Unidad Temática 1: Introducción a la Seguridad Informática

CIDAN: Qué es cada uno, ejemplos...

El sistema de seguridad informática se orienta a obtener altos niveles de **fiabilidad**. Un sistema es considerado seguro o fiable si garantiza cinco aspectos clave, agrupados bajo el acrónimo CIDAN: **Confidencialidad, Integridad, Disponibilidad, Autenticación y No Repudio**.

Principio	Definición	Ejemplo
Confidencialidad	Garantiza que la información solo es accesible y comprensible para personas o sistemas autorizados, previniendo la divulgación no autorizada.	El uso de la **criptografía** para cifrar datos, como el EFS (Encrypt File System) en particiones NTFS de Windows, o el acceso a cuentas mediante HTTPS.
Integridad	Asegura que los datos permanecen invariables desde su origen y no han sido modificados, alterados o destruidos accidental o intencionadamente.	Mecanismos que detectan alteraciones, como el uso de la **firma digital** y funciones **hash** (MD5 o SHA-256) para comprobar que la información no ha sido alterada.
Disponibilidad	Garantiza que el sistema, la información y los servicios estén accesibles y operativos el máximo tiempo posible para los usuarios autorizados.	Sistemas de **Alta Disponibilidad (High Availability)**, cuyo objetivo es funcionar 24/7/365, aspirando a una disponibilidad de "cinco nueves" (99,999%). También el uso de **Sistemas de Alimentación Ininterrumpida (SAI)**.
Autenticación	Verificación de la identidad de un usuario o del autor de una información para evitar la suplantación. Se comprueba que es quien dice ser.	El uso de credenciales (usuario y contraseña), o la comprobación de un **certificado digital** de una página web.
No Repudio (Irrenunciabilidad)	Permite probar ante un tercero la participación de las partes en una comunicación. Puede ser en origen (el emisor no puede negar el envío) o en destino (el receptor no puede negar la recepción).	Una declaración de la renta firmada con un certificado digital, lo que evita que el ciudadano firmante pueda negar el envío (No Repudio en origen).

Análisis de riesgos: Activos y tipos de activos, Amenazas y tipos, Vulnerabilidad, Ataque, Impacto y Riesgo

El análisis de riesgos es una aproximación metódica para determinar el riesgo de un sistema.

Activos y tipos de activos

Los **activos** son los recursos que forman parte del sistema, que pertenecen a la empresa y que deben ser protegidos, ya que facilitan su funcionamiento y consecución de objetivos.

Tipo de Activo	Ejemplos
Datos o Información	Constituyen el núcleo de la organización (económicos, fiscales, de clientes, etc.).
Software (Lógicos)	Aplicaciones informáticas (software) y sistemas operativos.
Equipos Informáticos (Hardware)	Servidores, terminales, periféricos, soportes de información.
Redes de Comunicaciones	Redes locales, metropolitanas, Internet; vías de comunicación y transmisión de datos.
Instalaciones	Lugares que albergan los sistemas de información (oficinas, locales, Data Centers).
Personal	Administradores, programadores, usuarios internos y externos, directivos.
Servicios	Productos, sitios web, correo electrónico y otros servicios ofrecidos a clientes o usuarios.
Intangibles	Imagen y reputación de la empresa.

La **Valoración** de un activo puede ser **cualitativa** (escala relativa, ej. X/10 o Bajo/Medio/Alto) o **cuantitativa** (valoración numérica en dinero). El valor del activo no se refiere a lo que cuesta, sino a lo que vale la pena proteger.

Amenazas y tipos

Una **amenaza** es la causa potencial de un incidente que puede causar daños a un sistema de información.

Clasificación (MAGERIT)	Descripción y Ejemplos
Origen natural	Accidentes naturales como terremotos o inundaciones.
Del entorno (industrial)	Desastres industriales, contaminación o fallos eléctricos.

