Desarrollo de un Sistema Básico de Gestión de Seguridad de la Información (SGSI) para una Organización Pública ficticia.

Paso 1: Selección de organización pública.

La organización escogida para el desarrollo del SGSI será una universidad pública ficticia de tamaño medio.
La universidad gestiona información sensible que incluyen datos personales, expedientes académicos, información financiera y datos de investigación.

Paso 2: Definición del alcance.

Identificar Activos de Información

- Datos:
  - Expedientes académicos.
  - Datos personales de empleados y estudiantes.
  - Información financiera.
- Hardware:
  - Servidores de bases de datos.
  - PCs administrativos.
  - Discos duros externos.
- Software:
  - Plataforma de gestión.
  - Web universidad.
  - Aula virtual.
- Personal:
  - Personal IT
  - Profesores
  - Alumnos

Definir límites físicos

- Edificio administrativo
- Centro de datos principal
- Facultades
- Departamentos
- Salas informática (acceso público)
- Salas servidores (acceso privado)

Definir límites virtuales

- Red interna de la universidad.
- Servidores locales
- Servicios en la nube
- Máquinas virtuales.

Identificación Partes Interesadas

- Dirección (Aprobación del SGSI)
- Equipo IT (Implementación y mantenimiento)
- Personal Administrativo (Uso de los sistemas de manera segura)
- Profesores (Protección de información académica)
- Alumnos (Uso responsable de servicios y equipos)

Alcance SGSI

El alcance del SGSI incluye los equipos, sistemas, redes, ubicaciones y personal importantes para el correcto funcionamiento del sistema de la universidad. De esta manera se consigue una gestión mas efectiva de los riesgos frente a fallas de seguridad.

Paso 3: Evaluación de Riesgos

Lista inventario de Activos

- Datos.
- Hardware
- Software.
- Personal.

Identificar Amenazas Potenciales

Prioridad	Activo afectado	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Ni Ri
1	Expedientes Academicos	Acceso No Autorizado	Contraseñas débiles	Alta	Alto	Alt
2	Plataforma Académica	Ataque malware	Sistemas desactualizados	Media	Alto	Alt
3	Servidores	Pérdida de datos	Falta copias de seguridad	Media	Alto	Alt
4	Red Interna	Ataque Externo	Firewall mal configurado	Media	MEdio	Me
5	Personal	Ingenieria Social	Falta de formación	Alta	Medio	Alt

Prioridad	Activo afectado	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Ni Ri
6	Sistemas en la nube	Fuga de información	Mala/Incorrecta configuración	Media	Alto	Alt
7	Infraestructura	Desastres naturales	Falta plan de contingencia	Baja	Alto	Me

Paso 4: Selección de Controles

Normas Relevantes

Prioridad	Riesgo	Control seleccionado	Tipo de control	Referencia ISO 27001
1	Acceso no autorizado	Control de accesos y autenticación multifactor	Técnico	A.5.15, A.5.17
2	Malware	Antivirus y gestión de parches	Técnico	A.8.7, A.8.8
3	Pérdida de datos	Copias de seguridad periódicas	Técnico/Organizativo	A.8.13
4	Firewall mal configurado	Reglas de firewall y segmentación de red	Técnico	A.8.20
5	Ingeniería social	Formación y concienciación	Organizativo	A.6.3
6	Fuga de información en la nube	Cifrado y control de acceso	Técnico	A.8.24
7	Desastres naturales	Plan de continuidad de negocio	Organizativo	A.5.29

Controles Seleccionados

- **Control de acceso y autenticacion**
  - Uso de credenciales únicas por cada usuario.
  - Implementación de autenticación multifactor.
  - Revisión periódica de permisos.
- **Protección frente a malware**
  - Instalación de antivirus actualizado.

