T3. SGSI: Gestión de la seguridad

Garantía y Seguridad de la Información.

Gestión de la seguridad

- Seguridad informática
  - protección de las infraestructuras de las tecnologías de la información y comunicación que soportan nuestro negocio.
- Seguridad de la información
  - protección de los **activos** de información fundamentales para el éxito de cualquier organización.
    - correos electrónicos, páginas web, imágenes, bases de datos, faxes, contratos, presentaciones, documentos...

- Lo que hoy es crítico para nuestro negocio puede dejar de tener importancia con el tiempo.

Gestión de la seguridad

- Política.
  - ¿Cómo establecer un marco de trabajo con el que satisfacer las necesidades de seguridad en la organización?
- Planificación.
  - ¿Cómo conocer si nuestra implementación satisface las necesidades de seguridad actuales y futuras?
- Análisis de riesgos.
  - ¿Cómo ponderar los beneficios de los controles (de seguridad) frente a sus costes y cómo justificar algunos controles?
- Control físico.
  - ¿Qué aspectos del entorno de computación tienen un impacto en la seguridad?

3.1 Estándares de Gestión de Seguridad

SGSI

Sistema de Gestión de Seguridad de la Información

- Una herramienta de gestión que nos va a permitir
  - conocer
  - gestionar
  - minimizar
- los posibles riesgos que atenten contra la *seguridad de la información* en nuestra empresa
- para preservar la confidencialidad, integridad y disponibilidad de la misma
  - en el interior de la empresa
  - ante nuestros clientes y
  - ante las distintas partes interesadas en nuestro negocio

Sistema de Gestión de Seguridad de la Información

- Analizar y ordenar la *estructura de los sistemas* de información.
- Facilitar la definición de *procedimientos de trabajo* para mantener su seguridad.
- Disponer de controles que permitan *medir la eficacia* de las medidas tomadas.
- Con el objetivo:
  - *Proteger la organización frente a amenazas y riesgos*
    - garantizar competitividad, rentabilidad y conformidad legal
    - mantener el riesgo por debajo del nivel asumible

Riesgos

- Físicos
  - Incendios, inundaciones, terremotos o vandalismo
    - Afectan a la disponibilidad de nuestra información y recursos.
- Lógicos
  - Relacionados con la propia tecnología
    - Hackers, robos de identidad, spam, virus, robos de información, espionaje industrial…
    - Acaban con la confianza de nuestros clientes y nuestra imagen en el mercado.

Beneficios de un SGSI

- Reducción de riesgos y de amenazas
  - si se produce una incidencia, los daños se *minimizan* y la continuidad del negocio está asegurada.
- Ahorro de costes por racionalización de los recursos.
  - Se eliminan inversiones innecesarias e ineficientes producidas por desestimar o sobrestimar riesgos.
- Cumplimiento de la legislación vigente
  - Sin costes innecesarios.
- Mejora de la competitividad en el mercado
  - más fiables
  - incremento del prestigio.
- La seguridad se transforma en un ciclo de vida metódico y controlado

Familia ISO/IEC 27000

- Facilita la implantación de un SGSI
- ¿A quién le interesa?
  - ¿Qué importancia tienen los activos de información dentro de la organización como elementos imprescindibles para la obtención de sus objetivos?
- Norma 27000
  - visión general de las normas que componen la serie 27000
  - introducción a los Sistemas de Gestión de Seguridad de la Información
  - breve descripción del proceso *Plan-Do-Check-Act*
  - términos y definiciones que se emplean en toda la serie 27000

Familia ISO/IEC 27000

- Norma 27001
  - norma principal de la serie
  - componentes del SGSI, documentos que forman parte de él y registros que demuestran el buen funcionamiento del sistema
  - norma con arreglo a la cual se certifican los SGSI de las organizaciones

Familia ISO/IEC 27000

- Norma 27002
  - guía de buenas prácticas
    - describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Familia ISO/IEC 27000