Defectos de las aplicaciones	Problemas inherentes al equipamiento o software por fallos en su diseño o implementación (vulnerabilidades técnicas).
Causadas por personas accidentalmente	Errores o negligencia por parte de los usuarios con acceso al sistema.
Causadas por personas deliberadamente	Ataques intencionados con ánimo de beneficio o de causar daño (hackers, crackers, ciberdelincuentes).

Otros tipos de amenazas son las **físicas** (robo, sabotaje, condiciones atmosféricas adversas) y **lógicas** (software malicioso o *malware*, errores de programación o *bugs*).

Vulnerabilidad

Una **vulnerabilidad** es una debilidad o fallo de seguridad de un activo que puede ser aprovechada por una amenaza para comprometer la seguridad del sistema, también conocida como agujero de seguridad. Un sistema es vulnerable cuando un fallo o amenaza compromete su seguridad.

Ataque

Un **ataque** es la **materialización de una amenaza** que se aprovecha de una o más vulnerabilidades y provoca un daño o impacto sobre el sistema. Los signos de ataque incluyen la denegación de servicio (DoS), intentos de escritura en ficheros del sistema, o logins a horas no habituales.

Impacto

El **impacto** es la consecuencia o efecto del ataque, es decir, el **daño real causado** sobre el activo.

- El impacto se estima multiplicando el valor del activo por el grado de degradación causado por la amenaza.
- La escala de impacto se clasifica habitualmente en: **Crítico** (40-50), **Grave** (25-40), **Moderado** (10-25) y **Menor** (1-10).
- Ejemplos de impactos incluyen la pérdida de reputación, pérdidas económicas por interrupción del servicio o incumplimiento de la legislación.

Riesgo

El **riesgo** es la medida del **daño probable** sobre un sistema. Es la posibilidad de que una amenaza se materialice aprovechando una vulnerabilidad y produzca un impacto negativo.

- El riesgo se estima ponderando el impacto con la tasa de ocurrencia (probabilidad) de la amenaza.
- La inversión en seguridad debe ser proporcional al riesgo.
- La **Gestión del Riesgo** implica decidir cómo tratar los riesgos: **Evitarlo** (ej. prohibir pendrives USB), **Reducirlo** (ej. permitir pendrives pero con antivirus

actualizado), **Asumirlo** (aceptar el riesgo si el impacto es bajo o el coste de mitigación es alto), o **Transferirlo** (ej. contratar un seguro).

Tipos de vulnerabilidades

Las vulnerabilidades, o debilidades en los activos, se clasifican en:

- **Físicas o estructurales:** Debilidades en la ubicación o estructura, como la ausencia de SAI o la falta de control de acceso al espacio de trabajo.
- **Ambientales y naturales:** Relacionadas con condiciones del entorno, como el polvo, la contaminación, la falta de pararrayos o la incapacidad de la infraestructura para resistir adversidades climáticas (terremotos, tormentas).
- **Hardware:** Defectos o configuraciones inadecuadas del equipo, como firmware sin actualizar o un mal sistema de *backup*.
- **Software:** Errores de aplicaciones, Sistemas Operativos, bases de datos o elementos de seguridad (ej. software de gestión sin mantenimiento o mala actualización de antivirus).
- **Medios de almacenamiento:** Uso inadecuado de soportes (caducados, mal estado) o almacenamiento en locales inseguros (humedad, magnetismo).
- **Redes de comunicación:** Transmisión de datos sin cifrar, mala configuración de la red, o dependencia exclusiva de un único proveedor de comunicaciones.
- **Humanas:** Daños causados por personas, ya sea intencionadamente o por desconocimiento, como la no existencia de una política de contraseñas.

Qué es una auditoría. Tipos de auditoría

Una **auditoría** es un análisis pormenorizado de los sistemas informáticos que tiene como objetivo descubrir, identificar y posteriormente corregir vulnerabilidades o debilidades en los activos y procesos que componen el sistema. Proporciona una imagen real y actual del estado de seguridad.

El informe resultante debe incluir la descripción de los activos, la detección y evaluación de vulnerabilidades, el análisis de eficiencia, la verificación del cumplimiento normativo (ej. LOPD) y recomendaciones de mejora.

