DISEÑO DE UN SGSI BASADO EN LA NORMA ISO 27001 PARA LA ORGANIZACIÓN 4GEEKS ACADEMY

Luis Fernando Espinoza Arias

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

Índice

Propósito del SGSI

El propósito del SGSI en 4Geeks Academy es establecer una estructura robusta que proteja la confidencialidad, integridad y disponibilidad de la información relacionada con sus operaciones académicas, comerciales y tecnológicas. El sistema permitirá a la institución gestionar adecuadamente los riesgos asociados a sus activos de información y cumplir con requisitos legales, regulatorios y contractuales.

Definición de Alcance

Alcance

El SGSI cubrirá:

- Gestión académica y administrativa
- Datos personales y académicos de estudiantes y personal
- Infraestructura cloud y recursos TI
- Infraestructura tecnológica y comunicaciones
- Gestión de pagos y datos financieros

Activos de Información

Activo	Tipo	Importancia
Base de datos de estudiantes	Información	Crítico
Servidores Cloud (AWS, GCP, Azure)	Infraestructura	Crítico
Backups de información crítica	Información	Crítico
CRM	Sistema	Crítico
Sistema de Gestión del Aprendizaje (LMS)	Sistema	Alto
Sistema de correo institucional	Servicio	Alto
Repositorios de código	Información	Alto
Sistema de pagos y facturación	Sistema	Alto
Equipo de cómputo del personal	Hardware	Medio
Sitio Web Institucional	Servicio	Medio
Herramientas de comunicación	Servicio	Medio

Límites Físicos

- Oficinas principales de 4Geeks

- Estaciones de trabajo del personal de TI
- Dispositivos portátiles autorizados
- Áreas restringidas con acceso controlado

Acceso Restringido

- Acceso administrativo a entornos cloud
- Acceso a bases de datos
- Oficinas de gestión de TI
- Espacios con archivos físicos sensibles

Límites Virtuales

- Sistemas internos como CRM, LMS
- Infraestructura en la nube
- Plataformas de pago
- Canales de comunicación digitales

Sistemas y Tipo bajo control del SGSI

- Datos personales
- Expedientes académicos e históricos
- Datos de facturación y pagos de estudiantes
- Contraseñas y credenciales de acceso

Partes Interesadas

Parte Interesada	Responsabilidad
Dirección de 4Geeks	Apoyo estratégico, aprobación de políticas
Departamento de TI	Implementación de controles y mantenimiento
Docentes y Estudiantes	Cumplimiento de políticas y buenas prácticas
Equipo de soporte	Gestión operativa y accesos

Limitación y Exclusión

- Excluye servicios no contratados directamente por la organización.
- No se considera información personal almacenada en dispositivos personales no autorizados.
- El SGSI no cubre datos de terceros fuera del entorno de 4Geeks.

Evaluación de Riesgos

Activo	Categoría	Amenaza Potencial	Vulnerabilidades

Base de datos de estudiantes	Datos	Robo de identidad, exposición de datos	Acceso amplio, sin cifrado, mala gestión de roles
Servidores Cloud (AWS, GCP, Azure)	Infraestructura	Acceso no autorizado, interrupciones, malware	Claves expuestas, falta de monitoreo, mal uso de roles IAM
Backups de información crítica	Información	Pérdida de datos, corrupción, acceso no autorizado	Backups sin cifrado, no verificados, acceso débil
CRM	Software	Fuga de información, manipulación de registros	Contraseñas débiles, permisos mal asignados
Sistema de Gestión del Aprendizaje (LMS)	Software	Ataques DDoS, robo de credenciales	Autenticación débil, software no actualizado
Sistema de correo institucional	Software	Phishing, malware	Filtros poco efectivos, usuarios mal entrenados
Repositorios de código	Información	Fuga de propiedad intelectual, ataques por código expuesto	Acceso sin revisión, claves expuestas
Sistema de pagos y facturación	Software	Fraude, fuga de información sensible	Privilegios mal asignados, falta de registro de auditoría
Equipo de cómputo del personal	Hardware	Robo físico, infección por malware	Dispositivos sin cifrado, antivirus desactualizado
Sitio Web Institucional	Software	Defacement, inyección SQL	Software CMS desactualizado, validación pobre
Herramientas de comunicación	Servicio	Suplantación de identidad, fuga de conversaciones	Accesos sin MFA, uso de enlaces públicos, historial expuesto

Riesgo	Probabilidad	Impacto	Nivel de Riesgo

Acceso no autorizado a CRM, LMS o servidores cloud	Alta	Crítico	Alto
Pérdida o corrupción de backups	Media	Crítico	Alto
Robo de identidad, exposición de datos	Media	Crítico	Alto
Repositorios públicos o sin control de acceso	Medio	Alto	Alto
Ataques DDoS, robo de credenciales	Media	Medio	Medio
Phishing, malware	Alta	Medio	Alto
Fraude en sistema de pagos o fuga de datos financieros	Media	Alto	Alto
Robo físico, infección por malware	Media	Bajo	Medio
Defacement, inyección SQL	Media	Bajo	Medio
Suplantación o filtración en herramientas de comunicación	Alta	Medio	Alta

Selección de Controles

Riesgo	Control	Descripción	Referencia
Acceso no autorizado a	Autenticación multifactor (MFA)	Se añade una capa adicional de	ISO 27001 A.5.15

