# Sistema de Gestión de Seguridad de la Información (SGSI) - 4Geeks Academy

4Geeks

## 1. Introducción

La Institución Educativa 4Geeks Academy reconoce la importancia de proteger la información de sus estudiantes, profesores y personal, así como la integridad y disponibilidad de sus sistemas, especialmente en el contexto de clases remotas y la gestión de su página web. Este SGSI se basa en la norma ISO 27001 y tiene como objetivo establecer, implementar, mantener y mejorar continuamente la seguridad de la información.

## 2. Objetivos del SGSI

- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Cumplir con leyes, regulaciones y normativas aplicables.
- Reducir riesgos de seguridad a un nivel aceptable.
- Mejorar continuamente la eficacia del SGSI.

## 3. Alcance del SGSI

Este SGSI cubre los siguientes activos de información:

- Página web: Información del sitio web, contenido educativo, datos de usuarios, plataforma de gestión de aprendizaje (LMS).
- Clases remotas: Plataforma de videoconferencia, materiales de clase, datos de acceso, grabaciones.
- Datos de estudiantes: Información personal, calificaciones, expedientes académicos.
- Datos de profesores y personal: Información personal, datos de acceso, información financiera.
- Infraestructura de TI: Servidores, equipos, redes, software.
- Aspectos legales: Cumplimientos normativos requeridos.
- Evaluación y control de Riesgos.
- Plan para la continuidad y evolución del negocio.

## 4. Identificación de Activos, Amenazas y vulnerabilidades encontradas

| ACTIVO | AMENAZAS | VULNERABILIDADES |
|---|---|---|
| Servidor FTP | Acceso no autorizado | Clave débil en servicio FTP (clave predeterminada) |
| Servidor SSH | Acceso no autorizado, escalada de privilegios (acceso root) | Clave débil en servicio SSH (ataque de fuerza bruta exitoso) |
| Sitio web (WordPress) | Exposición de información sensible, Posibilidad de acceso y modificación de la base de datos | Mala configuración en wp-config.php |

## 5. Clasificación de Riesgos de activos según criterios CID

La evaluación de riesgos basada en los criterios CID permite analizar de forma estructurada las amenazas y vulnerabilidades que pueden afectar a los activos de información, facilitando la toma de decisiones informadas para su protección

- **Confidencialidad:** Protección de la información sensible contra accesos no autorizados.
- **Integridad:** Garantía de que la información se mantiene precisa y completa, sin modificaciones no autorizadas.
- **Disponibilidad:** Asegurar que la información esté accesible para los usuarios autorizados cuando la necesiten.

| Activo | Confidencialidad | Integridad | Disponibilidad |
|---|---|---|---|
| FTP | **Alta** | **Media** | **Media** |
| SSH | **Muy Alta** | **Muy alta** | **Alta** |
| Sitio web (Wordpres) | **Alta** | **Alta** | **Alta** |

## 5. Matriz de Riesgos

La combinación de probabilidad e impacto determina el nivel de riesgo. Este nivel indica la prioridad para tomar medidas de seguridad.

| Activo | Probabilidad | Impacto | Nivel de Riesgo |
|---|---|---|---|
| FTP | **Alta** | **Alto** | **Alto** |
| SSH | **Media** | **Muy alto** | **Muy alto** |
| wp-config.php | **Media** | **Alto** | **Alto** |

# Controles de Seguridad para Vulnerabilidades identificadas basadas en normativas (NIST / ISO 27001)

**Vulnerabilidad: FTP (Protocolo de Transferencia de Archivos)**

**ISO/IEC 27001:**

- A.9.4.1 Restricción del acceso a la información: Limita el acceso a la información sensible transmitida por FTP mediante controles de acceso y autenticación robusta.
- A.12.1.1 (Procedimientos de operación y responsabilidades) - Se deben definir procedimientos claros para la gestión de accesos y permisos en servidores FTP.
- A.13.1.1 Uso de contraseñas: Implementa contraseñas fuertes y únicas para las cuentas FTP, y exige cambiarlas periódicamente.
- A.17.2.1 (Controles criptográficos) - Se deben utilizar técnicas de cifrado apropiadas para proteger la información sensible.

**NIST CSF:**

- PR.AC - Control de acceso: Restringe el acceso a los servidores FTP y a los archivos transferidos según el principio de "mínimo privilegio".

**CIS Controls:**

- Control de Inventario y Activos de Software: Identifica y gestiona los servidores FTP como activos de software, asegurando que estén actualizados y configurados de forma segura.
- Control de Inventario y Activos de Hardware: Similar al anterior, pero enfocado en los servidores FTP como activos de hardware.

**Vulnerabilidad: SSH**

**ISO/IEC 27001:**

- A.9.4.1 Restricción del acceso a la información: Asegura que solo usuarios autorizados accedan a los sistemas a través de SSH, utilizando autenticación de dos factores y claves SSH robustas.
- A.13.1.1 Uso de contraseñas: Aunque se recomienda el uso de claves SSH, si se usan contraseñas, deben ser fuertes y cambiarse periódicamente.
- A.13.2.1 (Protección contra software malicioso) - Se debe mantener el software SSH actualizado para corregir vulnerabilidades conocidas.