Existen diferentes **tipos de auditoría** de seguridad:

- **Auditoría de seguridad interna:** Contrasta el nivel de seguridad de las redes locales corporativas.
- **Auditoría de seguridad perimetral:** Se centra en el perímetro de la red local conectada a redes públicas, analizando el grado de seguridad en las entradas exteriores.
- **Test de intrusión:** Intenta acceder a los sistemas para comprobar su resistencia a intrusiones no deseadas.
- **Auditoría de código de aplicaciones:** Analiza el código de las aplicaciones, independientemente del lenguaje (ej. comprobación de inyección de código SQL).
- **Análisis forense:** Es una metodología de estudio posterior a un incidente que busca reconstruir cómo se penetró el sistema y valorar los daños ocasionados.

Qué tiene un plan de seguridad

El **Plan de Seguridad Integral** es un documento que debe ser definido y aprobado por la dirección de la organización y es elaborado a medida, basándose en las normas y estándares de seguridad informática (como COBIT e ISO 17799).

El contenido de un Plan de Seguridad incluye:

- **Descripción de la empresa** y justificación del plan.
- **Objetivo del plan** (expectativas de seguridad informática de la organización).
- **Responsabilidades** (del equipo de diseño, de la autoridad para aplicar sanciones, y del personal TIC).
- **Alcance** (descripción e inventario de activos a proteger).
- **Identificación y análisis de riesgos**.
- **Diseño de las políticas de seguridad y procedimientos** (física, lógica, en redes y en recursos humanos), incluyendo las medidas a tomar en caso de incumplimiento.
- **Planificación de contingencias y recuperación ante desastres**.

Políticas de seguridad. Qué son, Saber poner ejemplos de políticas y qué es una política de seguridad

Una **política de seguridad** es el conjunto de normas y protocolos que se deben seguir, donde se definen las medidas a tomar para la protección de la seguridad del sistema. Muestra el posicionamiento de la organización respecto a la seguridad y es la manera de controlar o gestionar el riesgo.

El objetivo principal de la política es **transmitir a los empleados las obligaciones y buenas prácticas** en relación con la seguridad de la información, definiendo las responsabilidades del personal con acceso al sistema y la manera de hacer un buen uso de los recursos (hardware y software).

Ejemplos de políticas y medidas que se pueden incluir:

- **Política de uso de correo electrónico**.
- **Política sobre el uso de dispositivos o sistemas de almacenamiento externo** y copias de seguridad.
- **Política sobre el uso de dispositivos personales** (BYOD) o portátiles.
- **Medidas de seguridad activa** como la creación y conservación en lugar seguro de copias de seguridad, y el uso de cifrado en la transmisión de información.
- **Políticas de identificación y autenticación** de usuarios.
- Mantener **todo el software actualizado** (antivirus, Sistema Operativo, software de gestión).
- Instalación de un **pararrayos** y revisión periódica de la instalación eléctrica.

Plan de contingencia: qué es, fases

Un **Plan de Contingencia** (o Plan de Contingencia y Continuidad del Negocio) es un documento que describe la estrategia o pasos a seguir para **recuperar o reestablecer el sistema de información** ante cualquier contingencia o desastre (físico o lógico), garantizando la continuidad de la actividad de la compañía. Son medidas de recuperación o paliativas, aplicadas *después* de que se ha producido el desastre.

Fases del Plan de Contingencia (según INCIBE):

1. **FASE 0: Determinación del alcance:** Identificar los elementos críticos de la organización a proteger mediante un análisis de riesgos.
2. **FASE 1: Análisis de la organización:** Analizar la estructura interna, dependencias, personal clave y activos esenciales. Incluye el análisis del impacto (cómo afectaría la interrupción) y el análisis del riesgo.
3. **FASE 2: Estrategia de continuidad:** Desarrollar estrategias para asegurar la continuidad de las operaciones y garantizar la resiliencia.
4. **FASE 3: Respuesta a la contingencia:**
    - **Plan de crisis (emergencia):** Define cómo actuar ante emergencias inmediatas.
    - **Planes operativos de recuperación:** Establecen procedimientos para restaurar sistemas.
    - **Procedimientos técnicos de trabajo:** Describen cómo gestionar incidentes técnicos.
    - Se definen prioridades, responsables y protocolos de actuación.
5. **FASE 4: Prueba, mantenimiento y revisión:** Probar las estrategias para asegurar su efectividad y actualizar los planes periódicamente.
6. **FASE 5: Concienciación:** Esfuerzos de capacitación y sensibilización del personal.

