Manual SGSI 4Geeks Academy

Valentina Alcubillas Arango
30/01/2026
4Geeks Academy

Índice

Introducción

El presente Manual del **Sistema de Gestión de Seguridad de la Información (SGSI)** establece el marco organizativo, técnico y procedimental para la protección de la información gestionada por la organización **dedicada** a la formación tecnológica, en adelante la empresa. Este manual tiene como finalidad garantizar la **confidencialidad**, **integridad** y **disponibilidad** de la información, así como asegurar la continuidad de los servicios educativos y operativos.

El SGSI se desarrolla conforme a los principios establecidos en la norma **ISO/IEC 27001:2022** y se adapta al contexto de una **entidad educativa** con fuerte dependencia de **plataformas digitales**, **servicios en la nube y entornos colaborativos**.

Alcance del SGSI

El SGSI es de aplicación a todos los sistemas, procesos, servicios y personas que intervienen en la gestión de la información de la empresa. El alcance incluye, entre otros:

- Plataformas educativas y de gestión académica.
- Sistemas web corporativos y dominios digitales.
- Infraestructura tecnológica y servicios en la nube.
- Información de estudiantes, personal, docentes y colaboradores.
- Proveedores y terceros con acceso a los sistemas.

Quedan excluidos del alcance los sistemas personales no autorizados y aquellos entornos no relacionados con la actividad educativa u operativa de la organización.

Contexto organizativo y partes interesadas

La organización desarrolla su actividad en un **entorno digital altamente distribuido**, con alcance internacional y dependencia de tecnologías en la nube. Este contexto implica riesgos asociados a la disponibilidad de los servicios, la protección de datos personales, la seguridad de accesos remotos y la continuidad operativa.

La naturaleza online de los servicios educativos exige elevados niveles de fiabilidad, cumplimiento normativo y protección de la información. Por ello, se implanta un SGSI formal que permita gestionar de manera sistemática los riesgos de seguridad.

Las principales partes interesadas identificadas incluyen estudiantes, personal docente y administrativo, equipo técnico, proveedores tecnológicos, socios comerciales y organismos reguladores. Las necesidades y expectativas de estas partes se consideran en el diseño, implementación y mejora continua del SGSI.

Compromiso de la Dirección La dirección de 4Geeks Academy se compromete a:

- Proporcionar los recursos necesarios para el mantenimiento del SGSI.
- Promover una cultura de "Seguridad por Diseño" en el desarrollo de sus plataformas.
- Revisar anualmente la eficacia de los controles frente a amenazas emergentes como el ransomware y la ingeniería social.

Inventario de activos

El inventario de activos recoge de forma estructurada los elementos que soportan las actividades educativas, administrativas y tecnológicas de la organización, permitiendo aplicar medidas de seguridad proporcionales a su criticidad y valor para el negocio.

Activos de información

Incluyen datos académicos de estudiantes (inscripciones, evaluaciones, progreso y certificaciones), información personal y de contacto de alumnos, docentes y personal interno, así como información administrativa, contractual y financiera.

También forman parte de estos activos los contenidos formativos digitales, materiales didácticos, grabaciones de clases, documentación técnica, políticas internas, procedimientos, credenciales de acceso, claves de autenticación, registros de actividad y copias de seguridad. Su pérdida, alteración o divulgación no autorizada podría afectar gravemente a la operación, reputación y cumplimiento normativo.

Activos de software

Comprenden plataformas de **aprendizaje en línea (LMS),** sistemas de gestión académica, aplicaciones administrativas y financieras, herramientas de comunicación y **colabora**ción, sistemas de autenticación y repositorios de código.

Estos activos soportan procesos críticos del negocio y requieren una gestión segura de configuraciones, actualizaciones, accesos y monitorización para reducir riesgos de explotación de vulnerabilidades o interrupciones del servicio.

Activos de infraestructura y servicios

Incluyen servidores virtuales en la nube, servicios de almacenamiento y bases de datos, redes, balanceadores de carga, certificados digitales, sistemas de copia de seguridad y servicios de monitorización.