Norma	Contenido
27000	Visión general de la serie.
27001	Norma principal de la serie. Requisitos del SGSI. Certificable.
27002	Guía de buenas prácticas: (11) dominios, (39) objetivos de control y (133) controles.
27003	Aspectos críticos para el diseño e implementación de un SGSI.
27004	Guía para el desarrollo y utilización de métricas y técnicas de medida de la eficacia de un SGSI y de los controles o grupos de controles.
27005	Directrices para la gestión del riesgo.
27006	Requisitos para la acreditación de entidades de auditoría y certificación.
27007	Guía de auditoría de un SGSI.
27008	Guía de auditoría de los controles seleccionados.
27013	Guía de implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.
27014	Guía de gobierno corporativo de la seguridad de la información.
27031	Guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
27032	Guía relativa a la ciberseguridad.
27033	Guía de seguridad en redes (7 partes).
27034	Guía de seguridad en aplicaciones informáticas.
27035	Guía de gestión de incidentes de seguridad de la información.
27036	Guía de seguridad de externalización de servicios.
27037	Guía de identificación, recopilación y preservación de evidencias digitales

3.2 Proceso de Ingeniería de Seguridad

SGSI

Marco de referencia. Espiral de Deming (I)

- Proceso
  - Conjunto de actividades que utiliza recursos y se gestiona de modo que permite la transformación de unos elementos de "entrada" en unos elementos de "salida".
- Enfoque por procesos
  - La aplicación de un conjunto de procesos en una organización, junto con la identificación de estos, sus interacciones y su gestión.

Marco de referencia. Espiral de Deming (II)

- Modelo PDCA (***P**lan-**D**o-**C**heck-**A**ct*)
  - una estrategia de mejora continua de la calidad en cuatro pasos.
  - Proceso cíclico
- *PLAN* (Planificar)
  - Establecer los objetivos y procesos necesarios para obtener los resultados de acuerdo con el resultado esperado.
- *DO* (Hacer)
  - Implementar los nuevos procesos. Si es posible, en una pequeña escala.

Marco de referencia. Espiral de Deming (III)

- *CHECK* (Verificar)
  - Pasado un periodo de tiempo previsto, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora esperada.
  - Documentar las conclusiones.
- *ACT* (Actuar)
  - Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario.
  - Aplicar nuevas mejoras, si se han detectado errores en el paso anterior.
  - Documentar el proceso.

Marco de referencia. Espiral de Deming (III)

