Plan de respuesta a incidentes y certificación

Versión	Fecha	Autor	Descripción
v.01	04/06/2025	Luis F. Gómez Guzmán	Fase 3 Proyecto final

Índice

1. Plan de respuesta a incidentes (NIST SP 800-61) 3
2. Sistema de gestión de Seguridad de la información (SGSI) 8

1. Plan de respuesta a incidentes (NIST SP 800-61)

Dado que 4Geeks Academy ofrece formación en tecnología y ciberseguridad, es fundamental contar con un plan de respuesta a incidentes que proteja la integridad de sus sistemas y datos.

Plan de respuesta a incidentes de

Seguridad de la información

Versión	Fecha de aprobación	Revisión prevista	Responsable
1.0	dd/mm/aaaa	Anualmente o tras incidentes significativos	CISO / Responsable de Seguridad de la información

1. Objetivo

Establecer un marco formal para identificar, gestionar y mitigar los incidentes de seguridad que afecten a los sistemas de información, infraestructuras y datos gestionados por 4Geeks Academy, de acuerdo con la guía NIST SP 800-61r2 y conforme al principio de responsabilidad proactiva del RGPD.

2. Alcance

Este plan aplica a todo el personal, infraestructuras, servicios, proveedores y sistemas que participen en el tratamiento o almacenamiento de información dentro del ámbito de 4Geeks Academy.

3. Definiciones

- **Incidente de seguridad:** Evento que compromete o amenaza la confidencialidad, integridad o disponibilidad de la información.
- **SIEM:** Sistema de gestión de eventos e información de seguridad.
- **EDR/XDR:** Herramientas para detección y respuesta en endpoints/redes.
- **Equipo de respuesta a incidentes:** Grupo designado para gestionar incidentes, liderado por el Responsable de Seguridad.

4. Preparación

- Inventario actualizado de activos críticos (plataformas LMS, servidores, backups).
- Definición de roles y responsabilidades (ver tabla RACI en Anexo I).
- Simulacros periódicos y ejercicios de concienciación.
- Manuales de comunicación interna y externa.
- Proveedores y SLA documentados.

5. Identificación y análisis

- Monitorización con SIEM e IDS/IPS.
- Detección de anomalías y alertas sospechosas.
- Categorización del incidente (p. ej. malware, DDoS, fuga de datos).
- Asignación de nivel de severidad (crítico, alto, medio, bajo).
- Registro inmediato en plataforma de ticketing.
- Notificación interna y activación del equipo de respuesta.

6. Contención

- Segmentación de redes y aislamiento de sistemas comprometidos.
- Revocación de accesos comprometidos.
- Aplicación de parches y configuraciones seguras.
- Preservación de evidencias digitales conforme a ISO/IEC 27037.

7. Erradicación

- Eliminación del código malicioso (uso de EDR/XDR).
- Análisis de logs para identificar vectores de ataque.
- Refuerzo de controles y reglas en los sistemas afectados.

8. Recuperación

- Restauración de sistemas desde respaldos verificados.
- Pruebas de integridad y escaneos de vulnerabilidades.

- Validación de normalidad operativa.
- Notificación a la AEPD si procede (art. 33 RGPD).

9. Lecciones aprendidas

- Documentación del incidente y de todas las actuaciones.
- Reunión de análisis postincidente.
- Actualización del plan y mejora continua.
- Revisión de controles, formación y contratos con terceros.

10. Anexos

Anexo I – Matriz RACI

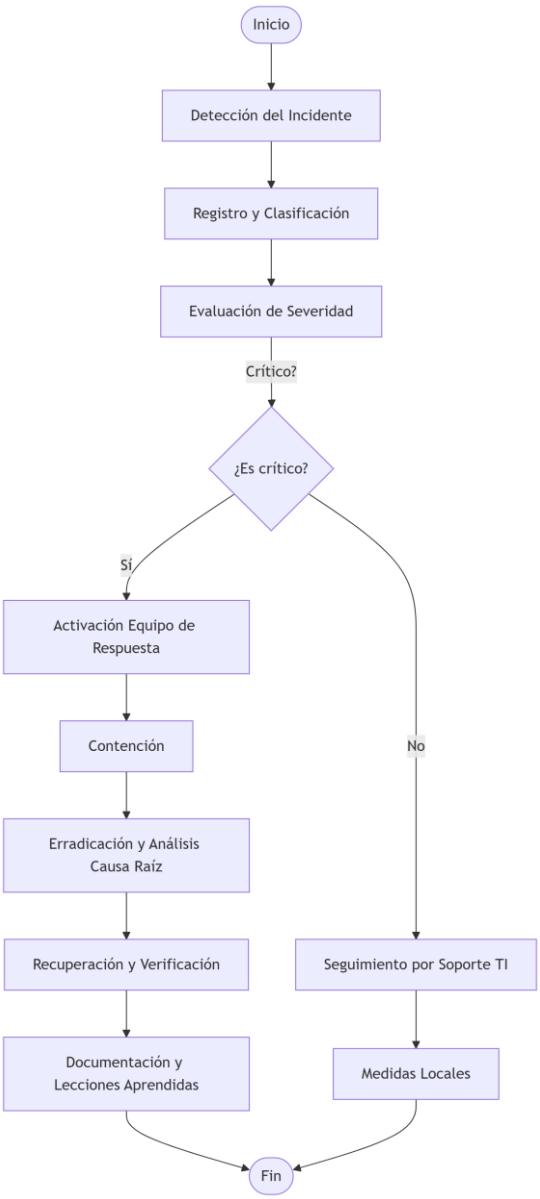
Actividad / Rol	CISO	Equipo Técnico	Compliance	Dirección	Soporte TI
Identificación del incidente	R	A	C	I	I
Análisis y clasificación	A	R	C	I	I
Contención y erradicación	C	R	I	I	A
Comunicación interna y externa	R	C	A	C	I
Notificación a la AEPD	A	C	R	I	I
Lecciones aprendidas	R	A	C	C	I

