SGSI: 4GEEKS ACADEMY

Nicolás Oriol Sengáriz

4Geeks

Índice

Alcance del SGSI

Activos de información

- **Inventario:** computadoras de profesores y personal, servidores de centros de datos, bases de datos de registros académicos (estudiantes), propiedad intelectual de proyectos y sistemas financieros.
- **Clasificación:** utiliza cuatro niveles de protección:
    - **P1 (Mínimo):** directorios de campus, programas de cursos, comunicados de prensa.
    - **P2 (Bajo):** presupuestos de departamentos, políticas internas en borrador.
    - **P3 (Moderado):** registros de estudiantes, evaluaciones de desempeño de empleados.
    - **P4 (Alto):** datos de tarjetas de crédito y de cuentas bancarias, propiedad intelectual como Learnpack o Rigobot.

Límites físicos

- **Ubicaciones:** todas las academias y oficinas administrativas.
- **Áreas restringidas:** centros de datos del campus, armario donde se guarde la propiedad intelectual.

Límites virtuales

- **Redes:** redes locales (LAN) y redes inalámbricas de cada academia.
- **Nube:** entornos en Amazon Web Services (AWS), Azure y Google Cloud.
- **Sistemas:** sistemas de gestión de aprendizaje (Learnpack y Rigobot) y plataformas de correo institucional (Google Workspace/Office 365).

Partes interesadas

- **Equipo de TI/Seguridad:** CISO y equipo de ciberseguridad que también hace de CERT.
- **Gestión:** CISO y dueño de la empresa.
- **Empleados:** profesorado y personal administrativo.
- **Estudiantes:** estudiantes de un curso.
- **Responsabilidades:** los "dueños de los datos" deben clasificar la información, mientras que los "protectores" (TI) deben implementar las medidas de protección.

Alcance del SGSI

- **Propósito:** proteger la confidencialidad, integridad y disponibilidad de los activos de información que respaldan la misión de enseñanza de la academia.
- **Objetivos:** cumplimiento con regulacione, además de reducción de riesgos de ciberataques.
- **Limitaciones o exclusiones:** podrían excluirse redes de invitados (Wi-Fi público) o dispositivos personales que no acceden a datos nivel P3 o P4 de ciertos controles estrictos.

Evaluación de riesgos

Clasificación de activos

- **Hardware:** ordenadores, servidores de datos y equipos de red.
- **Software:** plataforma de aprendizaje (Learnpack), Rigobot y la web de la academia.
- **Datos:** expedientes de estudiantes, propiedad intelectual de proyectos y datos financieros.
- **Personal:** personal administrativo, profesores, estudiantes y proveedores externos con acceso a sistemas.

Origen de amenazas potenciales

- **Externo:** ransomware dirigido a servidores de datos, ataques de phishing para robar credenciales de acceso institucional y suplantación de personal de proveedores.
- **Interno:** fuga de datos accidental o no accidental por trabajadores (profesores o personal administrativo), mal uso de privilegios de administrador y pérdida o robo de dispositivos físicos (portátiles/móviles) no cifrados.

Tipo de vulnerabilidad

- **Técnicas:** sistemas operativos sin actualizar con el último parche, programas sin actualizar a la última versión, falta de autenticación multifactor (MFA) en aplicaciones críticas y bases de datos con configuraciones de seguridad débiles.
- **Organizativas:** falta de capacitación en ciberseguridad para nuevos empleados y procesos lentos de baja de empleados que mantienen accesos activos tras su salida, offboarding deficiente.

Probabilidad

- **Alta**: sistemas operativos sin actualizar con el último parche, programas sin actualizar a la última versión.
- **Media**: falta de autenticación multifactor (MFA) en aplicaciones críticas y bases de datos con configuraciones de seguridad débiles
- **Baja**: falta de capacitación en ciberseguridad para nuevos empleados y procesos lentos de baja de empleados que mantienen accesos activos tras su salida, offboarding deficiente.

Impacto

- **Compromiso de datos sensibles y multas**: falta de autenticación multifactor (MFA) en aplicaciones críticas y bases de datos con configuraciones de seguridad débiles
- **Compromiso de datos sensibles y daño a la reputación**: sistemas operativos sin actualizar con el último parche, programas sin actualizar a la última versión.
- **Daño a la reputación**: falta de capacitación en ciberseguridad para nuevos investigadores y procesos de baja de empleados lentos que mantienen accesos activos tras su salida, offboarding deficiente.

