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

**4Geeks**

Informe políticas y procedimientos de seguridad de la información

**Organización:** 4Geeks Investments LLC

**Fecha**: julio 2025

**Versión:** 1.0

**Informe para:**

Proyecto final Bootcamp - Aplicar ISO 27001

Índice:

|  |  |
| --- | --- |
| Objetivo . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| Política de Seguridad de la Información . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| Política de Control de Acceso . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| Política de Uso Aceptable de Recursos TIC . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
| Política de Backup y Recuperación . . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
| Política de Seguridad en el Desarrollo Web . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
| Política de Concienciación y Formación . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
| Política de Gestión de Incidentes de Seguridad . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
| Procedimientos clave . . . . . . . . . . . . . . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 5 |
| Conclusión . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .. . . . . . . . . . . . . . . . . . . . . . . . . | 6 |

## 1. Objetivo

Definir el conjunto de normas, directrices y procedimientos que rigen el tratamiento seguro de la información en **4Geeks**, asegurando que todo el personal y colaboradores cumplan con buenas prácticas de ciberseguridad.

## 2. Política de Seguridad de la Información

**Propósito:** Establecer el compromiso de la empresa con la protección de la información.

**Contenidos:**

* Aplicación del principio de mínimo privilegio.
* Clasificación de la información (pública, interna, confidencial).
* Evaluación continua de riesgos.
* Revisión anual del SGSI.

## 3. Política de Control de Acceso

**Propósito:** Prevenir accesos no autorizados a sistemas y datos.

**Contenidos:**

* Implementación de MFA en todos los sistemas críticos.
* Gestión centralizada de credenciales con rotación periódica.
* Prohibición de compartir cuentas.
* Alta/baja/modificación de usuarios según función.

## 4. Política de Uso Aceptable de Recursos TIC

**Propósito:** Definir las condiciones de uso seguro de los activos tecnológicos.

**Contenidos:**

* Acceso a plataformas solo mediante dispositivos autorizados.
* Prohibición de instalar software no corporativo.
* Obligación de cifrar dispositivos portátiles y discos duros.

## 5. Política de Backup y Recuperación

**Propósito:** Garantizar la disponibilidad de los datos ante incidentes.

**Contenidos:**

* Realización de backups automáticos diarios en la nube y externos.
* Verificación mensual de integridad y restauración.
* Conservación mínima: 90 días.

## 6. Política de Seguridad en el Desarrollo Web

**Propósito:** Proteger las plataformas educativas ante vulnerabilidades comunes.

**Contenidos:**

* Aplicación de OWASP Top 10 en el ciclo de desarrollo.
* Uso de revisiones de código y pruebas de seguridad (SAST/DAST).
* Entornos separados: desarrollo, pruebas y producción.

## 7. Política de Concienciación y Formación

**Propósito:** Reducir el factor de riesgo humano mediante capacitación continua.

**Contenidos:**

* Formación obligatoria en ciberseguridad para todo el personal.
* Simulacros de phishing y buenas prácticas online.
* Evaluaciones anuales para validar la capacitación.

## 8. Política de Gestión de Incidentes de Seguridad

**Propósito:** Proporcionar una respuesta eficaz ante incidentes.

**Contenidos:**

* Registro de incidentes en un sistema centralizado (ticketing o SIEM).
* Equipo de respuesta a incidentes (CSIRT) interno.
* Comunicación rápida a partes interesadas y autoridad competente (si aplica).
* Post-mortem y plan de mejora tras cada incidente.

## 9. Procedimientos clave

**Procedimiento de alta y baja de usuarios**

* Registro en el sistema solo tras autorización del área responsable.
* Baja automática de cuentas tras 15 días de inactividad o cese laboral.

**Procedimiento de cifrado de datos sensibles**

* Uso obligatorio de HTTPS (TLS 1.2+).
* Cifrado AES-256 para datos en reposo.
* Cifrado de base de datos en AWS (RDS encryption).

**Procedimiento de actualización y parcheo**

* Escaneo mensual de vulnerabilidades.
* Aplicación de actualizaciones críticas en un plazo de 48h.
* Validación en entorno de pruebas antes de aplicar en producción.

**Procedimiento de gestión de contraseñas**

* Mínimo 12 caracteres, complejidad alta.
* Cambio cada 90 días o ante incidente.
* Uso de gestor de contraseñas corporativo.

## 10. Conclusión

Las políticas y procedimientos definidos en este apartado aseguran un marco formal y operativo para proteger los activos de información de **4Geeks**. Deben ser revisados al menos una vez al año, o tras cualquier incidente significativo.