    - Políticas de actualización automática de sistemas.
    - Restricción de ejecución de software no autorizado.
- **Copias de Seguridad**
    - Backups diarios de información crítica.
    - Almacenamiento cifrado.
    - Pruebas periódicas de restauración.
- **Firewall**
    - Definición de reglas restrictivas.
    - Segmentación de la red académica y administrativa.
    - Monitorización del tráfico.
- **Formación y concienciación**
    - Programas anuales de formación.
    - Simulaciones de phishing.
    - Material de concienciación accesible.
- **Seguridad en la nube**
    - Cifrado de datos en tránsito y reposo.
    - Acceso basado en roles.
    - Revisión periódica de configuraciones.
- **Continuidad del negocio**
    - Plan de contingencia documentado.
    - Identificación de servicios críticos.
    - Pruebas anuales del plan.

Implementación de Controles

Rol	Responsabilidad
Dirección	Aprobar políticas y recursos
Responsable de Seguridad	Supervisar el SGSI
Equipo IT	Implementar controles técnicos
Usuarios	Cumplir políticas
Auditor interno	Revisar cumplimiento

Plan Implementación

Control	Responsable	Prioridad	Plazo
Multifactor	IT	Alta	1 mes
Antivirus	IT	alta	1 mes

Control	Responsable	Prioridad	Plazo
Backups	IT	Alta	1 mes
Firewall	IT	Media	2 meses
Formación	RRHH/IT	Media	3 meses
Continuidad	Dirección/IT	Media	3 meses

Paso 5: Documentación de Políticas y Procedimientos de Seguridad

Politica de Seguridad

- **Principios fundamentales:**
  - **Confidencialidad**: La información solo será accesible por personal autorizado.
  - **Integridad**: La información será protegida contra modificaciones no autorizadas.
  - **Disponibilidad**: La información estará disponible cuando sea requerida.
- **Aplicabilidad:**
  - Esta política se aplica a todos los empleados, estudiantes, proveedores y terceros que tengan acceso a los sistemas de información de la universidad.

Control de Acceso de Usuarios

- **Gestion de usuarios y accesos**
  - Acceso a los sistemas se concede según el principio de mínimo privilegio.
  - Cada usuario dispone de credenciales únicas.
  - Los accesos se revisan periódicamente.
  - Los accesos se revocan cuando un usuario deja la organización.
- **Política de contraseñas**
  - Longitud mínima de 8 caracteres.
  - Combinación de letras, números y símbolos.
  - Cambio periódico de contraseñas.
  - Prohibido compartir credenciales.

Respuesta Incidentes

- **Incidentes:**
  - Acceso no autorizado.
  - Malware.
  - Pérdida o filtración de datos.
  - Caídas de sistemas críticos.
- **Procedimiento gestión incidentes:**

    - Detección del incidente.
    - notificación al equipo de IT o responsable de seguridad.
    - Análisis y contención del incidente.
    - Erradicación y recuperación.
    - Documentación y lecciones aprendidas.
- **Roles:**
    - **Responsable de seguridad**: Coordinación.
    - **Equipo de IT**: Análisis técnico.
    - **Dirección**: Decisiones estratégicas.

Copia de seguridad y Recuperación de Datos

- **Procedimientos de backup:**
    - Copias de seguridad periódicas de los sistemas críticos.
    - Almacenamiento cifrado de los backups.
    - Al menos una copia fuera del entorno principal.
    - Pruebas periódicas de restauración.
- **Responsables:**
    - Equipo IT.

Concienciación y Capacitación de Empleados

- **Plan de capacitación:**
    - Formación anual obligatoria en seguridad de la información.
    - Sesiones específicas para personal con acceso a datos sensibles.
    - Campañas de concienciación (phishing, contraseñas, uso seguro del correo).
- **Objetivo:**
    - Reducir riesgos derivados del factor humano.

Aprobación y Revision de Documentos

- Todas las políticas serán aprobadas por dirección.
- Revisión periódica.
- Actualización en función de cambios tecnológicos o normativos.

Paso 6: Manual de SGSI

Documentación

Propósito del Manual

Este manual describe el Sistema de Gestión de Seguridad de la Información (SGSI) implementado en la universidad pública ficticia, con el objetivo de proteger la información

frente a amenazas internas y externas, garantizar la continuidad de los servicios y cumplir con los requisitos legales y normativos aplicables.