Asimismo, se consideran los servicios prestados por proveedores externos, cuya disponibilidad y seguridad resultan esenciales para garantizar la continuidad y escalabilidad de los servicios educativos.

Activos humanos

Incluyen al personal técnico, equipo docente, personal administrativo, responsables de seguridad y proveedores con acceso autorizado. El factor humano constituye un elemento clave tanto en la correcta aplicación de los controles de seguridad como en la prevención de incidentes derivados del error humano.

Roles y responsabilidades

La implantación y mantenimiento del SGSI exige una asignación clara de roles y responsabilidades dentro de la organización:

- **Dirección**: Es responsable de aprobar el SGSI, garantizar su alineación con los objetivos estratégicos de la empresa y proporcionar los recursos necesarios para su implantación, mantenimiento y mejora continua.
- **Responsable de Seguridad de la Información:** Este rol coordina el SGSI, supervisa el cumplimiento de las políticas de seguridad, gestiona la evaluación de riesgos y lidera la respuesta ante incidentes de seguridad, actuando como punto de referencia en materia de seguridad de la información.
- **Equipo técnico:** El equipo técnico es responsable de implementar y mantener los controles de seguridad definidos, administrar los sistemas, gestionar accesos, realizar copias de seguridad y asegurar la disponibilidad y correcto funcionamiento de los servicios.
- **Personal docente y administrativo:** El personal docente y administrativo debe cumplir las políticas y procedimientos de seguridad, hacer un uso adecuado de los sistemas de información y notificar cualquier incidente o anomalía detectada.
- **Proveedores y terceros:** Los terceros con acceso a sistemas o información están obligados a cumplir los requisitos de seguridad establecidos por la empresa, de acuerdo con los contratos y acuerdos de confidencialidad suscritos.

Segregación de funciones

Rol	Funciones Principales	Restricciones de segregación
Dirección	Aprobación del SGSI y asignación de recursos	No interviene en la operación técnica diaria
Responsable de Seguridad de la Información	Supervisión del SGSI y gestión de riesgos	No administra sistemas productivos
Equipo Técnico	Administración de sistemas y controles técnicos	No aprueba políticas ni excepciones
Personal Docente	Administración de sistemas y controles técnicos	No gestiona accesos ni configuraciones
Personal Administrativo	Gestión operativa y académica	No administra infraestructuras críticas
Proveedores	Soporte técnico específico	Acceso limitado y supervisado

Evaluación y tratamiento de riesgos

La evaluación de riesgos se realiza siguiendo un enfoque basado en activos, identificando amenazas, vulnerabilidades y el impacto potencial sobre la organización.

Proceso de evaluación de riesgos

La evaluación de riesgos se realiza siguiendo un enfoque basado en activos, identificando amenazas, vulnerabilidades y el impacto potencial sobre la organización. Los riesgos se valoran en función de su probabilidad e impacto, permitiendo su priorización y tratamiento mediante controles adecuados.

Análisis y evaluación del riesgo

El análisis se realiza de forma sistemática y documentada, permitiendo determinar el nivel de riesgo y establecer prioridades de tratamiento alineadas con los objetivos del SGSI.

Criterios de impacto

El impacto se evalúa en función de las consecuencias potenciales sobre la confidencialidad, integridad y disponibilidad de la información, así como sobre la continuidad del servicio, la reputación y el cumplimiento normativo.

Nivel	Descripción
Nivel	Impacto significativo en la operación, reputación o cumplimiento legal
Medio	Impacto moderado con afectación limitada y recuperable
Bajo	Impacto reducido sin afectación relevante

Criterios de probabilidad

La probabilidad se determina considerando la frecuencia histórica, la exposición a la amenaza y la existencia de controles preventivos.

