puede implicar la desconexión de sistemas comprometidos o la revocación de accesos.
3. Análisis y Remediación
   * Investigación: El equipo de seguridad realizará una investigación completa para comprender el alcance del incidente y determinar su causa raíz.
   * Mitigación: Se implementarán acciones correctivas para evitar que el incidente se repita en el futuro, como la actualización de sistemas, la aplicación de parches, etc.
4. Recuperación
   * Recuperación de datos: En caso de pérdida de datos, se procederá con la restauración desde copias de seguridad.
   * Restauración de servicios: Los servicios afectados se restaurarán gradualmente para garantizar la mínima interrupción a los usuarios.
5. Comunicación
   * Notificación a las partes interesadas: Dependiendo de la gravedad del incidente, se notificará a la alta dirección, autoridades regulatorias y a los usuarios afectados (en caso de violaciones de datos).
6. Informe Post-incidente
   * Evaluación: Se realizará una evaluación post-incidente para determinar la efectividad de la respuesta y se documentarán las lecciones aprendidas.

Revisión de políticas y procedimientos: Se actualizarán las políticas y procedimientos según sea necesario para mejorar la gestión de incidentes en el futuro.

Procedimientos de Copias de Seguridad de Datos

1. Frecuencia de Copias de Seguridad
   * Datos críticos (bases de datos de pacientes, registros operativos): Se realizarán copias de seguridad diarias.
   * Datos menos críticos (documentación administrativa, informes históricos): Se realizarán copias de seguridad semanales.
2. Almacenamiento de Copias de Seguridad
   * Copia local: Se almacenarán copias de seguridad en servidores locales dentro de las instalaciones de los centros de datos de 4 GEEKS.
   * Copia remota: Se almacenarán copias adicionales en la nube (por ejemplo, Azure o AWS) para garantizar la recuperación ante desastres.
3. Verificación y Pruebas
   * Verificación mensual: Se verificará la integridad de las copias de seguridad cada mes para asegurar que no haya datos corruptos.
   * Pruebas anuales: Se realizarán pruebas anuales de recuperación para validar la capacidad de restaurar datos de las copias de seguridad.
4. Roles y Responsabilidades
   * Equipo de TI: Responsable de la gestión, almacenamiento y verificación de las copias de seguridad.
   * Equipo de seguridad: Responsable de realizar pruebas periódicas de recuperación y validar los procedimientos.

Plan de Capacitación y Concienciación en Seguridad

1. Capacitación Inicial
   * Frecuencia: Los empleados nuevos recibirán capacitación en seguridad de la información dentro de sus primeras dos semanas de trabajo.
   * Contenido: Incluye políticas de seguridad, gestión de accesos, políticas de contraseñas, y procedimientos ante incidentes.
2. Capacitación Continua
   * Frecuencia: Se realizarán cursos de actualización cada seis meses.

Contenido: Nuevas amenazas y vulnerabilidades, mejores prácticas de seguridad, y lecciones aprendidas de incidentes previos.

1. Materiales de Concienciación
   * Carteles y Directrices: Se distribuirán carteles y directrices con prácticas de seguridad básicas, como evitar hacer clic en enlaces sospechosos o asegurar los dispositivos móviles.

Revisión y Actualización de Políticas

* + Revisión periódica: Todas las políticas y procedimientos de seguridad serán revisados anualmente o cuando se produzcan cambios significativos en el entorno de TI o regulatorio.
  + Aprobación: Las políticas serán aprobadas por la alta dirección antes de su implementación y se comunicarán a todo el personal.

Manual del Sistema de Gestión de Seguridad de la Información (SGSI)

1. Introducción

El presente manual tiene como objetivo proporcionar un marco detallado para la implementación y gestión de la seguridad de la información dentro de 4 Geeks, garantizando la confidencialidad, integridad y disponibilidad de los activos de información de la organización.

El SGSI cubre todos los sistemas de información y activos de datos gestionados por 4 Geeks academy, incluidos los datos sensibles de alumnos, información personal de empleados y redes internas y externas.

La seguridad de la información de los alumnos es crítica no solo por la naturaleza sensible de los datos que se gestionan, sino también por la confianza que los alumnos, empleados y docentes tienen en que su información está protegida. 4 Geeks academy es responsable de información económica y otros detalles personales que deben estar resguardados de accesos no autorizados, alteraciones o destrucción. Además, el cumplimiento de regulaciones de privacidad y protección de datos es una prioridad para evitar sanciones y pérdidas de confianza pública.

