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

**4Geeks**

Informe alcance definido del SGSI

**Organización:** 4Geeks Investments LLC

**Fecha**: julio 2025

**Versión:** 1.0

**Informe para:**

Proyecto final de Bootcamp - Aplicar ISO 27001

Índice:

|  |  |
| --- | --- |
| Introducción . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| Propósito del SGSI . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| Alcance del SGSI . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| Exclusiones . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
| Partes interesadas . . . . . . . . . . . . . . . . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 5 |
| Objetivos del SGSI . . . . . . . . . . . . . . . . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 5 |

## 1. Introducción

**4Geeks** es una empresa dedicada a la formación online en el sector tecnológico. Opera principalmente en modalidad remota, aunque mantiene varias sedes físicas utilizadas para actividades administrativas, soporte y ocasionalmente formación presencial.

## 2. Propósito del SGSI

El objetivo del Sistema de Gestión de Seguridad de la Información (SGSI) es garantizar la **confidencialidad, integridad y disponibilidad** de la información gestionada por **4Geeks**, incluyendo los datos personales de los alumnos, materiales didácticos, plataformas tecnológicas y sistemas de soporte.

## 3. Alcance del SGSI

**1. Activos de información incluidos:**

* Plataformas de formación online (LMS y CMS)
* Infraestructura en la nube (servidores, bases de datos)
* Cuentas y accesos de usuarios (profesores, alumnos, personal)
* Repositorios de código y contenido educativo
* Sistemas de soporte y atención al cliente
* Correos electrónicos corporativos
* Documentación interna y contratos digitales
* Datos personales, de acceso y académicos de los alumnos

**2. Tecnologías cubiertas:**

* CMS: WordPress
* Frontend: React.js, Bootstrap
* Backend: Node.js, Express
* Infraestructura: Amazon Web Services (AWS)
* Analítica: Google Tag Manager, Hotjar
* Seguridad: Cloudflare, certificados SSL, reCAPTCHA
* Herramientas de automatización: Zapier, Segment
* Pasarelas de pago: Stripe, PayPal

**3. Límites físicos:**

* Oficinas centrales (Madrid y Barcelona)
* Sedes satélite (coworking u oficinas compartidas)
* Dispositivos remotos (teletrabajo) bajo políticas BYOD

**4. Límites virtuales:**

* Entornos en la nube (AWS)
* Infraestructura propia y de terceros
* Accesos VPN y aplicaciones web privadas

## 4. Exclusiones

El SGSI no cubre:

* Dispositivos personales no gestionados sin control de acceso corporativo
* Plataformas de terceros no integradas directamente con el LMS

## 5. Partes interesadas

Las partes interesadas relevantes para el SGSI incluyen:

* Ciudadanos y pacientes que utilizan los servicios de la OMS
* Dirección general
* Equipo técnico (desarrolladores, sysadmins)
* Departamento legal y administrativo
* Docentes y personal académico
* Estudiantes y usuarios finales
* Proveedores tecnológicos y partners externos

## 6. Objetivos del SGSI

Los objetivos específicos del SGSI en **4Geeks** son:

* **Proteger la información sensible** (datos personales, académicos y administrativos) frente a accesos no autorizados, pérdidas o alteraciones.
* **Asegurar la continuidad de los servicios online**, minimizando interrupciones causadas por incidentes de seguridad.
* **Cumplir con requisitos legales y normativos**, incluyendo el RGPD, leyes de propiedad intelectual y normativas de educación online.
* **Establecer un marco de mejora continua**, que permita actualizar políticas, controles y procedimientos conforme evolucionan los riesgos tecnológicos.
* **Fomentar la concienciación y responsabilidad** entre el personal, los docentes y los alumnos sobre buenas prácticas de seguridad de la información.
* **Supervisar y auditar la infraestructura tecnológica**, detectando vulnerabilidades y aplicando correcciones de forma proactiva.