Nivel de riesgo

- **Riesgo alto:** falta de autenticación multifactor (MFA) en aplicaciones críticas y bases de datos con configuraciones de seguridad débiles
- **Riesgo medio:** sistemas operativos sin actualizar con el último parche, programas sin actualizar a la última versión.
- **Riesgo bajo:** falta de capacitación en ciberseguridad para nuevos investigadores y procesos lentos de baja de empleados que mantienen accesos activos tras su salida, offboarding deficiente.

Metodología de evaluación de riesgos

El proceso de evaluación de riesgos consiste en los siguientes pasos:

Primero hay que tener clasificados los datos.

Una vez los datos ya están clasificados se procede a rellenar el formulario de la página: https://forms.gle/pBEEcwDZZGDfC3So8

Las imágenes de abajo son del formulario

Selección de controles

Normas relevantes

La academia de 4Geeks no inventa sus propios controles, sino que los alinea con estándares internacionales y regulaciones específicas.

- **Regulaciones sectoriales:**
    - **NIST 800-171:** requerido para proteger información no confidencial controlada en contratos de investigación federal.
    - **PCI-DSS:** para cualquier unidad que procese pagos con tarjeta de crédito.
    - **FERPA:** para la protección de expedientes académicos de estudiantes.

Selección de controles

- **Autenticación Multifactor (MFA):** obligatorio uso de MFA en el 100% de sistemas de correo y aplicaciones críticas.
- **Cifrado de información:** obligatorio para que toda la información institucional esté protegida, ya sea en reposo o en movimiento, y para el 100% de los dispositivos (ordenadores de sobremesa, portátiles y móviles).
- **Endpoint Detection and Response (EDR):** instalación obligatoria de EDRs en el 100% de los activos para monitorear amenazas en tiempo real.
- **Firewalls:** uso de firewalls para filtrar el tráfico de entrada hacia las redes de la universidad y hacia los servidores con información clasificada.
- **Gestión de vulnerabilidades:** escaneos periódicos y aplicación de parches de seguridad obligatorios en todos los sistemas operativos y aplicaciones.

Documentación de la implementación de los controles

A continuación, se realiza una lista de los controles a implementar, qué riesgo mitigará y cómo mitigará el riesgo correspondiente:

- El uso del **MFA** sirve para autenticar que la persona autorizada a acceder es realmente la que dice ser, este control ayuda a evitar el acceso no autorizado.
- **Cifrado de información** sirve para proteger la información en caso de un ciberataque, si no cuentan con la clave de cifrado no pueden leer la información de los archivos, de esta manera se evitan filtraciones accidentales o no accidentales de empleados o ataques de ransomware de ciberdelincuentes.
- El **EDR** sirve para detectar una intrusión de forma rápida y así evitar la propagación del ataque, de esta manera se evitan ataques de ransomware de ciberdelincuentes.
- **Firewalls** sirve para detectar una intrusión de forma rápida y así evitar la propagación del ataque, de esta manera se evitan ataques de ransomware de ciberdelincuentes.
- **Gestión de vulnerabilidades** consiste en realizar escaneos periódicos y aplicar parches de seguridad en todos los sistemas operativos y aplicaciones, así se ayuda a evitar intrusiones de ciberdelincuentes.

Planificación de la implementación

El orden de implementación es el siguiente:

1. **MFA**
    a. **Recursos:** suscripciones a plataformas (Duo Security, Okta) y personal de soporte para ayudar a miles de estudiantes y profesores con el proceso y funcionamiento.
    b. **Requisitos:** definir una política de acceso donde se nombren las aplicaciones que requieran obligatoriamente del MFA.

2. **Cifrado**
    a. **Recursos:** software de cifrado (BitLocker para Windows, FileVault para macOS) y sistemas de gestión de claves (Key Management Systems) para no perder el acceso a los datos.
    b. **Requisitos:** tener una clasificación de datos para saber cuáles son P3 y P4 para priorizar su cifrado, los ordenadores deben tener chips TPM en las placas base.

3. **Firewall**
    a. **Recursos:** firewalls de nueva generación.
    b. **Requisitos:** presupuesto aprobado para la compra de licencias para el uso de firewalls de nueva generación.

4. **EDR**
    a. **Recursos:** tener agentes de software (ej. CrowdStrike, SentinelOne) instalados en cada equipo (endpoint) y un SOC para analizar las alertas las 24h del día, los 7 días de la semana y los 365 días o 366 días del año.
    b. **Requisitos:** se debe tener un inventario completo, no se puede proteger lo que no se sabe que existe; se requiere una lista total de dispositivos conectados.

