**1.1.- Seguridad informática: mecanismos básicos de seguridad.**

## 1.1.1.- Ciberseguridad, seguridad informática y seguridad de la información.

1. **Seguridad de la información:** conjunto de medidas **preventivas y reactivas** que permiten almacenar y proteger la información.
2. **Seguridad informática:** protege la **integridad y privacidad** de la información, evitando que agentes maliciosos accedan al sistema y detectando riesgos como virus, códigos dañados y fallos eléctricos.
3. **Ciberseguridad:** defiende con **prácticas ofensivas** todos los equipos informáticos

## 1.1.2.- Sistemas de información.

Un SI es un conjunto de recursos cuyo objetivo es **administrar datos e información** en general, de forma que puedan ser procesados y/o recuperados de forma sencilla y rápida.

***Tipos de recursos:***

* **Humanos.**
* **Datos:** el SI procesa los datos transformándolos en información.
* **Procesos:** acciones necesarias para lograr el objetivo del SI.
* **Tecnológicos:** físicos y lógicos.

***El funcionamiento básico de un SÍ sería:***

* **Entrada de datos:** a través de código de barras, código QR, teclado, voz, escáner, etc.
* **Procesamiento de la información registrada:** se transforman los datos de entrada en información para la toma de decisiones
* **Almacenamiento de la información:** se registra de forma persistente en el sistema.
* **Salida de la información:** se extrae en algún tipo de soporte o es enviada por la red.

## 1.1.3.- Sistema de gestión de seguridad de la información.

Un sistema de gestión de seguridad de la información consiste en políticas, procedimientos, guías, recursos y actividades asociadas, colectivamente gestionadas por la organización, con la **intención de proteger sus activos de información**.

Un **SGSI se basa en las ISO 27001 y 27002**, así como en el **ciclo de Deming**, para garantizar la actualización del sistema y la mejora continua. Este tiene cuatro niveles:

1. **Planificar (Plan):** establecer el contexto.
2. **Hacer (Do):** implementar el SGSI.
3. **Verificar (Check):** monitorizar y revisar.
4. **Actuar (Act):** ejecutar tareas de mantenimiento y propuestas de mejora.

**1.2.- Vulnerabilidades de un sistema informático.**

En un SI, **lo que queremos** **proteger son sus activos**, es decir, los recursos que forman parte del sistema:

* **Hardware**.
* **Software**.
* **Datos e información**: los datos son procesados por el software haciendo uso del hardware para obtener la información buscada.
* **Otros**: fungibles, personas, elementos externos al sistema informático.

**Vulnerabilidad** → cualquier debilidad que comprometa la seguridad del SI.

1. **Diseño**: debilidad de los protocolos en redes, política de seguridad inexistente o deficiente.
2. **Implementación:** errores de programación, existencia de puertas traseras, descuido de los fabricantes.
3. **Uso**: configuración inadecuada del SI, falta de formación de los usuarios y responsables informáticos, limitación legal en tecnologías de seguridad.

Cuando se acaba de detectar una **vulnerabilidad que aún no tiene solución se le llama vulnerabilidad del día cero.**

**Amenaza** → es un evento que compromete la seguridad de un Sistema de Información. Si dicho evento ocurre, causará daños generando un impacto en el SI.

Las vulnerabilidades y las amenazas están relacionadas, ya que una amenaza solo puede causar impacto si aprovecha una vulnerabilidad.

**Contramedidas** → son acciones preventivas ante amenazas conocidas o futuras.

**Riesgo** → el impacto potencial que puede sufrir el SI, considerando las amenazas, vulnerabilidades y las contramedidas implementadas.

## 1.2.1.- Análisis de vulnerabilidades.

Para llevar a cabo un análisis de vulnerabilidades en la organización se plantean algunas cuestiones básicas:

* **Conocer cuando se realizó el último análisis.**
* **Conocer la frecuencia de los análisis.**
* **Estar al día de las nuevas vulnerabilidades y conocer si puede afectarnos.**
* **Disponer de un historial de vulnerabilidades** de nuestra organización, cuándo se detectaron y como se corrigieron.