Nivel	Descripción
Alto	Alta probabilidad de ocurrencia
Medio	Ocurrencia posible
Bajo	Ocurrencia poco probable

Matriz de riesgos

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de riesgo
Contenidos del portal	Acceso no autorizado	Controles de acceso insuficientes	Alto	Medio	Alto
Credenciales administrativas	Phishing	Falta de concienciación	Alto	Alto	Crítico
Plataforma web	Fallo del servicio	Dependencia del proveedor	Medio	Medio	Medio
Registros de actividad	Manipulación	Falta de monitoreo	Medio	Bajo	Bajo

Controles de seguridad seleccionados

Los controles seleccionados responden a los riesgos identificados y se implementan de forma proporcional, garantizando un equilibrio entre seguridad, operatividad y viabilidad técnica.

La selección de controles se ha realizado considerando los siguientes criterios:

- Nivel de riesgo asociado a cada activo.
- Impacto potencial sobre la reputación, continuidad educativa y operativa.
- Viabilidad técnica y organizativa.
- Madurez del entorno tecnológico existente.

CTRL 01 - Control de accesos lógicos

Este control limita el acceso a los sistemas únicamente a usuarios autorizados mediante autenticación robusta y gestión individual de credenciales. Se aplica el principio de mínimo privilegio y se realizan revisiones periódicas de accesos para reducir el riesgo de accesos indebidos o no autorizados.

CTRL 02 - Gestión de identidades y privilegios

Se establecen procesos formales para la gestión del ciclo de vida de las identidades digitales, incluyendo altas, modificaciones y bajas. Los privilegios se asignan según el rol y se revisan periódicamente para evitar accesos innecesarios o desactualizados.

CTRL 03 - Protección de la integridad de la información

Se implementan controles que previenen la modificación no autorizada o accidental de la información académica y administrativa. Estos incluyen restricciones de edición, control de versiones y validación de cambios, garantizando la fiabilidad de la información.

CTRL 04 - Registro y monitorización de actividades

Se mantienen registros de eventos relevantes asociados al acceso y uso de los sistemas. La monitorización permite detectar comportamientos anómalos, facilitar la investigación de incidentes y apoyar procesos de auditoría y mejora continua.

CTRL 05 - Disponibilidad y continuidad del servicio

Se aplican medidas de redundancia, copias de seguridad y planes de recuperación ante incidentes. El objetivo es minimizar interrupciones y asegurar la continuidad de los servicios educativos y operativos críticos.

CTRL 06 - Concienciación y formación en seguridad

Se desarrollan programas de formación y concienciación dirigidos al personal, orientados a promover el uso seguro de los sistemas, la protección de credenciales y la detección temprana de amenazas como el phishing.

Planificación de implementación de controles seleccionados

La implementación de los controles de seguridad se realiza de forma progresiva y priorizada, en función del nivel de riesgo identificado:

- **Fase inicial:** controles de acceso, autenticación y gestión de identidades.
- **Fase intermedia:** refuerzo de registros, monitoreo, integridad de la información y disponibilidad de servicios.
- **Fase continua:** concienciación, revisiones periódicas y optimización del SGSI.

Política de Prevención de Pérdida de Datos (DLP)

La organización implementa políticas de Data Loss Prevention (DLP) con el objetivo de prevenir la pérdida, filtración o uso no autorizado de información sensible. Estas políticas se basan en la clasificación de la información y en la aplicación de controles técnicos y organizativos adecuados.

Los datos se clasifican en públicos, privados y sensibles, aplicando medidas proporcionales a su criticidad. Se establecen controles de cifrado, monitoreo del uso de la información, restricciones de transferencia y concienciación del personal. La política DLP contribuye a reducir fugas accidentales o intencionadas y refuerza el cumplimiento normativo en materia de protección de datos.

Nivel	Descripción	Ejemplos
Pública	Información sin restricciones	Contenidos web
Interna	Uso exclusivo interno	Documentación operativa
Sensible	Datos protegidos	Datos personales, credenciales