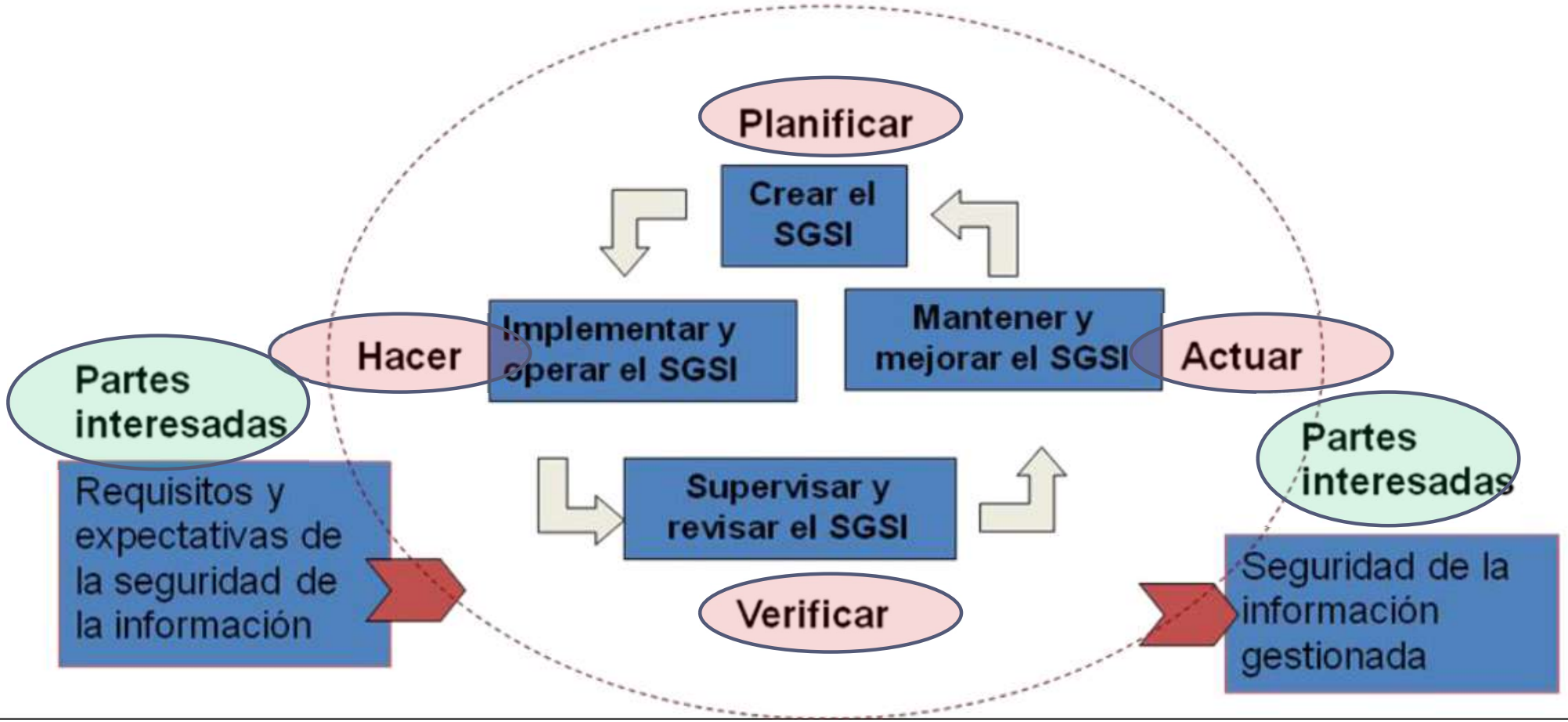
Espiral de Deming en un SGSI (I)

- *PLAN* (Planificar). Crear el SGSI
  - Definir la política, objetivos, procesos y procedimientos del SGSI
    - gestionar el riesgo y mejorar la seguridad de la información,
    - obtener resultados acordes con las políticas y objetivos generales de la organización.
- *DO* (Hacer). Implementar y operar
  - Implementar y operar la política, controles, procesos y procedimientos del SGSI.

Espiral de Deming en un SGSI (II)

- *CHECK* (Verificar). Supervisar y revisar
  - Evaluar y medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI
  - Informar de los resultados a la Dirección para su revisión.
- *ACT* (Actuar). Mantener y mejorar
  - Adoptar medidas correctivas y preventivas
    - en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la Dirección
    - para lograr la mejora continua del SGSI.

Espiral de Deming en un SGSI (III)



Documentación del SGSI, según la Norma

- Declaraciones de política y objetivos
- Alcance del SGSI
- Procedimientos y mecanismos de control que soporta el SGSI
- Metodología de evaluación de riesgo
- Informe de evaluación de riesgos
- Plan de tratamiento de riesgos
- Procedimientos de procesos de seguridad y medida de controles
- Registros de desarrollo del proceso y de incidentes de seguridad
- Declaración de aplicabilidad

3.3 Diseño de Políticas de Seguridad

Política de Seguridad

- Es un **requisito** de la norma ISO 27001 y debe considerar **en líneas generales los objetivos de la seguridad** de la información de la empresa u organización.

- Es la Fase 3 de la implementación de un ISO27001
  - Define lo que se quiere proteger así como las reglas y conductas para los usuarios del sistema para preservar la seguridad de los mismos.
    - Cada servicio ya sea interno o externo plantea riesgos para su sistema y la red a la que está conectado.
  - Una política de seguridad es un conjunto de pautas que se aplican a actividades y los recursos de una organización incluyendo áreas como:
    - seguridad física, seguridad del personal, seguridad administrativa y seguridad de la red.