5. **Gestión de vulnerabilidades**
    a. **Recursos:** Herramientas de escaneo (ej. Nessus, Qualys). Tiempo de los administradores de sistemas para aplicar parches (reboot de servidores).
    b. **Requisitos:** se deben crear ventanas de mantenimiento que consisten en acuerdos con los departamentos para apagar sistemas y actualizarlos sin afectar la investigación. Además, se deben tener permisos de escaneo, el CISO o un alto cargo de la universidad debe firmar una autorización legal y técnica para escanear redes.

Políticas y procedimientos de seguridad

Política de Seguridad

El objetivo es establecer el marco de gobernanza para proteger los activos de información de la academia contra amenazas internas y externas.

- 4Geeks Academy se compromete a proteger la confidencialidad, integridad y disponibilidad de la información que sustenta la excelencia académica.
- Esta política es de cumplimiento obligatorio para todo el personal (docente y administrativo), estudiantes con acceso a la web y proveedores externos.
- El SGSI se alinea con el estándar ISO/IEC 27001.

Política de Control de Acceso y Gestión de Identidades

Basado en el principio de **Mínimo privilegio.**

- **Ciclo de vida de la cuenta:**
    - **Alta (Onboarding):** verificación de identidad obligatoria antes de crear el usuario, contraseña y asignación de permisos necesarios para realizar su trabajo adecuadamente.
    - **Modificación:** ajuste de permisos inmediato si el empleado cambia de departamento.
    - **Baja (Offboarding):** desactivación automatizada en menos de 24 horas tras la terminación del contrato.
- **Autenticación robusta:** uso de **MFA (Duo Security)** para todos los sistemas de correo y aplicaciones críticas.
- **Cuentas superprivilegiadas:** los administradores de sistemas deben usar cuentas separadas de sus cuentas de usuario estándar para tareas de mantenimiento.
- **Política de contraseñas:** se debe usar Bitwarden para guardar las contraseñas, se deben crear de forma aleatoria con una longitud mínima de 16 caracteres con una letra mayúscula, una letra minúscula, un número y un símbolo especial. Además, deben ser cambiadas cada 6 meses.

Plan de Respuesta a Incidentes

Un incidente consiste en un ciberataque ya sea con éxito o sin éxito a un sistema, equipo, servidor o red, normalmente explotando una vulnerabilidad.

- **Fases del incidente:**
    1. **Detección:** alertas provenientes del EDR o reportes de usuarios.
    2. **Contención:** aislamiento de sistemas afectados para evitar que el ataque se propague.
    3. **Erradicación:** eliminación de la causa raíz del ataque.
    4. **Recuperación:** restauración de servicios desde backups verificados.
    5. **Verificación:** se comprueba que la restauración del backup funcione correctamente.
    6. **Informe post-incidente:** se habla sobre el ataque y cómo corregir la vulnerabilidad involucrada en el ataque.

El SOC tiene la responsabilidad de detectar y responder a los incidentes priorizando los exitosos sobre los no exitosos.

El CISO tiene la responsabilidad de comunicarlo a las autoridades pertinentes y a los afectados, ya sean empleados, estudiantes o proveedores.

Política de continuidad y copias de seguridad (Backups)

Asegura que la academia pueda seguir operando tras un desastre ya sea natural o un ciberataque.

Las copias de seguridad se deben hacer según criticidad de los datos, para los datos **P4** se deben realizar copias de seguridad diarias, para los datos **P3** se deben realizar copias de seguridad una vez por semana, para los datos **P2** se deben realizar copias de seguridad cada 15 días, para los datos **P1** se deben realizar copias de seguridad cada 30 días.

El proceso de realizar las copias de seguridad se puede automatizar mediante un cronjob, al principio interesa verificar que el cronjob realiza el backup de lo que se le pide, así no habrá sustos más adelante.

Se seguirá la estrategia 3-2-1 para realizar las copias de seguridad, la **estrategia 3-2-1** significa lo siguiente: 3 copias de datos, en 2 medios diferentes, con 1 copia fuera del sitio (Cloud o Bóveda).

Todos los respaldos de datos (backups) **P3 y P4** deben estar cifrados en movimiento y en reposo.

Se deben realizar simulacros de pruebas de restauración trimestrales para asegurar que las copias de seguridad no están corruptas y pueden restaurarse.