Alcance del SGSI

- Sistemas académicos y administrativos.
- Infraesctrucura IT.
- Datos de estudiantes y empleados.
- Servicios en la nube.
- Instalaciones críticas.

Objetivos del SGSI

- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Identificar y mitigar riesgos de seguridad.
- Cumplir normativas aplicables.
- Establecer un proceso de mejora continua.

Roles y Responsabilidades

Rol	Responsabilidad
Dirección	Aprobar políticas y recursos
Responsable del SGSI	Coordinar y supervisar el SGSI
Equipo de IT	Implementar controles técnicos
Usuarios	Cumplir políticas
Auditor Interno	Revisar el SGSI

Metodología de Evaluación de Riesgos

Clasificación de riesgos

Impacto/Probabilidad	Baja	Media	Alta
Bajo	Riesgo Bajo	Riesgo Bajo	Riesgo Medio
Medio	Riesgo Bajo	Riesgo Medio	Riesgo Alto
Alto	Riesgo Medio	Riesgo Alto	Riesgo Alto

Controles de Seguridad Implementados

- Técnicos.
- Organizativos.

- Físicos.

Políticas y Procedimientos

- Política de Seguridad de la Información.
- Control de accesos.
- Gestión de incidentes.
- Copias de seguridad.
- Formación y concienciación.

Monitoreo y Medición del SGSI

Indicador Clave (KPIs)	Descripción
Incidentes detectados	Número mensual
Tiempo de respuesta	Tiempo medio de resolución
Sistemas actualizados	Porcentaje de cumplimiento
Formación completada	Porcentaje de personal formado

Mejora Continua del SGSI

- Auditorías internas.
- Revisión de riesgos.
- Actualización de políticas.

Documentación y Registros

- Manual del SGSI.
- Informes de riesgos.
- Informes de auditoría.
- Registros de incidentes.

Paso 7: Revisión y Presentación del SGSI.

Revisión del SGSI

Revision del alcance y objetivos

- El alcance cubre:
  - Infraestructura IT.
  - Datos personales y académicos.
  - Personal y terceros.
  - Servicios críticos.

Revisión de la evaluación de riesgos

- Verificaciones realizadas:
  - Riesgos documentados y clasificados.
  - Riesgos altos priorizados.
  - Controles asignados a cada riesgo.

Revisión de controles de seguridad

- Controles alineados con ISO 27001.
- Roles y responsabilidades definidos.
- Plan de implementación documentado.

Revisión de políticas y procedimientos

- Política de seguridad.
- Control de accesos.
- Gestión de incidentes.
- Copias de seguridad.
- Formación.

Preparación de presentación del SGSI

Estructura de presentación

- Introducción y objetivos del SGSI.
- Alcance del SGSI.
- Resultados de la evaluación de riesgos.
- Controles de seguridad implementados.
- Políticas y procedimientos.
- Beneficios del SGSI.
- Próximos pasos y mejora continua.

Riesgos clave identificados

Los principales riesgos identificados están relacionados con el acceso no autorizado a información sensible, la posibilidad de incidentes de malware, la falta de concienciación del personal y la dependencia de sistemas críticos para la actividad académica.

Medidas de mitigación destacadas

- Implementación de controles de acceso.
- Protección frente a malware.
- Copias de seguridad periódicas.
- Formación y concienciación.

- Planes de continuidad.

Areas de Mejora Futura

Como parte del proceso de mejora continua del SGSI, se han identificado áreas de mejora futura que permitirán fortalecer la seguridad de la información de la universidad.

- Auditorías internas periódicas.
- Automatización de monitoreo de seguridad.
- Mejora de controles en la nube.
- Simulacros de incidentes de seguridad.
- Certificación ISO 27001 a largo plazo.

Conclusión

El desarrollo del SGSI para la universidad pública ficticia proporciona una base sólida para la gestión de la seguridad de la información, permitiendo identificar y mitigar riesgos de manera sistemática. Este sistema fomenta una cultura de seguridad, mejora la resiliencia organizativa y sienta las bases para una mejora continua alineada con estándares internacionales.