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

**4Geeks**

Informe evaluación de riesgos del SGSI

**Organización:** 4Geeks Investments LLC

**Fecha**: julio 2025

**Versión:** 1.0

**Responsable:** CISO – 4Geeks

**Informe para:**

Proyecto final Bootcamp - Aplicar ISO 27001

Índice:

|  |  |
| --- | --- |
| Objetivo de la evaluación de riesgos . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| Metodología de evaluación de riesgos . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| Identificación de activos clave . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
| Principales amenazas identificadas . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
| Análisis de riesgos (Impacto x Probabilidad) . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 5 |
| Tratamiento y recomendaciones . . . . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 6 |
| Conclusión . . . . . . . . . . . . . . . . . . . . .. . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 6 |

## 1. Objetivo de la evaluación de riesgos

La evaluación de riesgos tiene como objetivo identificar, analizar y valorar las amenazas y vulnerabilidades que afectan a los activos de información de **4Geeks**, con el fin de priorizar controles de seguridad adecuados que reduzcan el impacto de posibles incidentes.

## 2. Metodología de evaluación de riesgos

Se ha empleado una **metodología cualitativa** basada en la norma **ISO/IEC 27005**, que incluye las siguientes fases:

1. **Identificación de activos**
2. **Identificación de amenazas y vulnerabilidades**
3. **Evaluación del impacto y la probabilidad**
4. **Determinación del nivel de riesgo**
5. **Propuesta de tratamiento del riesgo**

## 3. Identificación de activos clave

| **Activo** | **Tipo** | **Responsable** | **Clasificación** |
| --- | --- | --- | --- |
| Plataforma LMS (formación) | Software | CTO | Crítico |
| Base de datos de alumnos | Información | DPO / Administrador BD | Crítico |
| Servidores AWS | Infraestructura | Administrador Cloud | Crítico |
| Repositorio de contenidos | Documentación | Equipo docente | Alto |
| Sistema de pagos online | Aplicación web | CFO / CTO | Crítico |
| Cuentas de correo electrónico | Comunicación | Dpto. IT | Alto |
| Panel de gestión de usuarios | Plataforma web | Dpto. Soporte | Medio |

## 4. Principales amenazas identificadas

| **Amenaza** | **Vulnerabilidad asociada** |
| --- | --- |
| Acceso no autorizado | Contraseñas débiles, falta de MFA |
| Pérdida de datos | Falta de backups, errores de configuración |
| Ataques DDoS | Ausencia de CDN/mitigación (ej. Cloudflare básico) |
| Ransomware | Falta de antivirus en equipos docentes |
| Fuga de información (DLP) | Uso indebido de datos por empleados o terceros |
| Phishing y malware | Falta de formación al personal remoto |
| Código malicioso en plugins LMS | Software desactualizado o sin revisión de terceros |

## 5. Análisis de riesgos (Impacto x Probabilidad)

**Escala cualitativa:**

* **Impacto**: Bajo / Medio / Alto / Crítico
* **Probabilidad**: Baja / Media / Alta

**Matriz ejemplo:**

| **Riesgo identificado** | **Impacto** | **Probabilidad** | **Nivel de Riesgo** | **Prioridad** |
| --- | --- | --- | --- | --- |
| Acceso no autorizado a la base de datos | Crítico | Alta | Muy Alto | Alta |
| Fallo en el sistema de pagos | Crítico | Media | Alto | Alta |
| Inyección SQL en formularios | Alto | Media | Medio | Media |
| Ransomware en dispositivos docentes | Alto | Alta | Alto | Alta |
| Fuga de datos por empleados | Alto | Media | Alto | Media |
| Phishing a usuarios remotos | Medio | Alta | Medio | Media |
| Pérdida de datos por falta de backup | Crítico | Baja | Medio | Alta |

## 6. Tratamiento y recomendaciones

| **Riesgo** | **Control propuesto** |
| --- | --- |
| Acceso no autorizado | Implementar autenticación multifactor (MFA) |
| Ransomware | Soluciones antivirus/EDR, backup offline |
| Fallo del sistema de pagos | Auditoría y redundancia en integración de pasarela |
| Fuga de datos (DLP) | Aplicar controles de acceso y monitoreo de uso |
| Phishing y errores humanos | Capacitación y simulacros de ciberseguridad |
| Inyección SQL | Validación de entradas, WAF |
| Pérdida de datos | Backups automáticos con restauración probada |

## 7. Conclusión

La evaluación ha identificado múltiples amenazas con riesgos **críticos y altos** que requieren tratamiento inmediato, especialmente los relacionados con la base de datos de alumnos, el sistema de pagos y los dispositivos remotos. Se recomienda implementar una combinación de controles técnicos (MFA, backups, antivirus, WAF) y organizativos (formación, auditorías, políticas de acceso).