Programa de concientización y cultura de ciberseguridad

- **Entrenamiento inicial:** módulo obligatorio al entrar a trabajar o a estudiar donde se explican las políticas de seguridad y las responsabilidades que tienen los usuarios, tiene que ser antes de recibir acceso a los sistemas institucionales.
- **Talleres sobre seguridad en la red:** todo el mundo sería obligado a realizarlo y se haría cada 3 meses.
- **Campañas de phishing:** pruebas mensuales para identificar a usuarios vulnerables y ofrecerles recapacitación.
- **Boletines de amenazas:** comunicación mensual sobre nuevas estafas detectadas en el entorno universitario.

Control y revisión de documentos

Para que el SGSI sea válido bajo **ISO 27001**, debe estar controlado.

- **Historial de versiones:** cada documento sobre la política en ciberseguridad debe incluir una tabla con fechas, autores y cambios realizados.
- **Revisión anual:** todo procedimiento debe ser revisado al menos una vez al año, cuando ocurra un cambio significativo en la tecnología de la universidad o después de un ciberataque para ver cómo mejorar e implementar esa mejora y redactar cómo ha quedado todo después de los cambios, quizás se ha cambiado de EDR y hay que escribir sobre el nuevo EDR.
- **Aprobación formal:** firma digital del CISO y del dueño de la academia, así se certifica que la versión está revisada por un experto en ciberseguridad y que un alto cargo del personal no experto en ciberseguridad conoce el cambio o mejora en la política de ciberseguridad.
- **Auditoría:** el cumplimiento de estos seis puntos será auditado internamente cada año por el CISO y por una unidad externa cada tres años para mantener la certificación de ISO 27001.

Roles y responsabilidades

El **CISO** supervisa y valida que se implementen los controles del SGSI de la forma adecuada, además también supervisa el cumplimiento del SGSI y las auditorías internas y externas que se realizan para cumplir con la normativa y la certificación.

El **equipo de ciberseguridad** realiza la implementación de los controles establecidos.

Este equipo de ciberseguridad también es el CERT.

Los líderes de la academia están comprometidos con el SGSI ya que quieren evitar multas económicas cuantiosas, quieren mantener el buen nombre de la academia y porque todo el mundo se merece tener privacidad ya que los datos pertenecen a sus dueños y a los que el dueño quiera contar.

Monitoreo y medición de la efectividad del SGSI

El SGSI se monitoreará y se medirá su efectividad y cada 6 meses el CISO y el dueño de la academia tendrán una reunión para hablar de cómo les ha ido con el SGSI, si se ha tenido que hacer algún cambio para mejorarlo, así habrá una mejora continua

La estrategia de monitoreo y medición consiste en lo siguiente:

- **Monitoreo continuo:** vigilancia técnica de redes, logs y alertas en tiempo real.
- **Revisiones periódicas:** auditorías internas y revisiones del CISO.
- **Análisis de eficacia:** comparar los resultados obtenidos contra los objetivos de seguridad establecidos al inicio del año.

Se deben incluir KPIs para poder medir mejor la eficacia del SGSI.

Se clasifican los KPIs en tres grupos ya que no todos los indicadores están relacionados, al separarlos en tres grupos se puede distribuir el trabajo y se puede hacer más rápido.

KPIs

Gestión de vulnerabilidades

Indicador	Objetivo
Porcentaje de Parcheo	% de activos críticos actualizados en menos de 48h desde el aviso.
Densidad de Vulnerabilidades	Número de vulnerabilidades críticas abiertas por cada 100 activos.
Tiempo Medio de Detección (MTTD)	Tiempo promedio desde que ocurre un incidente hasta que el equipo lo identifica.

Respuesta a incidentes

Indicador	Objetivo
Tiempo Medio de Respuesta (MTTR)	Tiempo promedio para mitigar o resolver un incidente una vez detectado.
Eficacia de los backups	% de restauraciones exitosas durante las pruebas trimestrales.
Frecuencia de incidentes críticos	Cantidad de brechas de seguridad que impactaron la disponibilidad del negocio.

Cultura y cumplimiento

Indicador	Objetivo
Tasa de éxito en Phishing	% de empleados que "caen" en simulacros internos de correos maliciosos.
Nivel de capacitación	% de la plantilla que ha completado la formación anual de seguridad.
Cumplimiento de los proveedores	% de proveedores críticos que han firmado y cumplen los acuerdos de seguridad (SLAs).