1. Visión general del SGSI

El Sistema de Gestión de Seguridad de la Información (SGSI) del 4 GEEKS academy tiene como principal objetivo garantizar la protección y gestión adecuada de la información sensible que maneja la organización. Este sistema busca minimizar los riesgos asociados con el manejo, almacenamiento, y transmisión de datos, tales como los datos personales o económico de los alumnos, y registros operativos. A través del SGSI, 4 Geeks academy se compromete a mantener la confidencialidad, integridad y disponibilidad de sus activos de información, alineándose con las mejores prácticas internacionales y cumpliendo con las regulaciones legales como el Reglamento General de Protección de Datos (GDPR) y la Directiva NIS.

Los objetivos del SGSI son los siguientes:

* + Proteger los datos sensibles contra accesos no autorizados.
  + Cumplir con los requisitos regulatorios aplicables.
  + Reducir la probabilidad e impacto de incidentes de seguridad.
  + Fomentar una cultura de seguridad de la información en todos los niveles de la organización.
  + Asegurar que los controles de seguridad sean apropiados y efectivos.
  + Establecer procedimientos claros para la gestión de incidentes.
  + Proveer una infraestructura robusta de protección de datos.

Modelo de Gestión de Seguridad de la Información

El SGSI de 4 Geeks academy se basa en un marco integral que incorpora las mejores prácticas internacionales, principalmente las establecidas en la norma ISO/IEC 27001, el NIST (National Institute of Standards and Technology) y las directrices del Centro para la Seguridad en Internet (CIS). Estos marcos proporcionan un enfoque sistemático para la gestión de la seguridad de la información, asegurando que se implementen controles adecuados para proteger los activos de información y que las amenazas y vulnerabilidades sean identificadas, evaluadas y mitigadas de manera efectiva.

El SGSI no solo se enfoca en los controles tecnológicos, sino también en los controles organizacionales y humanos. Esto incluye la capacitación continua del personal, la definición de roles y responsabilidades, así como la implementación de procesos y procedimientos para garantizar que la seguridad sea gestionada de manera integral y continua en toda la organización.

Cumplimiento Regulatorio

La seguridad de la información en 4 Geeks academy no solo es fundamental para proteger los datos, sino también para cumplir con diversas normativas y regulaciones. El cumplimiento con el GDPR es esencial para garantizar que los datos personales de los alumnos sean manejados adecuadamente, con medidas de protección que permitan a la organización cumplir con los requisitos de transparencia, consentimiento y notificación de brechas de seguridad.

Descripción de los Activos de Información

El alcance del SGSI incluye todos los activos de información, tanto digitales como físicos, utilizados por 4 Geeks academy. Estos activos incluyen:

* Hardware:
  + Servidores Centrales: Donde se almacenan los datos de pacientes y registros médicos.
  + Equipos de Escritorio y Portátiles: Utilizados por el personal administrativo y clínico para acceder a información sensible.
  + Dispositivos Móviles: Tabletas, teléfonos inteligentes y otros dispositivos portátiles utilizados para acceder a datos en cualquier momento y lugar.

* Software:
  + Campus virtual: Programas utilizados para registrar y gestionar la información académica.
  + Intranet: Programas para el registro, alta, baja y modificación de los alumnos.
  + Bases de Datos: Sistemas como Oracle y SQL Server que almacenan y gestionan grandes volúmenes de datos de salud.
* Datos Sensibles:
  + Datos Personales del alumno: Contienen información crítica de carácter económico como cuentas corrientes, etc…
  + Información Personal de Empleados: Datos sensibles relacionados con los empleados de 4 Geeks academy.
  + Información Personal de docentes: Datos Personales de los docentes -

Clasificación y Valoración de Activos

* Alto:
  + Servidores de Aplicaciones: La pérdida o alteración de estos datos podría afectar directamente la atención de los pacientes.
  + Red interna con aplicaciones de gestión de alumnos
  + Bases de Datos de Alumnos: Contienen información sensible que, si se ve comprometida, podría tener consecuencias graves.