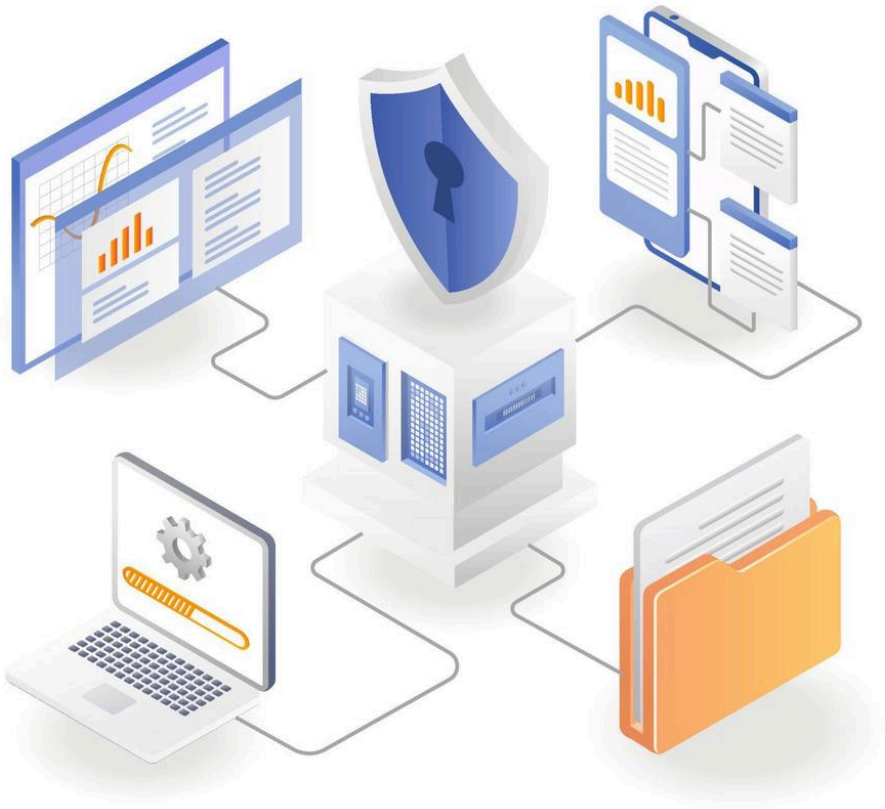
Medidas DLP aplicadas

- Cifrado de datos sensibles en tránsito y en reposo
- Restricciones de descarga y compartición
- Monitoreo del uso de información crítica
- Concienciación del personal
- Control de accesos basado en roles

Estas medidas reducen el riesgo de fuga de información y refuerzan el cumplimiento normativo.

Implementación Técnica de DLP

- **Nivel de Red (Symantec DLP):** Monitorización de archivos enviados por correo electrónico o subidos a nubes externas. Bloqueo automático si se detectan patrones de tarjetas de crédito o IDs de alumnos.
- **Nivel de Endpoint (Digital Guardian):** Instalación de agentes en las laptops del personal para evitar el volcado de bases de datos MariaDB a memorias USB no autorizadas.



Gestión de incidentes de seguridad

Gestión de incidentes NIST

El SGSI se apoya en el marco NIST Cybersecurity Framework, estructurando la gestión de la seguridad en las funciones Identify, Protect, Detect, Respond y Recover. Este enfoque permite una visión integral del riesgo, facilitando la identificación de activos y amenazas, la implementación de controles preventivos, la detección temprana de incidentes, una respuesta estructurada y la recuperación efectiva de los servicios afectados, fortaleciendo la resiliencia operativa de la organización.

Identificar

En esta fase se identifican los activos de información, procesos críticos, dependencias tecnológicas y riesgos asociados. Se analizan amenazas, vulnerabilidades y requisitos legales con el objetivo de comprender el contexto de riesgo de la organización. Esta información sirve como base para la priorización de controles y la planificación de respuestas ante incidentes.

Proteger

La fase de protección incluye la implementación de controles preventivos destinados a limitar o evitar la materialización de incidentes. Entre estos controles se incluyen la gestión de accesos, autenticación robusta, concienciación del personal, protección de datos (DLP), copias de seguridad y políticas de seguridad. Estas medidas reducen la probabilidad de impacto sobre los activos críticos.

Detectar

La detección se basa en mecanismos de monitoreo continuo, análisis de registros y alertas automáticas que permiten identificar eventos anómalos o comportamientos sospechosos. Una detección temprana resulta clave para reducir el alcance de los incidentes y facilitar una respuesta rápida y eficaz.

