Desarrollo de un Sistema Básico de Gestión de Seguridad de la Información (SGSI) para 4Geeks

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

Organización: 4Geeks Investments LLC

Fecha: julio 2025

Versión: 1.0

Informe para:

Proyecto final Bootcamp - Aplicar ISO 27001

Índice:

1. Introducción

Este manual describe el Sistema de Gestión de Seguridad de la Información (SGSI) de **4Geeks**. Su propósito es establecer un marco para la protección de la información digital y física gestionada por la organización, en línea con los principios de la norma ISO/IEC 27001.

2. Objetivo del SGSI

El objetivo del SGSI es:

- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Gestionar riesgos de seguridad de forma proactiva.
- Cumplir con las obligaciones legales, contractuales y regulatorias (como el RGPD).
- Establecer procedimientos para la respuesta a incidentes.
- Garantizar la continuidad del negocio ante eventos disruptivos.
- Fomentar una cultura organizacional centrada en la ciberseguridad

3. Alcance del SGSI

El SGSI cubre:

- Plataformas tecnológicas (LMS, CMS, sistemas de pagos).
- Infraestructura en la nube (AWS, backups).
- Aplicaciones web internas y externas.
- Datos personales y académicos de estudiantes.
- Equipos y dispositivos utilizados en modalidad remota o en sedes físicas.
- Servicios subcontratados con acceso a datos.

Exclusiones:

- Dispositivos personales sin gestión corporativa.
- Sistemas no operados directamente por **4Geeks**.

4. Marco normativo y regulatorio

Este SGSI se fundamenta en los siguientes marcos:

- ISO/IEC 27001:2022 e ISO/IEC 27002
- RGPD (Reglamento General de Protección de Datos)
- Política de Privacidad de la OMS
- Guías de ciberseguridad de la ONU y la OMS

5. Partes interesadas

- Dirección General
- Departamento IT / Seguridad
- Área Académica
- Estudiantes y personal docente
- Proveedores de tecnología (hosting, pagos, LMS)
- Entidades regulatorias y clientes finales

6. Evaluación y tratamiento de riesgos

Metodología: Evaluación cualitativa basada en ISO/IEC 27005.
Pasos realizados:

1. Identificación de activos.
2. Detección de amenazas y vulnerabilidades.
3. Estimación de impacto y probabilidad.
4. Determinación del nivel de riesgo.
5. Propuesta de medidas de tratamiento.

7. Controles de seguridad implementados

- Control de accesos con MFA.
- Backups cifrados y automáticos.
- Política de contraseñas robustas.
- Auditoría y monitoreo de acceso a datos.
- Gestión de parches mensuales.
- Herramientas antimalware y firewall activo.
- Segmentación de entornos (desarrollo, producción

8. Políticas de seguridad

Las políticas aprobadas incluyen:

- Política general de seguridad.
- Política de accesos.
- Política de uso aceptable.
- Política de protección de datos.
- Política de backups.
- Política de gestión de incidentes.
- Política de concienciación y formación.
- Política de seguridad en el desarrollo.

9. Gestión de incidentes

Se han documentado procedimientos detallados para:

- Sistema de reporte centralizado.
- Equipo de respuesta CSIRT designado.
- Clasificación de incidentes por criticidad.
- Notificación a usuarios y autoridades cuando aplique.

- Lecciones aprendidas y revisión post-incidente

10. Monitorización y auditoría

- Revisión periódica de logs y accesos.
- Escaneos de vulnerabilidades internos.
- Auditorías internas anuales.
- Seguimiento de KPIs de seguridad

11. Mejora continua

El SGSI se revisa de manera continua mediante:

- Revisión anual del manual y políticas.
- Simulacros de incidentes y formación continua.
- Retroalimentación del personal.
- Seguimiento de no conformidades detectadas en auditorías

12. Conclusión

Este manual representa el compromiso de **4Geeks** con la seguridad de la información como parte de su estrategia organizativa. Su implementación efectiva requiere la colaboración de todas las partes interesadas y una cultura sólida de seguridad.