* Medio:
  + Equipos de Oficina y Sistemas de Respaldo: Aunque son importantes, no están directamente involucrados en la gestión de datos sensibles de pacientes.
* Bajo:
  + Documentación Pública: Información accesible al público y no sensible. Áreas de Acceso Restringido y Ubicaciones Físicas

El SGSI establece que ciertas áreas de la organización deben tener acceso restringido para garantizar la seguridad de los activos de información:

* Centros de Datos Nacionales y Regionales: Almacenamiento físico de la infraestructura crítica de TI.
* Salas de Servidores: Solo el personal autorizado tiene acceso a estas áreas.
* Laboratorios de Investigación: Áreas en las que se gestionan datos de investigación médica sensibles.

1. Roles y responsabilidades

La correcta implementación y mantenimiento del SGSI en 4 Geeks Academy requiere la participación activa de varios roles dentro de la organización. A continuación, se describen los principales roles y sus responsabilidades dentro del SGSI:

* + Director de Seguridad de la Información (CISO-Chief Information Security Officer)

Responsabilidad: Supervisar la implementación, gestión y mejora continua del SGSI. Es responsable de garantizar que la organización cumpla con las normativas y regulaciones relevantes, y de reportar directamente a la alta dirección sobre el estado de la seguridad de la información.

Tareas:

* + Asegurar que el SGSI esté alineado con los requisitos regulatorios y las mejores prácticas internacionales.
  + Supervisar la evaluación de riesgos y la implementación de controles de seguridad.
  + Desarrollar estrategias de mitigación de riesgos y gestionar incidentes de seguridad.
  + Equipo de TI (Tecnologías de la Información)

Responsabilidad: Implementar, mantener y operar los sistemas tecnológicos que forman parte del SGSI. Asegurar la infraestructura tecnológica, la protección de los activos de información y el monitoreo continuo de la seguridad.

Tareas:

* + Implementar controles técnicos como firewalls, cifrado, autenticación multifactor.
  + Mantener actualizados los sistemas y aplicar parches de seguridad.
  + Gestionar los incidentes de seguridad desde el punto de vista técnico.
  + Gestores de Datos y Seguridad

Responsabilidad: Supervisar el cumplimiento de las políticas de privacidad y la seguridad de los datos. Asegurar que se realicen evaluaciones de riesgos periódicas y que las políticas de seguridad sean revisadas y actualizadas regularmente.

Tareas:

* + Monitorear el acceso a los datos sensibles y asegurarse de que solo el personal autorizado tenga acceso.
  + Evaluar los riesgos asociados con los datos y recomendar medidas correctivas.
  + Asegurar que los procedimientos de respuesta a incidentes sean implementados correctamente.
  + Personal Clínico y Administrativo

Responsabilidad: Asegurarse de que las políticas y procedimientos de seguridad sean seguidos de manera adecuada. Ser los primeros en detectar incidentes de seguridad relacionados con el manejo de datos sensibles.

Tareas:

* + Cumplir con las directrices de seguridad en el manejo de la información de los pacientes.
  + Informar sobre incidentes de seguridad o comportamientos sospechosos.
  + Alta Dirección

Responsabilidad: Proveer el apoyo necesario para la implementación y mejora continua del SGSI, asegurando que los recursos sean asignados adecuadamente y que el SGSI esté alineado con los objetivos estratégicos de la organización.

Tareas:

* + Aprobar las políticas de seguridad de la información y garantizar que se asignen recursos adecuados.
  + Revisar los informes periódicos de seguridad y tomar decisiones sobre la mejora continua del SGSI.

Mantenimiento y Mejora Continua del SGSI

El SGSI debe ser evaluado y ajustado continuamente para abordar los cambios en el entorno de amenazas, las tecnologías y las normativas. Esto requiere una participación activa de todos los roles mencionados, con especial énfasis en el monitoreo continuo de la efectividad de los controles, la gestión de incidentes y la actualización de políticas.

1. Compromiso del Liderazgo con el SGSI

Declaración de Compromiso de la Alta Dirección

La alta dirección de 4 Geeks Academy está comprometida con la seguridad de la información y la protección de los datos sensibles que maneja la organización. Este compromiso se manifiesta a través de su liderazgo activo en la implementación del SGSI y el establecimiento de los recursos necesarios para su éxito. La alta dirección entiende que la seguridad de la información es un proceso continuo y esencial para mantener la confianza del público y cumplir con las normativas de protección de datos.