Pregunta CLAVE de la Política de Seguridad

- **¿Qué queremos conseguir con la Seguridad de la información?**
  - Documento responsabilidad de la dirección.
  - Misiones:
    - Establecer los objetivos.
    - Obtener una visión sintetizada de la funcionalidad y estado del sistema de gestión de la seguridad de la información.
  - La política de la seguridad de la información debe ser:
    - Fácil de entender.
    - Explicar de forma resumida para qué sirve la aplicación de esta política de seguridad en la empresa, su utilidad y los responsables.

Redactar una Política de Seguridad (I)

- REDACTAR UNA POLÍTICA DE ACUERDO A LAS NECESIDADES DE CADA ORGANIZACIÓN
  - Debemos tener en cuenta el tamaño, la estructura y actividad de cada organización …
    - No es lo mismo redactar una política para una gran organización donde quizás se requiera un apartado o párrafo específico para cada división y actividad de la misma que para una pequeña empresa.
    - Tampoco será lo mismo si la actividad de la empresa es la fabricación de componentes que para una empresa que se dedique a proveer servicios de TI.

Redactar una Política de Seguridad (II)

- LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN DEBE TENER EN CUENTA LOS OBJETIVOS DE CADA ORGANIZACIÓN
  - **¿cómo la seguridad de la información respalda al negocio en el logro de sus objetivos?**

- Dos perspectivas para los objetivos de una organización:
  - Los objetivos comerciales
  - Los objetivos de Seguridad de la información

- Objetivos **medibles**:
  - Considerar métricas que permitan la comparación entre la capacidad de seguridad actual y la capacidad requerida para cumplir con los requisitos del negocio.

Redactar una Política de Seguridad (III)

- DEBE DEMOSTRAR QUE SE TIENEN EN CUENTA LOS REQUISITOS DE LAS PARTES INTERESADAS
  - Mencionar el compromiso de la organización en la satisfacción de estos intereses y de cómo la política de Seguridad e la información contribuye a ello.
- SE DEBE COMUNICAR A LAS PARTES INTERESADAS
  - Dar visibilidad a la preocupación de la compañía.
  - Nombrar responsable, establecer procedimientos de comunicación.
- IDENTIFICAR AL PROPIETARIO DE LA POLÍTICA
  - Quién o quiénes son los responsables de la política
  - Y de la gestión de cambios
- OTROS …
  - Alcance del SGSI (partes y procesos afectados)
  - Responsabilidades del SGSI (qué partes / personas son responsables de qué)
  - Estructura de la empresa (organizacional)
  - Enfoque y metodología de análisis de riesgos

Políticas y Objetivos de Seguridad

- La política de la Seguridad de la Información proporciona una base para la planificación de seguridad incluso cuando se amplían los sistemas o se crean nuevas aplicaciones:
  - Describiendo las responsabilidades del usuario, como proteger la información confidencial y crear contraseñas no triviales.
  - Explicando cómo controlará la efectividad de sus medidas de seguridad.
  - El control y la monitorización nos ayuda a determinar si alguien intenta eludir las salvaguardas para proteger la información.
- Para desarrollar su política de seguridad, debe definir claramente sus objetivos de seguridad.

Objetivos de Seguridad

- **El objetivo general es implementar una serie de iniciativas que en conjunto logren todos los objetivos de seguridad del SGSI**

- Los objetivos de seguridad se suelen clasificar en las siguientes categorías:

OBJ 1: PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

- Un esquema de protección de activos o recursos de información debe garantizar que solo los usuarios autorizados puedan acceder a objetos de información en el sistema.

  - La capacidad de asegurar todos los tipos de recursos del sistema es una fortaleza del sistema.
  - Debe definir cuidadosamente las diferentes categorías de usuarios que pueden acceder a su sistema.
  - Como un concepto dentro de la política de seguridad deberíamos definir qué tipos de autorizaciones de acceso se otorgaran a los distintos grupos de usuarios.