Anexo II – Clasificación de incidentes

Tipo de Incidente	Descripción breve
Acceso no autorizado	Acceso indebido a cuentas, sistemas o datos
Malware	Infección por software malicioso

DDoS	Ataques de denegación de servicio
Pérdida de datos	Eliminación o filtración de información sensible
Phishing / Ingeniería social	Suplantación de identidad y manipulación del personal
Fallo de disponibilidad	Interrupción accidental de servicios críticos

Anexo III – Flujograma de actuación



Anexo IV – Procedimiento de notificación a la AEPD

1. Evaluar si el incidente afecta a datos personales.

2. Valorar el riesgo para los derechos y libertades de los afectados.
3. Si procede, notificar a la AEPD en un plazo máximo de 72 horas desde que se tiene constancia.
4. La notificación debe incluir:
    a. Naturaleza del incidente
    b. Categorías y volumen de datos afectados
    c. Medidas adoptadas o propuestas
    d. Datos de contacto del responsable de protección de datos
5. Documentar todas las actuaciones, incluso si no se notifica.

Anexo V – Checklists por tipo de incidente

Incidente: Malware

- Aislar el dispositivo afectado
- Ejecutar análisis con herramienta EDR
- Recolectar evidencias
- Eliminar malware
- Restaurar desde backup si necesario

Incidente: Acceso no autorizado

- Cambiar credenciales comprometidas
- Revisar logs de acceso
- Notificar a los usuarios afectados
- Verificar si se accedió o alteró información sensible

Incidente: Pérdida de datos

- Confirmar tipo de datos perdidos
- Analizar causa raíz
- Recuperar datos desde respaldo
- Evaluar necesidad de notificar a la AEPD

Este documento forma parte del Sistema de Gestión de Seguridad de la Información (SGSI) de 4Geeks Academy y será revisado al menos una vez al año o tras cada incidente significativo.

2. Sistema de gestión de Seguridad de la información (SGSI)

La Política global de seguridad de 4Geeks Academy es un reflejo del compromiso institucional con la confianza, la innovación y el desarrollo seguro.

Esta política y su marco normativo, refuerza el compromiso de 4Geeks Academy con la creación de un entorno educativo digital seguro, resiliente y transparente, protegiendo tanto a su comunidad como a los activos estratégicos que sustentan su misión.

En un entorno donde la tecnología es una herramienta y también un activo muy valioso, asegurar la integridad y el uso responsable es esencial para el cumplimiento de la misión educativa.

A) Política global de seguridad de la información

Política global de Seguridad de la información

Introducción

En un entorno cada vez más digital, la seguridad de la información se ha convertido en un pilar estratégico para 4Geeks Academy. Como institución educativa global con presencia en múltiples países y enfocada en la formación en tecnología, asumimos la responsabilidad de proteger tanto los datos personales de nuestros estudiantes y colaboradores, como la integridad de nuestros activos digitales y tecnológicos.

Nuestra Política Global de Seguridad establece los principios, la estructura organizativa y los planes estratégicos que guían este compromiso. Este documento refleja nuestra intención de crear un entorno de aprendizaje y operación seguro, resiliente y alineado con las mejores prácticas internacionales en materia de ciberseguridad, privacidad y cumplimiento regulatorio.

La política será revisada periódicamente para asegurar que se mantiene actualizada y efectiva frente a la evolución de las amenazas, las necesidades de la comunidad académica y los requisitos regulatorios vigentes.

Principios de seguridad de 4Geeks Academy

Nuestra estrategia de seguridad se basa en los siguientes principios fundamentales:

1. Principio de legalidad

4Geeks Academy cumple con todas las leyes y regulaciones aplicables en materia de protección de datos, ciberseguridad y privacidad, tanto a nivel local como internacional, en cada una de las jurisdicciones donde opera.

2. Principio de prevención y proactividad

Adoptamos un enfoque preventivo, anticipándonos a las amenazas mediante análisis de riesgos continuos y actualizados. Implementamos controles de seguridad adecuados para reducir los riesgos a niveles aceptables, asegurando la continuidad de nuestras operaciones académicas y administrativas.