Responder

La respuesta contempla la activación de procedimientos formales para el análisis, contención y erradicación del incidente. Se asignan responsabilidades, se coordinan acciones técnicas y se comunica la información relevante a las partes interesadas internas, garantizando una gestión ordenada y documentada del incidente.

Recuperar

La fase de recuperación tiene como objetivo restaurar los servicios afectados y asegurar la vuelta a la normalidad operativa. Incluye la recuperación desde copias de seguridad, la validación de sistemas y la aplicación de mejoras para evitar la recurrencia del incidente, fortaleciendo la continuidad del negocio.

Plan de Respuesta a Incidentes

La organización dispone de un Plan de Respuesta a Incidentes alineado con el marco NIST, cuyo objetivo es garantizar una actuación coordinada, eficaz y documentada ante cualquier evento que comprometa la seguridad de la información.

Fases del plan de respuesta

Fase	Descripción
Detección	Identificación del incidente mediante alertas, monitoreo o notificación del personal
Análisis	Evaluación del tipo de incidente, alcance, activos afectados e impacto potencial
Contención	Aplicación de medidas inmediatas para limitar la propagación del incidente
Erradicación	Eliminación de la causa raíz del incidente
Recuperación	Restauración de sistemas y servicios afectados
Cierre	Documentación del incidente y validación de la recuperación

Roles durante un incidente

Rol	Responsabilidades
Responsable SGSI	Coordinación general y toma de decisiones
Equipo Técnico	Contención, erradicación y recuperación
Dirección	Aprobación de acciones críticas y comunicación externa
Personal afectado	Notificación y colaboración

Lecciones aprendidas

Tras la resolución de cada incidente, se realiza un análisis posterior con el objetivo de identificar deficiencias en los controles, oportunidades de mejora y acciones preventivas. Las lecciones aprendidas se documentan y se integran en el proceso de mejora continua del SGSI, reforzando la madurez del sistema.

Monitoreo, medición y mejora continua

El monitoreo de los controles incluye la supervisión de la correcta aplicación de las medidas de seguridad, mediante revisiones periódicas de accesos, análisis de configuraciones, verificación de copias de seguridad y revisión de registros de actividad.

La medición del desempeño del SGSI permite evaluar el grado de cumplimiento de las políticas establecidas, detectar desviaciones y facilitar la toma de decisiones orientadas a la mejora continua y a la reducción del riesgo.

Indicadores del SGSI

Indicador	*Descripción*	*Frecuencia*	*Responsable*
Incidentes registrados	Número de incidentes de seguridad detectados	Trimestral	Responsable SGSI
Revisiones de accesos	Accesos revisados y validados	Semestral	Equipo Técnico
Copias de seguridad verificadas	Pruebas de restauración realizadas	Anual	Equipo Técnico
Formación en seguridad	Personal capacitado	Anual	RRHH
Cumplimiento de políticas	Nivel de cumplimiento de políticas internas	Anual	Responsable SGSI
Tiempo medio de resolución	Tiempo medio de cierre de incidentes	Trimestral	Responsable SGSI
Acciones correctivas cerradas	% de acciones cerradas	Trimestral	Responsable SGSI

Acuerdo de Nivel de Servicio (SLA)

El **Acuerdo de Nivel de Servicio (SLA)** establece los compromisos de la organización en relación con la gestión de incidentes de seguridad y operativos que puedan afectar a la disponibilidad, integridad o confidencialidad de los servicios. Este acuerdo define tiempos de respuesta, planificación y resolución en función de la criticidad del incidente, permitiendo una actuación coordinada y eficaz. El SLA constituye un elemento clave para garantizar la continuidad del servicio y la confianza de los usuarios.

Objetivo del SLA

El SLA define los compromisos de la organización en relación con los tiempos de respuesta, planificación y resolución de incidentes de seguridad y operativos, asegurando una gestión acorde a la criticidad del incidente.