OBJ 2: AUTENTICACIÓN

- Deberemos **verificar que un acceso de cualquier tipo en el otro extremo de la sesión realmente es lo que dice ser**.
  - La autenticación sólida protege a un sistema contra el riesgo de suplantación de identidad:
    - Un usuario ya sea humano o una interfaz entre aplicaciones, usa una identidad falsa para acceder a un sistema.
  - Tradicionalmente, los sistemas han utilizado contraseñas y nombres de usuarios para la autenticación.
    - Podemos utilizar también certificados digitales como una mejora en la seguridad.
  - Cuando accedemos desde el sistema a una red pública como Internet, la autenticación del usuario adquiere nuevas dimensiones.
    - Una diferencia importante entre Internet y su intranet ya que la capacidad para confiar en la identidad de un usuario que inicia sesión se reduce drásticamente.
    - Deberemos pensar en utilizar métodos de autenticación más sólidos que los que proporcionan los procedimientos tradicionales de inicio de sesión de nombre de usuario y contraseña.

OBJ 3: AUTORIZACIÓN

- Los usuarios autenticados pueden tener diferentes tipos de permisos según sus niveles de autorización.
  - El nivel de autorización se define en la política de seguridad
    - Discriminar los usuarios que tienen autorización para el acceso a determinados recursos
    - Proceso de segmentación de las aplicaciones y el acceso a los diferentes recursos
  - Mediante los procesos de autenticación se determina
    - Si el usuario una vez identificado tiene los permisos o la autorización necesaria para acceder a los recursos.
  - Por lo general, la autorización se realiza en el contexto de la autenticación.
  - Necesidad de revocar las autorizaciones periódicamente
    - Política de renovaciones para garantizar que las personas que acceden a determinadas informaciones sensibles son siempre las que se han determinado

OBJ 4: INTEGRIDAD DE LA INFORMACIÓN

- La información se mantiene íntegra dentro las operaciones que se realizan y, sobre todo, en los procesos de comunicación:

- Integridad de los datos
  - Proteger la información contra modificaciones o manipulaciones no autorizadas.
  - Reconocer naturaleza de las fuentes de los datos

- Integridad del sistema
  - El sistema nos proporcione siempre resultados consistentes.

- Irrenunciabilidad de transacciones (No repudio)

- Confidencialidad

OBJ 5: AUDITORÍA DE ACTIVIDADES DE SEGURIDAD.

- Constante vigilancia y registro de los posibles incidentes y de actividades sospechosas.
  - Prevenir los eventos no deseados
  - Supervisar los eventos relevantes para la seguridad
    - Disponer de un registro de accesos exitosos y no exitosos o denegados.
    - Evaluar quién está haciendo qué en nuestros sistemas.
      - Si alguien está intentando violar su seguridad o que se están teniendo dificultades para acceder a nuestro sistema.

En resumen: Alcance y política

- Conocer / Establecer:
  - Los objetivos de seguridad de la organización.
  - ¿En quién recae la responsabilidad de la seguridad?
  - El compromiso de la organización respecto a la seguridad.
- Responder a tres preguntas fundamentales:
  - ¿Quién tiene permitido el acceso?
  - ¿A qué recursos del sistema y organizativos se le permite acceder?
  - ¿Qué tipo de acceso a cada recurso está permitido a cada usuario?

3.4 Metodología de Trabajo

Planificación

PLAN (Planificar). Crear el SGSI

- Precisar el alcance del sistema de gestión.
- Detallar la política de seguridad
- Reconocer las vulnerabilidades y amenazas hacia los activos.
- Análisis y evaluación de riesgos
- Evaluar impactos.
- Definición del plan de tratamiento de riesgos
- Enumerar los activos necesarios
- Elegir los controles para cumplir la política de seguridad que se van a llevar a cabo

Análisis y evaluación de riesgos

- Estudio de la situación de la organización desde el punto de vista de la seguridad.
  - Análisis de Riesgos
    - Para valorar los activos de información y sus vulnerabilidades
  - Gestión de riesgos
    - para reducirlos en la medida de lo posible.
  - Controles que nos permitan minimizar los riesgos.