Las vulnerabilidades pueden atenuarse mediante:

* **La automatización de los procedimientos de detección.**
* **La formación del personal responsable de su detección.**

Para controlar y evaluar las vulnerabilidades, los responsables de seguridad cuentan con un conjunto de herramientas, procedimientos y tecnologías que les ayudan:

* Parches del sistema operativo y actualizaciones de las aplicaciones.
* Seguridad en los ficheros y control de acceso de los usuarios a los recursos.
* Cuentas de usuarios y políticas de gestión de contraseñas.
* Control de los servicios y aplicaciones instaladas.
* Registro y auditoría de eventos.
* Configuración de herramientas de seguridad: antivirus, cortafuegos, copias de seguridad, etc.
* Test de penetración frente a ataques internos y externos.

## 1.2.1.- Análisis de vulnerabilidades.

Frente a un riesgo de cualquier naturaleza, caben cinco posibilidades:

1. **Evitar el riesgo:** se evita cuando la organización rechaza aceptarlo, lo que exige el compromiso de no realizar nunca la acción que origina el riesgo.
2. **Reducir el riesgo:** cuando no puede evitarse, podemos reducirlo a unos mínimos asumibles.
3. **Asumir el riesgo:** se acepta el riesgo al no ser posible ni evitarlo ni reducirlo, asumiendo sus consecuencias en caso de que ocurra.
4. **Compartir el riesgo:** se trata de buscar un respaldo en caso de que se produzca la amenaza, compartiendo el impacto con otras entidades.
5. **Transferir el riesgo:** se deriva su control a una entidad externa, asumiendo esta entidad toda la responsabilidad de sus consecuencias.

**1.3.-Amenazas.**

*Tipos de amenazas:*

* **Vulnerabilidad:** Debilidad que puede dar lugar a una amenaza
* **Amenaza:** Posible daño al sistema
* **Ataque:** La amenaza se plasma en alguna acción concreta
* **Impacto:** Daño producido

*Tipos de confidencialidad:*

* **Confidencialidad:** Nadie puede acceder a la información
* **Integridad:** Los datos no se modifican
* **Disponibilidad:** El acceso es correcto

## 1.3.1.- Clasificación de las amenazas.

*Agrupación por amenazas:*

* **Físicas y ambientales:** Afectan tanto al hardware como a las personas

* **Lógicas:** Afectan a la parte lógica

*Una vez entendidas las amenazas:*

* **Naturales:** Incendio, inundación…
* **Agentes externos:** Virus informáticos, disturbios ….
* **Agentes internos:** Empleados descuidados, mala utilización de las aplicaciones

*Teniendo en cuenta la intencionalidad:*

* **Accidentes:** Averías del sistema informático
* **Errores:** Errores en la ejecución de procedimientos establecidos
* **Malintencionadas**: Robos, sabotajes…

*Siguiendo el factor de seguridad, la agrupación de las amenazas es la siguiente:*

1. **Interceptación**
   1. Acceso a la información por personas no autorizadas
   2. Privilegios no adquiridos
   3. Detección difícil mientras se produce, no deja huellas

**Se garantiza la integridad y disponibilidad pero no la confidencialidad**

1. **Modificación**
   1. El intruso accede con los privilegios para realizar cambios
   2. Detección difícil según circunstancias

**Se garantiza la disponibilidad pero no la integridad y confidencialidad**

1. **Interrupción**
   1. El intruso provoca que el objeto se pierda, quede inutilizable o no disponible
   2. Detección inmediata ya que es muy difícil de cubrir

**No se garantiza ni la integridad, confidencialidad y disponibilidad**

1. **Fabricación**
   1. El intruso inserta objetos falsificados en el sistema
   2. Detección difícil

**Se garantiza la disponibilidad y la confidencialidad pero no la integridad.**

**1.4.- Seguridad física y ambiental. Seguridad pasiva.**

## 1.4.1.- Seguridad física y ambiental.

Conjunto de **controles y medidas de seguridad** **para evitar accesos no autorizados**.

Las normas de seguridad deben **restringir el acceso solo al personal autorizado y mantener condiciones ambientales adecuadas**. Las **amenazas físicas** incluyen incendios, inundaciones, robos, cortes de luz, entre otras, y deben prevenirse con medidas como aire acondicionado para controlar la temperatura.