Principales compromisos:

* + Asegurarse de que el SGSI esté alineado con los objetivos estratégicos de 4 Geeks Academy, priorizando la protección de los datos de los pacientes y cumpliendo con las regulaciones nacionales e internacionales.
  + Asignar recursos adecuados para implementar, operar y mejorar continuamente el SGSI.
  + Apoyar la cultura de seguridad dentro de la organización, promoviendo la capacitación y concientización en todos los niveles, desde el personal administrativo hasta el personal clínico.
  + Realizar revisiones periódicas del SGSI y evaluar su efectividad en la gestión de riesgos y la protección de los activos de información.

Revisión y Aprobación de Políticas y Procedimientos

La alta dirección debe revisar y aprobar las políticas de seguridad de la información, así como los procedimientos para garantizar que se mantengan actualizados y que continúen siendo efectivos frente a los riesgos emergentes. Este proceso de revisión será anual, o en un plazo menor si se detectan cambios significativos en el entorno de amenazas o en las regulaciones aplicables.

1. Evaluación de Riesgos

La evaluación de riesgos en el SGSI de 4 GeeksAcademy se basa en un proceso sistemático que permite identificar, analizar y evaluar los riesgos asociados con los activos de información de la organización. La metodología utilizada sigue un enfoque cualitativo y cuantitativo, con un enfoque en la probabilidad de ocurrencia de los riesgos y su impacto en la organización.

Proceso de Evaluación de Riesgos:

* + 1. Identificación de Activos: Se realiza un inventario completo de los activos de información y su clasificación según su importancia.
    2. Identificación de Amenazas y Vulnerabilidades: Se analizan las amenazas y vulnerabilidades asociadas a cada activo.
    3. Evaluación de Riesgos: Se evalúa la probabilidad e impacto de cada riesgo identificado.
    4. Prioridad de Riesgos: Los riesgos se priorizan con base en su impacto y probabilidad, asignando un nivel de atención adecuado.
    5. Selección de Controles: Se seleccionan controles apropiados para mitigar los riesgos más críticos.

Plantillas/Formularios de Evaluación de Riesgos:

* + Formulario de Inventario de Activos.
  + Formulario de Identificación de Amenazas y Vulnerabilidades. - Plantilla de Evaluación de Riesgos (probabilidad e impacto).

Indicadores Clave de Riesgo (KPIs):

* + Número de incidentes de seguridad: Se monitoriza el número de incidentes reportados por los empleados y el equipo de TI, evaluando su impacto.
  + Cumplimiento con las políticas de seguridad: Se mide el grado de cumplimiento con las políticas de seguridad de la información a través de auditorías y revisiones internas.
  + Tiempo de respuesta ante incidentes: Se evalúa la rapidez con la que el equipo de TI responde a incidentes de seguridad y su efectividad en la mitigación.
  + Porcentaje de dispositivos protegidos con medidas de seguridad: Se verifica la cobertura de los controles de seguridad en los dispositivos utilizados por el personal.

1. Selección de Controles de Seguridad

Para garantizar que el SGSI de 4 Geeks Academy sea efectivo en la protección de la información sensible y en la mitigación de riesgos, se ha implementado un proceso de selección de controles de seguridad basado en la evaluación de riesgos, así como la implementación de un proceso de monitoreo continuo. Este proceso está alineado con las mejores prácticas establecidas en la norma ISO/IEC 27001:2022 y otros marcos regulatorios pertinentes. El monitoreo ayudará a identificar posibles fallos en los controles, a detectar amenazas emergentes y a evaluar si el SGSI está cumpliendo con los objetivos establecidos.

Los criterios para la selección de controles son los siguientes:

* + Identificación de activos críticos de información.
  + Evaluación de vulnerabilidades y amenazas potenciales.
  + Impacto de los riesgos en la confidencialidad, integridad y disponibilidad de la información.
  + Coste-beneficio de la implementación de controles de seguridad.