Análisis de Riesgos

- El objeto a proteger (activo).
  - aquello que tiene la organización, cuya pérdida o deterioro causaría un perjuicio
- Dimensiones de la seguridad
  - Autenticidad:
    - ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
  - Confidencialidad:
    - ¿Qué daño causaría que conociera un activo quien no debe?
  - Integridad:
    - ¿Qué perjuicio causaría que un dato estuviera dañado o corrupto?
  - Disponibilidad:
    - ¿Qué perjuicio causaría no tener o no poder utilizar un activo?

Análisis de Riesgos

- Una avería eléctrica de 24 horas de duración supondría un perjuicio (disponibilidad)
  - valor correspondiente a la reparación de la avería,
  - la de los equipos que hayan podido quedar dañados más
  - las derivadas de no haber podido facilitar durante ese tiempo los servicios comprometidos.
- Dependencia entre activos,
  - un activo P puede depender de otro H
    - si H sufriera un percance, P se vería indirectamente perjudicado.

Activos (assets)

- los servicios
  - procesos de negocio de la organización: gestión de nóminas,…
- los datos e información
  - núcleo del sistema
- las aplicaciones de software
- los equipos informáticos
- el personal
  - personal interno, subcontratado, de los clientes, etcétera.
- las redes de comunicaciones
  - redes propias o subcontratadas a terceros

Activos (assets)

- los soportes de información.
  - almacenamiento de la información durante un largo período de tiempo.
- los equipos auxiliares
  - de destrucción de documentación o los equipos de climatización.
- las instalaciones
  - oficinas, edificios o vehículos.
- la imagen y la reputación de la empresa.

Inventario de activos

- Cada activo debe incluir, al menos, su descripción, localización y propietario.
- Dependencias entre activos.
- Valoración de los activos
  - relevancia que tiene para el negocio
  - impacto que una incidencia produce
    - se establece según una escala (del 0 al 10 o con valores bajo, medio y alto)

Inventario de activos

Clase de activo	Descripción
[D] Datos / Información	Información generada o manejada por el centro almacenado en diferentes soportes de información.
[S] Servicios	Servicios o funciones prestados por la organización para cubrir una necesidad de los usuarios.
[SW] Software	Aplicaciones informáticas tanto de desarrollo propio como aplicaciones externas que permiten que ciertas tareas se desempeñen a través del equipo informático.
[HW] Hardware	Equipo informático que actúan como soportes de datos o que albergan los servicios informáticos del centro

Valor	Descripción
Muy Alto	Daño crítico para el centro
Alto	Daño grave para el centro
Medio	Daño importante para el centro
Bajo	Daño reparable para el centro

Inventario de activos

[D] Datos	
Código: D.2	**Nombre:** Expedientes académicos
Descripción: Información relacionada con el expediente académico de los estudiantes como pueden ser calificaciones, asistencia a clases o partes disciplinarios.	
Tipo: Ficheros	
Dependencias	
Activos: SW.2	**Grado:** Alto
¿Por qué? Todos los datos relacionados con los expedientes académicos de los alumnos deben introducirse en la plataforma de Itaca para que desde la Consellería d'Educació tengan acceso a estos datos	

Valor

Total	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad
Muy Alto	Muy Alto	Muy Alto	Medio	Muy Alto	Alto

Amenazas

- Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos
  - Degradación:
    - Porcentaje en que quedaría afectado el activo en caso de que la amenaza se materializase
  - Frecuencia:
    - Tasa anual de ocurrencia de la amenaza

Tipos de amenazas

Categoría de amenaza	Descripción
[N] Desastres naturales	Sucesos que puede ocurrir sin intervención de los seres humanos como causa directa o indirecta.
[I] De origen industrial	Sucesos que pueden ocurrir de forma accidental derivados de la actividad humana de tipo industrial y que pueden darse de forma accidental o deliberada.
[E] Errores y fallos no intencionados	Fallos no intencionales causados de forma directa por la actividad de personas que tienen acceso al sistema de información. Normalmente se producen por error u omisión.
[A] Ataques intencionados	Fallos deliberados causados por la actividad humana con el objetivo o bien de beneficiarse indebidamente o de causar daños a la organización.

Tipos de amenazas

I.10 Degradación de soportes de información

Descripción: Errores o averías en los dispositivos de soporte de información debido al paso del tiempo y al uso continuado.