CRM, LMS o servidores cloud		seguridad para el acceso	
Robo de datos de estudiantes	Cifrar los datos y realizar backups	Protege la confidencialidad de los datos en tránsito y reposo	ISO 27001 A.8.24
Phishing por correo institucional	Filtrado avanzado de correo y realizar capacitación al personal	Bloquear correos sospechosos y realizar formaciones sobre ciberataques	CIS Control 14
Repositorios públicos sin control	Revisión de permisos	Previene fugas de código o exposición de credenciales	NIST CM-6
Fraude en sistema de pagos	Control en las funciones y auditoría de accesos	Evita accesos indebidos y errores en la gestión de información financiera	ISO 27001 A.5.17
Inyección SQL en sitio web	Validación de entradas y pruebas periódicas	Prevención de inyecciones y vulnerabilidades en web	NIST SI-10
Pérdida o corrupción de backups	Backup cifrado, automatizado y verificado	Asegura disponibilidad e integridad de la información crítica	ISO 27001 A.5.30
Robo de equipos	Cifrado de disco y bloqueo remoto	Protege datos si el dispositivo se pierde o es robado	CIS Control 1
Filtración en herramientas de comunicación	MFA y gestión de enlaces y permisos por canal	Asegura entornos de colaboración contra suplantaciones o fuga de información	ISO 27001 A.9.4.2

Plan de Implementación

Control	Tiempo	Recursos	Dependencia

Autenticación multifactor (MFA) en LMS, CRM, cloud	1 mes	Licencia de software, soporte técnico	Capacitación, políticas
Cifrado de datos y backups	2 meses	Herramientas de cifrado y revisión de infraestructura cloud	Auditoria de datos
Filtros de correo y capacitación	3 semanas	Software y material educativo	Recursos y apoyo de RRHH
Plan de recuperación (DRP)	2 meses	Personal técnico, documentación	Backups actualizados y verificados
Revisión de permisos en GitHub, CRM y LMS	3 semanas	Checklists, auditorías manuales o automatizadas	Roles definidos, integración con IAM si aplica
Seguridad web (SQL injection)	Constante	Pentesting, desarrollo seguro	Entorno de pruebas
Formación en ciberseguridad	Permanente	Charlas, evaluaciones	Aprobación del rectorado
Cifrado de disco y bloqueo remoto	1 mes	Software de gestión (MDM), configuración remota	Inventario actualizado, aprobación de TI

Documentación de Políticas y Procedimientos de Seguridad

Se busca establecer el compromiso institucional con la protección de la información, asegurando su confidencialidad, integridad y disponibilidad.

Con los siguientes objetivos:

- Alcance en la política: aplicarlo a todo el personal, estudiantes y sistemas.
- Principios: confidencialidad de datos personales y financieros, integridad de la información académica y administrativa.
- Cumplimiento normativo: referencias a leyes nacionales y normas ISO/NIST/CIS.

Gestión de Accesos

Procedimiento:

- Solicitud de acceso: formulario gestionado por TI.
- Modificación de accesos: tras cambios de rol o departamento.
- Revocación de acceso: inmediata al terminar relación laboral, contractual o académica.

Controles:

- Principio de mínimo privilegio aplicado a todos los roles.
- Políticas de contraseñas:
    - Longitud mínima: 12 caracteres.
    - Complejidad: letras, números, símbolo, mayúscula.
    - Cambio obligatorio cada 90 días.
    - No repetir últimas 5 contraseñas.
- Autenticación multifactor (MFA) para sistemas críticos.

Respuesta a Incidentes

Es cualquier evento que comprometa la seguridad de la información, incluyendo accesos no autorizados, malware, fuga de datos, suplantación de identidad, etc.

Procedimiento:

- Identificar el incidente.
- Notificación inmediata.
- Evaluación de impacto.
- Contención y erradicación.
- Recuperación del servicio.
- Documentación y lecciones aprendidas.

Roles:

- Usuario afectado: reporta de forma inmediata.
- Equipo TI: realiza acciones de contención y recuperación.
- Responsable de SGSI: coordina, comunica y documenta.
- Dirección: aprueba acciones mayores o legales.

Copia de Seguridad y Backups

Política:

- Frecuencia: diaria para bases de datos críticas, semanal para sistemas administrativos.
- Retención: mínimo 30 días.
- Ubicación: cifrado local y copia en nube institucional segura.
- Verificación: pruebas de restauración mensuales.

Responsables:

- Personal TI asignado.
- Validaciones auditadas trimestralmente por SGSI.

Concienciación y Capacitación

Plan de formación:

- Capacitaciones obligatorias para todo el personal (mínimo 1 vez por año).
- Simulacros de phishing 2 veces al año.
- Curso virtual para estudiantes sobre seguridad digital en el campus.

Materiales de concienciación:

- Infografías digitales en plataformas internas (Slack)
- Guías prácticas: uso seguro del correo, configuración de MFA, detección de correos sospechosos.

Aprobación y Revisión

Aprobación: todas las políticas deben ser revisadas y aprobadas por el Comité de Seguridad de la Información y la Dirección General.

Revisiones periódicas: mínimo una vez al año o tras incidentes graves o cambios tecnológicos.

Documentación: cada documento debe tener número de versión, fecha y responsables de su redacción o aprobación.

Monitoreo y Medición

El SGSI se basa en el ciclo PHVA (Planificar - Hacer - Verificar - Actuar):

- Planificar: Identificación de activos críticos, evaluación de riesgos, definición de políticas, controles y procedimientos de seguridad.
- Hacer: Implementación de los controles técnicos y administrativos, según el plan establecido.
- Verificar: Monitoreo continuo de eventos de seguridad, cumplimiento de políticas, revisiones periódicas, auditorías técnicas y evaluar el desempeño del SGSI.
- Actuar: Corregir desviaciones, mejorar controles y actualizar procedimientos
- Indicadores de desempeño (KPIs): número de incidentes, tiempo de respuesta, cumplimiento de backups, asistencia a capacitaciones.