Análisis forense: qué es, usos, fases

El **Análisis Forense** (o Informática Forense) es una metodología de estudio que se le puede considerar un tipo de auditoría. Es una ciencia metódica que pretende averiguar todo lo ocurrido durante una intrusión o delito, reuniendo y analizando pruebas para reconstruir la sucesión de acontecimientos.

Usos y Finalidad:

- Extraer información y determinar el agente que perpetró el ataque.
- Identificar qué activos de información se vieron afectados y en qué grado, cuándo y dónde se originó, y qué vulnerabilidades se explotaron.
- Es crucial en **procesos judiciales** ya que busca y ofrece evidencias digitales que permitan llevar adelante una causa judicial o sirvan de prueba legal.
- Permite prevenir posibles ataques posteriores.

Fases (Metodología de la Cadena de Custodia):

Para que la evidencia digital tenga validez legal (demostrando su integridad), se sigue el procedimiento de supervisión técnico-legal conocido como **Cadena de Custodia**:

1. **Identificar la evidencia:** Determinar el sistema informático y dónde se encuentran las evidencias digitales, priorizando la preservación de la información **volátil** (ej. memoria RAM).
2. **Aseguramiento de la evidencia:** Proteger la escena del incidente. Esto incluye establecer un perímetro de seguridad, documentar (fotografiar/grabar), desconectar redes y etiquetar cables.
3. **Recogida de la evidencia digital:** Recolección cuidadosa de la evidencia, registrando, fotografiando y precintando los dispositivos, documentando todos los pasos. La información se recoge en orden de volatilidad (de mayor a menor).
4. **Transporte de la evidencia digital:** Trasladar la evidencia temporalmente al laboratorio forense para su análisis y finalmente al depósito de la fiscalía para su custodia y preservación hasta el juicio. Este transporte debe estar claramente documentado.
5. **Realización del informe:** Preparar un informe después del análisis e investigación de las evidencias, redactado en lenguaje asequible, para ser utilizado en procesos judiciales.

Seguridad activa y pasiva. Ejemplos

Tipo de Seguridad	Definición	Ejemplos
Seguridad Activa (Proactiva)	Conjunto de medidas que **previenen** e intentan **evitar los daños** en los sistemas informáticos antes de que se produzca el percance.	Uso de contraseñas, encriptación, *firewalls*, software antivirus, listas de control de acceso (ACLs) y firmas digitales.
Seguridad Pasiva (Correctiva/Reactiva)	Conjunto de medidas que **corrigen y minimizan los efectos** ocasionados por un ataque, accidente, avería o mal funcionamiento.	Sistemas RAID (Redundant Array of Independent Disks), Sistemas de Alimentación Ininterrumpida (SAI) y realización de *Backups*.

Seguridad física y lógica

La seguridad se puede clasificar según el recurso que protege:

- **Seguridad Física:** Conjunto de medidas destinadas a la protección del **hardware** del sistema y su **ubicación** contra amenazas físicas, como desastres naturales, accidentes, averías o robos.
- **Seguridad Lógica:** Conjunto de medidas destinadas a proteger el **software** del sistema (Sistema Operativo, aplicaciones y datos) de diferentes ataques como virus, modificaciones no autorizadas o pérdida de información.