Probabilidad: Alta

Si bien no es algo muy frecuente es inevitable que cada mes o cada varios meses los soportes de almacenamientos electrónicos den algún fallo

Activos afectados

Nombre	Degradación				
	C	I	D	A	T
Media.1 - Discos duros de Administración	-	-	A	-	-
Media.2 - Almacenamiento USB	-	-	M	-	-

Tipos de amenazas

A.7 Uso no previsto					
Descripción: Utilización de recursos del sistema para fines no previstos, típicamente de interés personal, juegos, consultas personales en internet, programas personales etc.					
Probabilidad: Muy Alta El hecho de que haya dispositivos personales de profesores y que los alumnos tengan acceso a equipos informáticos hace difícil controlar el uso que se le da a estos y por tanto este tipo de situaciones son muy comunes.					
Activos afectados					
Nombre	**Degradación**				
	C	**I**	**D**	**A**	**T**
S.2 - Servicio de correo electrónico	B	B	B	-	-
HW.2 - Ordenadores para alumnado	B	B	B	-	-
HW.3 - Ordenadores para profesorado	B	B	B	-	-
COM.1 - Red telefónica	B	B	B	-	-
COM.2 - Red WiFi	B	B	B	-	-
Media.3 - Memoria USB	M	M	M	-	-

Riesgos

- El riesgo tiene en cuenta tanto el impacto como la probabilidad de que materialice la amenaza sobre el activo y en la dimensión de seguridad afectados.

HW.2 – Ordenadores para alumnado													
Amenazas	Impacto Potencial			Impacto Acumulado			Riesgo Potencial			Riesgo Acumulado		
	C	I	D	C	I	D	C	I	D	C	I	D
N.1 – Fuego	-	-	B	-	-	-	-	-	MB	-	-	-
N.2 - Agua	-	-	B	-	-	-	-	-	MB	-	-	-
I.3 – Contaminación mecánica	-	-	MB	-	-	-	-	-	B	-	-	-
I.6 – Corte suministro eléctrico	-	-	M	-	-	-	-	-	M	-	-	-
A.7 – Uso no previsto	-	-	MB	-	-	-	-	-	MB	-	-	-
A.15 – Modificación/Destrucción de info.	-	-	MB	-	-	-	-	-	MB	-	-	-

Gestión de Riesgos

- La Dirección deberá decidir para cada riesgo
  - Rechazarlo.
    - No viajar en avión para evitar el riesgo asociado
  - Asumirlo.
  - Transferirlo.
    - Contratación de una póliza de seguros.
  - Gestionarlo (gestión de riesgos).

Gestión de Riesgos

- Actuar sobre las vulnerabilidades
  - implantar mecanismos de salvaguarda o controles
  - para reducir el riesgo a un valor
    - asumirlo
    - continuar mejorando las salvaguardas

- Las salvaguardas actúan sobre las amenazas reduciendo la degradación y/o la probabilidad.

Salvaguardas

D.1 – Datos de Matrícula												
Amenazas	Salvaguardas	Probabilidad	Dimensiones			Impacto Res.			Riesgo Res.		
			C	I	D	C	I	D	C	I	D
E.1 - Errores de los usuarios	CR.1 – Cuentas de administración	Muy Alta	B	B	B	M	M	MB	A	A	MB
	AD.1 – Formalización de procedimientos	Media	B	A	B	M	MA	MB	M	A	MB
	RC.1 – Copias de seguridad periódicas	Muy Alta	B	B	MB	M	M	MB	A	A	MB
E.19 – Fugas de información	AW.1 – Elaborar normas del uso de TI	Baja	A	-	-	MA	-	-	M	-	-
	AW.2 – Formación sobre aplicación RGPD	Baja	A	-	-	MA	-	-	M	-	-
	IM.1 – Cifrado de equipos hardware	Media	B	-	-	M	-	-	M	-	-
	PR.7 – Formateo periódico de equipos	Media	B	-	-	M	-	-	M	-	-
A.5 – Suplantación de identidad	PR.1 – Uso de claves y certificados para conexiones inalámbricas	Muy Baja	A	B	-	MA	M	-	M	MB	-
	PR.3 – Control de acceso lógico	Muy Baja	A	B	-	MA	M	-	M	MB	-
	PR.4 – Implantación contraseñas seguras	Muy Baja	A	B	-	MA	M	-	M	MB	-
	IM.1 – Cifrado de equipos hardware	Muy Baja	B	B	-	M	M	-	MB	MB	-

Activo, amenaza, vulnerabilidad, impacto, probabilidad

Impacto o consecuencia de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad.