Los controles seleccionados para mitigar los riesgos identificados incluyen medidas como:

* + Control de Acceso:
    - Autenticación multifactor (MFA) para usuarios privilegiados y críticos.
    - Políticas de acceso basadas en roles (RBAC).
    - Registro y auditoría de accesos.
  + Protección de Datos:
    - Cifrado de datos en reposo y en tránsito con AES-256.
    - Uso de VPN y TLS 1.3 para comunicaciones seguras.
  + Gestión de Identidades y Seguridad de Cuentas:
    - Políticas de contraseñas robustas.
    - Desactivación inmediata de cuentas inactivas.
  + Seguridad de la Red y Sistemas:
    - Firewalls de nueva generación (NGFW).
    - Monitoreo de red mediante SIEM.
    - Análisis de comportamiento del usuario (UEBA).
  + Capacitación y Concienciación:
    - Programas de formación continua sobre ciberseguridad para todo el personal.
    - Simulacros de ataques de phishing.

1. Procedimientos de Seguridad

El cumplimiento de las políticas de seguridad se garantiza mediante la implementación de procedimientos detallados en diferentes ámbitos clave:

* + Política de Acceso y Control de Usuarios: Describe cómo se concederán, modificarán y revocarán los accesos a los sistemas.
    - Proceso de Solicitud de Acceso: Procedimiento formal para solicitar y aprobar el acceso a sistemas sensibles.
    - Control de Contraseñas: Requisitos de complejidad, frecuencia de cambio y almacenamiento seguro: longitud mínima de 12 caracteres, cambio obligatorio cada 90 días y bloqueo tras 5 intentos fallidos.
  + Gestión de Incidentes de Seguridad: Procedimiento detallado para la identificación, reporte y resolución de incidentes de seguridad.
    - Definición de Incidentes: Qué constituye un incidente de seguridad, cómo se debe reportar y cómo se gestionará. Pérdida de datos, accesos no autorizados, malware, denegación de servicio.
    - Proceso de Respuesta a Incidentes: Involucra identificación, contención, erradicación y recuperación de un incidente.
  + Política de Copias de Seguridad y Recuperación de Datos:
    - Frecuencia de las Copias de Seguridad: Se realizan copias diarias, semanales y mensuales de los datos críticos.
    - Ubicación: Almacenamiento en sitio primario y secundario.
    - Pruebas de Restauración: Simulacros trimestrales de recuperación.
    - Roles Responsables: El equipo de TI será responsable de las copias de seguridad, con un plan de recuperación probado periódicamente.

1. Plan de Capacitación y Concienciación

Para fortalecer la seguridad de la información, se han diseñado programas de concienciación dirigidos a todos los empleados y terceros que acceden a sistemas críticos.

* + Programa de Formación: Incluir capacitación regular sobre amenazas cibernéticas, uso seguro de sistemas y protección de datos personales.
  + Materiales de Concienciación: Carteles, boletines y recordatorios digitales sobre prácticas de seguridad.
  + Evaluaciones Periódicas: Exámenes de conocimientos y reportes de efectividad de la formación.

1. Monitoreo y Medición de la Efectividad del SGSI
   * Indicadores Clave de Desempeño (KPIs): Se definirán KPIs para medir la efectividad del SGSI, incluyendo:
     + Número de incidentes de seguridad reportados.
     + Porcentaje de cumplimiento con políticas de acceso.
     + Tiempo de respuesta ante incidentes de seguridad.
     + Porcentaje de personal capacitado en ciberseguridad.
     + Frecuencia y éxito de las auditorías de seguridad.
   * Auditorías Internas y Revisiones: Se realizarán auditorías periódicas del SGSI para evaluar su eficacia, con el apoyo de los auditores internos y externos.
   * Mecanismos de monitoreo:
     + Uso de SIEM: Análisis en tiempo real de eventos de seguridad.
     + Pruebas de Penetración: Evaluación periódica de vulnerabilidades.
2. Revisión y Actualización del SGSI

El SGSI es un sistema dinámico que requiere revisión continua para adaptarse a nuevos riesgos y cambios en la organización.

* + Cronograma de Revisiones
  + Revisión Anual: Evaluación completa del SGSI con ajuste de controles.
  + Evaluación Post-Incidente: Ajuste inmediato tras incidentes significativos.
  + Auditorías Externas Bienales: Validación de cumplimiento con regulaciones.
  + Proceso de Mejora Continua
  + Lecciones Aprendidas: Implementación de recomendaciones tras auditorías e incidentes.
  + Actualización de Procedimientos: Revisión y ajuste basado en tendencias de seguridad.

Este manual estará accesible para todas las partes interesadas clave y será actualizado periódicamente para reflejar la evolución del panorama de seguridad de la información.