3. Principio de corresponsabilidad

La seguridad es responsabilidad de todos. Todo el personal, instructores, estudiantes y colaboradores deben asumir un compromiso activo con la protección de la información y los recursos digitales de la organización, siguiendo los procedimientos, normativas internas y buenas prácticas definidas por 4Geeks Academy.

4. Principio de cooperación

Fomentamos una cultura de seguridad colaborativa entre nuestras sedes, equipos técnicos, académicos y administrativos. La coordinación eficiente entre las distintas unidades garantiza respuestas integradas ante posibles incidentes y fortalece nuestras capacidades colectivas de protección.

Organización de la seguridad

La estructura de seguridad en 4Geeks Academy está diseñada para ser flexible, eficiente y adaptada a las necesidades propias de una organización educativa tecnológica.

Responsable de Seguridad de la Información (RSI): Cada sede o región contará con un Responsable de Seguridad designado, que actuará como enlace entre la dirección global de seguridad y las operaciones locales. Este perfil podrá adaptarse según el contexto tecnológico y regulatorio del país correspondiente.

Dirección de Tecnología y Seguridad: A nivel global, la estrategia y las políticas de seguridad son lideradas por la Dirección de Tecnología y Seguridad de la Información, que se encarga de definir directrices, coordinar su implementación y supervisar la adopción de estándares.

Comité de Seguridad y Privacidad: Este comité, compuesto por miembros clave de las áreas académica, tecnológica y administrativa, se reúne periódicamente para evaluar riesgos, establecer prioridades y desarrollar planes estratégicos de seguridad. Además, supervisa la respuesta ante incidentes y la actualización de protocolos.

Reportes y Transparencia: La Dirección de Seguridad reportará a la alta dirección de 4Geeks Academy sobre el estado de la seguridad de la información, propondrá mejoras continuas y garantizará la transparencia en los procesos relacionados con protección de datos y gestión de incidentes.

Marco normativo de seguridad

El Marco Normativo de Seguridad de 4Geeks Academy es una guía integral que forma parte de nuestra política organizativa general en materia de protección de la información, ciberseguridad y privacidad. Este marco regula aspectos clave como la organización funcional y territorial de la seguridad, las funciones asignadas a los diferentes actores dentro de la organización, así como los principios operativos que guían nuestra actuación.

Objetivos del marco

El objetivo fundamental de este marco es asegurar un entorno tecnológico seguro, confiable y conforme con las normativas internacionales, permitiendo la ejecución eficaz de nuestras actividades educativas y operativas. Para lograrlo, el marco define:

- Los objetivos y metas de seguridad alineados con los valores y el plan estratégico de 4Geeks Academy.
- Los requisitos de seguridad mínimos aplicables a todas nuestras plataformas, sistemas, sedes y herramientas de gestión académica.
- Las tecnologías y controles por implementar para proteger los datos, prevenir incidentes y garantizar la integridad de la información.
- El cumplimiento obligatorio de todas las leyes locales e internacionales en materia de ciberseguridad y protección de datos personales.
- La inclusión de cláusulas contractuales de seguridad en los acuerdos con colaboradores, proveedores y socios estratégicos.

El marco está diseñado para aplicarse de forma global, pero con adaptaciones locales que respeten las particularidades regulatorias y tecnológicas de cada país en el que 4Geeks Academy opera, sin comprometer los estándares mínimos definidos por la dirección global de seguridad.

Gobernanza y aplicación

La Dirección de tecnología y seguridad de la información de 4Geeks Academy tiene la autoridad para definir, interpretar y desarrollar los principios generales de este marco normativo. A su vez, los responsables de seguridad regionales o locales tienen autonomía para elaborar normativas específicas ajustadas a su contexto, siempre en coherencia con la política general.

Para garantizar su correcta aplicación, el marco será difundido mediante:

- Programas de concienciación y formación dirigidos al personal, instructores y estudiantes.
- Materiales divulgativos y campañas internas, orientados a fortalecer la cultura de la seguridad digital en toda la comunidad académica.

Planes estratégicos de seguridad y auditoría

El desarrollo e implementación de los planes estratégicos de seguridad son responsabilidad de la Dirección de tecnología y seguridad, que lidera su elaboración, seguimiento y mejora continua. Estos planes:

- Identifican, priorizan y planifican proyectos clave de seguridad a corto, medio y largo plazo.
- Definen el presupuesto necesario para implementar medidas de protección efectivas y sostenibles.
- Incluyen mecanismos de seguimiento y evaluación del cumplimiento de las políticas internas y los objetivos de ciberseguridad.

Además, se establecen procedimientos de auditoría interna a cargo de la Dirección administrativa y de control, o terceros autorizados, para:

- Verificar el cumplimiento normativo y técnico del marco de seguridad.
- Detectar vulnerabilidades u oportunidades de mejora.
- Formular recomendaciones correctivas y preventivas que se integren en los ciclos de mejora continua.