El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo

¿Cómo se mide el nivel de riesgo?

- El impacto indica las consecuencias de la materialización de una amenaza.
- El nivel de riesgo es una estimación de lo que puede ocurrir.
  - Se valora como el producto del impacto de una amenaza por la probabilidad de la misma.

Estimación del riesgo

Gravedad del efecto causado por la amenaza y probabilidad de que ocurra:

-riesgo crítico: generan un alto impacto con una probabilidad alta

- riesgo asumible: amenazas poco probables que no generen un gran impacto.

Riesgo		Probabilidad				
		Muy raro	Poco probable	Posible	Probable	Prácticamente Seguro
Impacto	Muy Alto	Importante	Crítico	Crítico	Crítico	Crítico
	Alto	Apreciable	Importante	Importante	Crítico	Crítico
	Medio	Bajo	Apreciable	Apreciable	Importante	Importante
	Bajo	Asumible	Bajo	Bajo	Apreciable	Apreciable
	Muy Bajo	Asumible	Asumible	Asumible	Bajo	Bajo

Estimación del riesgo

- Riesgo intrínseco
  - posibilidad de que se produzca un impacto determinado en un activo o en un grupo de activos.
- Salvaguardas
  - prácticas, procedimientos o mecanismos que reducen el riesgo.
    - pueden actuar disminuyendo el impacto o la probabilidad.
- Riesgo residual
  - el riesgo que queda tras la aplicación de salvaguardas.
  - Por muy bien que protejamos nuestros activos, es imposible eliminar el riesgo al 100% por lo que siempre quedará un riesgo residual en el sistema que la organización deberá asumir y vigilar.

Fases de la implantación de un SGSI

Implementar, Supervisar, Mantener

DO (Hacer). Implementar y operar

- Implantar el plan de tratamiento de riesgos
- Implantar los controles necesarios para cumplir con la política de seguridad
- Asignar responsables a cada tarea

CHECK (Verificar). Supervisar y revisar

- Revisión del SGSI
- Medición de la eficacia de los controles de la política de seguridad
- Elaboración de auditorías internas
- Control del funcionamiento de los activos utilizados para la seguridad del sistema.

ACT (Actuar). Mantener y mejorar

- Adoptar medidas correctoras
- Adoptar medidas preventivas
- Adoptar medidas que ayuden a mejorar el sistema

Certificación

- Consultoría
  - Un equipo de expertos en la norma ayuda a la organización a cumplir con los requisitos necesarios para obtener la certificación.
    - También se detallarán las medidas, tanto correctivas como preventivas, que se van a tomar en la organización.
- Auditoría
  - Un organismo experto en gestión de seguridad revisa los procedimientos requeridos por la norma y la implantación de los controles.
    - En España, este organismo es AENOR (Asociación Española de Normalización y Certificación).

Referencias

- ISO27000.es: http://www.iso27000.es/
- Página localizada en el Software Engineering Institute relacionada con temas de seguridad.

  http://www.cert.org/
- EEUU NIST, National Institute of Standards and Technology (2012), «Special Publication 800-30 Rev.1», Guide for conducting risk assessment, Computer Security Division Information Technology Laboratory, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- MAGERIT versión 3 (idioma español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Xd2hI9V7nDd
- Betancourt, D. F. (02 de agosto de 2018). *Ciclo de Deming (PDCA): Qué es y cómo logra la mejora continua*. Recuperado el 30 de noviembre de 2020, de Ingenio Empresa: www.ingenioempresa.com/ciclo-pdca.