**NIST CSF:**

- PR.AC - Control de acceso: Implementa controles de acceso para restringir el acceso a los sistemas a través de SSH, incluyendo el uso de listas blancas de direcciones IP.

**CIS Controls:**

- Control de Inventario y Activos de Software: Gestiona los servidores SSH como activos de software, asegurando que estén actualizados y configurados de forma segura.
- Control de Inventario y Activos de Hardware: Similar al anterior, pero enfocado en los servidores SSH como activos de hardware.

## Vulnerabilidad: wp-config.php (sitio Web Wordpress)

**ISO/IEC 27001:**

- A.9.4.1 (Restricción del acceso a la información) - Se deben aplicar permisos restrictivos para proteger el archivo de configuración de modificaciones no autorizadas.
- A.12.1.1 (Procedimientos de operación y responsabilidades) - Se deben definir procedimientos para la gestión de permisos de archivos y directorios.
- A.13.2.1 Protección contra software malicioso: Protege el archivo wp-config.php de modificaciones no autorizadas y acceso malicioso, ya que contiene información sensible de la base de datos.
- A.16.1.1 (Planificación de la continuidad del negocio) - Se deben realizar copias de seguridad periódicas del archivo de configuración para asegurar su disponibilidad en caso de pérdida o corrupción.
- A.17.2.1 (Controles criptográficos) - Se deben utilizar técnicas de cifrado apropiadas para proteger la información sensible en reposo.
- A.18.2.1 (Responsabilidades de gestión de activos) - Se deben asignar responsabilidades para la gestión de copias de seguridad de activos de información críticos.

**NIST CSF:**

- DE.CM - Gestión de la configuración: Implementa medidas para asegurar la integridad y confidencialidad del archivo wp-config.php, como permisos de archivo restrictivos y monitorización de cambios.

**CIS Controls:**

- Control de Inventario y Activos de Software: Gestiona el archivo wp-config.php como parte del software de WordPress, asegurando que esté configurado de forma segura y protegido contra modificaciones no autorizadas.

# Plan de respuesta de incidentes

Este plan tiene como objetivo asegurar la continuidad de los servicios críticos de la academia 4Geeks en caso de incidentes de seguridad que comprometan la disponibilidad, integridad o confidencialidad de la información. Se enfoca en las vulnerabilidades identificadas en los servicios FTP, SSH y el archivo wp-config.php.

**Este plan cubre los siguientes sistemas y servicios:**

- Servidor web principal (donde reside el CMS WordPress)
- Servidor de archivos (que aloja el servicio FTP)
- Servidores de acceso remoto (que utilizan SSH)
- Base de datos (utilizada por WordPress)

**Procedimientos de Recuperación**

**1.Incidente Detectado:**

- Activar el equipo de respuesta a incidentes.
- Evaluar la naturaleza y el alcance del incidente.
- Determinar los servicios afectados y el nivel de impacto**.**

**2. Contención:**

- Aislar los sistemas afectados para evitar la propagación del incidente.
- Deshabilitar cuentas de usuario comprometidas.
- Bloquear direcciones IP maliciosas.

**3. Erradicación:**

- Parchear las vulnerabilidades explotadas (FTP, SSH, wp-config.php).
- Actualizar software a versiones seguras.

**4. Recuperación:**

- 
- Restaurar copias de seguridad de los sistemas y datos afectados.
- Verificar la integridad de los datos restaurados.
- Reiniciar los servicios críticos de forma controlada.

**5. Análisis Post-Incidente:**

- Documentar el incidente y las acciones tomadas.
- Identificar las causas raíz del incidente.
- Implementar medidas preventivas para evitar incidentes similares.

## Conclusión

Es completamente necesario realizar copias de seguridad completas del servidor web y base de datos diariamente, así como almacenar copias de seguridad en un lugar seguro, haciendo pruebas periódicas para su control.
.
Es Importante mantener canales de comunicación claros para notificar a usuarios y partes interesadas sobre incidentes y el estado de los servicios.

Es fundamental implementar sistemas de respaldo y plan de contingencia para activos críticos.

Realizar pruebas y actualizaciones periódicas del plan de recuperación para asegurar su efectividad y lograr así la continuidad de los servicios.

.....

Este informe resume el trabajo realizado para implementar el Sistema de Gestión de Seguridad de la Información (SGSI) en 4Geeks Academy. Hemos establecido una base sólida para proteger nuestra información y activos digitales.

El SGSI es una herramienta viva que requiere monitoreo y mejora continua. Confío en que este sistema fortalecerá la seguridad de la información y contribuirá al éxito de la academia. Agradezco su liderazgo y apoyo en este tema crucial.

Me complace discutir este informe en detalle y responder sus preguntas.

Atentamente

Departamento de Seguridad Informática