Los **centros de procesos de datos (CPD)** son críticos, y un **centro de respaldo** debe asumir el control en caso de problemas, manteniéndose siempre actualizado. El **control de acceso** debe identificar usuarios y gestionar entradas, sirviendo además como medida disuasoria.

Algunas técnicas de control de acceso son las siguientes:

* Utilizar personal de seguridad y/o animales.
* Detectores de metales.
* Sistemas biométricos: termografía, huella digital, voz, iris, etc.
* Protección electrónica: barreras infrarrojas, detectores ultrasónicos, recintos electrificados, etc.

## 1.4.1.1.- Ubicación y protección física.

La ubicación física de los servidores es muy importante para la **protección física del sistema informático**, debiéndose descartar sobre todo:

* Zonas cercanas a paredes exteriores y plantas bajas, pues son más sensibles al vandalismo o sabotaje.
* Los sótanos, ya que pueden dar problemas de inundaciones.
* Últimas plantas, para evitar desastres aéreos.

**La mejor ubicación de los CPD son las plantas intermedias** de un edificio o lugares centrales en parques empresariales.

## 1.4.2.- Seguridad pasiva.

Se define como el conjunto de medidas que la organización **aplica después de producirse el incidente de seguridad**, **intentando minimizar el impacto** que pueda tener sobre el sistema informático.

El objetivo de las medidas de seguridad pasiva es **recuperar el sistema al estado anterior al incidente.**

Algunas medidas pueden ser: RAID, sistemas de archivos tolerantes a fallos, SAI/UPS, copia de seguridad, extintores/muros/paredes cortafuegos.

## 1.4.2.1.- SAI.

* Proporcionar corriente eléctrica a partir de un acumulador o de otra forma de energía.
* Mejorar la calidad de la corriente eléctrica filtrando las subidas y bajadas de tensión.

Las partes más importantes de un SAI son: **rectificador, baterías y convertidor**.

1. **OFF-LINE o STAND BY**: SAI común para equipos domésticos y pequeñas empresas. Se activa durante cortes de suministro, pero tiene un tiempo de reacción considerable y no estabiliza la corriente.
2. **ON-LINE**: SAI avanzado para entornos industriales. Conectado permanentemente, ofrece corriente continua y batería instantánea en cortes, aunque estabiliza poco la corriente.
3. **SAI INTERACTIVO (IN-LINE)**: Similar al OFF-LINE, pero estabiliza mejor la corriente. Se activa en casos de tensión anómala o cortes totales.

## 1.4.2.2.- Copias de seguridad.

Son duplicados de archivos o aplicaciones para **recuperar datos en caso de pérdidas**. Aseguran la integridad y disponibilidad de la información y deben planificarse adecuadamente.

1. **Completa** (nivel 0 o normal)
2. **Diferencial** (diferencial acumulativa)
3. **Incremental** (progresiva)

## 1.4.2.3.- Recuperación de la información.

La recuperación de datos incluye técnicas para **extraer información de dispositivos dañados**, incluso a costa de destruirlos. Se divide en:

* **Lógica**: Para dispositivos funcionales que han perdido su estructura lógica. Herramientas: DISM, CHKDSK, SFC; fsck, DDRescue-GUI, TestDisk, PhotoRec.
* **Física**: Para daños en componentes físicos, con recuperación según la tecnología de almacenamiento (magnética, óptica, electrónica).

## 1.4.3.- Destrucción de la información.

Desde el punto de vista de la seguridad, es crucial destruir la información de dispositivos en desuso para evitar la recuperación de datos. Los métodos incluyen:

1. **Destrucción física**: Dañar el dispositivo para que no se pueda acceder a los datos.
2. **Sobreescritura de datos**: Técnicas como el **método Gutmann**, que impiden descifrar el contenido anterior.

## 

## 1.4.4.- Medios de almacenamiento.

Para aumentar la seguridad del almacenamiento, se sugiere usar sistemas de archivos con listas de control de acceso (ACL) que asignan propietarios y definen el acceso. La encriptación también mejora la seguridad, aunque puede ralentizar el proceso de almacenamiento y recuperación.