Niveles de prioridad

Prioridad	Tiempo de respuesta	Tiempo de planificación	Tiempo de resolución
Crítica	1 horas	2 horas	8 horas
Alta	2 horas	4 horas	16 horas
Media	4 horas	8 horas	24 horas
Baja	8 horas	16 horas	48 horas

Disponibilidad de los servicios

Los servicios críticos asociados a los activos tecnológicos deben mantener altos niveles de disponibilidad, apoyados por infraestructura en la nube, mecanismos de redundancia y procedimientos de recuperación que minimicen interrupciones y garanticen la continuidad del aprendizaje y la gestión académica.

Gestión de no conformidades y acciones correctivas

La organización establece un proceso formal para la identificación, registro y tratamiento de no conformidades detectadas en el SGSI, ya sea como resultado de auditorías, incidentes de seguridad, revisiones internas o desviaciones operativas.

Para cada no conformidad identificada se realiza un análisis de causa raíz y se definen acciones correctivas orientadas a eliminar su origen y prevenir su recurrencia. El seguimiento de estas acciones forma parte del proceso de mejora continua del SGSI.

Competencia, concienciación y comunicación

Competencia		
Rol	**Requisitos de competencia**	**Requisitos de competencia**
Responsable SGSI	Formación en seguridad	Certificados
Equipo Técnico	Conocimientos técnicos	Formación técnica
Personal general	Uso seguro de sistemas	Registros de formación

Concienciación		
Acción	**Frecuencia**	**Público objetivo**
Formación básica en seguridad	Anual	Todo el personal
Simulaciones de phishing	Anual	Personal con acceso
Difusión de buenas prácticas	Trimestral	Todo el personal

Comunicación		
Tipo de comunicación	**Canal**	**Responsable**
Incidentes de seguridad	Correo / ticket	Responsable SGSI
Cambios en políticas	Correo interno	Dirección
Alertas de seguridad	Plataforma interna	Equipo Técnico

Gestión documental

La organización establece un sistema de gestión documental que garantiza la correcta creación, control, aprobación y actualización de la documentación del SGSI, asegurando su disponibilidad, integridad y confidencialidad.

Documento	Responsable	Revisión	Acceso
Manual SGSI	Dirección	Anual	Restringido
Políticas de seguridad	Responsable SGSI	Anual	Restringido
Procedimientos	Equipo Técnico	Anual	Controlado
Registros de incidentes	Responsable SGSI	Trimestral	Restringido
Evaluaciones de riesgos	Responsable SGSI	Anual	Restringido

Revisión y mejora continua

El SGSI se revisa de forma periódica y siempre que se produzcan cambios significativos en el entorno tecnológico, organizativo y normativo. Estas revisiones permiten evaluar la eficacia de los controles implementados, analizar incidentes y resultados de auditorías, y actualizar la evaluación de riesgos.

Los resultados obtenidos sirven como base para la mejora continua del sistema, asegurando su adaptación a la evolución de las amenazas, tecnologías y necesidades operativas de la organización.

Conclusiones

El manual establece un marco integral y coherente para la gestión de la seguridad de la información dentro de la organización. La definición clara de roles, controles, procesos y niveles de servicio permite reducir los riesgos identificados, proteger los activos críticos y garantizar la continuidad de los servicios educativos. Este documento constituye la base para la mejora continua del SGSI y refuerza el compromiso de la empresa con la seguridad de la información y el cumplimiento normativo.

Anexo - Glosario

Palabra	Descripción
Activo	Elemento que tiene valor para la organización y requiere protección.
Amenaza	Evento o circunstancia que puede causar un incidente de seguridad.
Vulnerabilidad	Debilidad que puede ser explotada por una amenaza.
Impacto	Consecuencia de la materialización de un riesgo sobre la organización.
Probabilidad	Posibilidad de que una amenaza explote una vulnerabilidad.
Riesgo	Combinación de la probabilidad y el impacto de un incidente.
SGSI	Sistema de Gestión de Seguridad de la Información.
SLA	Acuerdo de Nivel de Servicio que define tiempos y compromisos de respuesta.
CIA	Confidencialidad, Integridad y Disponibilidad