Unidad Temática 2: Seguridad Física y Ambiental

Condiciones ambientales

Suelos, edificio, tratamiento acústico, iluminación

Aspecto	Consideraciones de Seguridad
Edificio / Ubicación	Evaluar que el espacio sea suficiente, el acceso de equipos y personal sea adecuado, y las características de suministro eléctrico y acondicionamiento térmico.
Suelos	Deben evitarse suelos laminados (tarimas, moquetas, PVC) por su mala conductividad eléctrica, ya que acumulan **electricidad estática**. Deben tratarse con productos de limpieza que neutralicen las descargas electroestáticas. Se recomienda elevar la zona de servidores (doble suelo) para proteger contra inundaciones.
Tratamiento Acústico	Los equipos de climatización son ruidosos. Deben instalarse en entornos donde el ruido y la vibración estén amortiguados. Es importante instalar un **techo acústico absorbente** para mitigar el "efecto túnel" de canalización del sonido producido por el falso suelo y falso techo.
Iluminación	Es aconsejable evitar la **luz solar directa** para prevenir el sobrecalentamiento de los equipos. Debe existir alumbrado de **emergencia** y señalización con unidades autónomas de batería.

Temperatura y humedad

- **Temperatura:** La temperatura ideal para los equipos informáticos se sitúa **entre 15 y 25 ºC**. Los cambios extremos de temperatura provocan la dilatación y contracción de los componentes metálicos, lo que puede generar fallos en el equipo. Es vital asegurar la libre circulación de aire y utilizar instalaciones de refrigeración/climatización.
- **Humedad:** El rango ideal de humedad relativa es **entre 35 y 50 %**. Las humedades altas provocan condensación y corrosión de los componentes. Las humedades bajas provocan **descargas eléctricas estáticas** que pueden dañar gravemente los componentes. Se pueden instalar humidificadores o deshumidificadores.

Protección contra incendios: tipos de extinción

Para la protección contra incendios, se debe considerar la seguridad **pasiva** (medidas estructurales) y **activa** (detección y prevención).

- **Medidas Pasivas:** La sala no debe ubicarse sobre áreas con materiales inflamables. Los materiales de construcción deben ser **ignífugos** (paredes, techo, suelo, canalizaciones). Los armarios de almacenamiento de datos críticos deben tener una resistencia al fuego mínima de dos horas.
- **Tipos de Extinción (Agentes Extintores):**
    - **Extintores de agua o espuma están excluidos** en salas de equipos informáticos.

    - Se recomiendan los de **Clase C (o ABC)**, de polvo seco polivalente o **CO2**. El CO2 sofoca el fuego eliminando el oxígeno y no deja residuos contaminantes.
    - **Sistemas de desplazamiento de oxígeno:** Reducen la concentración de oxígeno para extinguir el fuego. Requieren que el personal siga estrictamente las normas de evacuación.
    - **Rociadores de agua nebulizada:** Utilizan agua como agente extintor impulsado por nitrógeno. Es inócua para los equipos y elimina el oxígeno solo en la zona de contacto directo con la llama, lo que no supone riesgo para el personal.

Climatización en CPD pequeño y grande

La climatización debe estar diseñada no solo para aclimatar el cuarto, sino para **refrigerar el equipo**.

- **CPD pequeño:** Se puede optar por un simple aparato de aire acondicionado, el uso de rejillas de ventilación en los muros, o unidades de refrigeración mural o de techo de tipo *split* cuando hay varios equipos en armarios *rack*.
- **CPD grande (con varios racks):** Se implementan **pasillos fríos y calientes**.

Pasillos fríos y calientes. Explicación

En los CPD con varios racks dispuestos en pasillos, se organizan:

- **Pasillos Fríos:** Se enfrentan las partes frontales de los equipos (por donde se introduce el aire frío para la refrigeración), concentrando el aire frío.
- **Pasillos Calientes:** Se enfrentan las partes posteriores de los equipos (por donde estos expulsan el aire caliente en el proceso de ventilación), concentrando el aire caliente.

La eficiencia se puede mejorar con el **cerramiento o contención** de los pasillos fríos o calientes, lo que minimiza la mezcla de aire. El cerramiento de pasillos calientes puede ahorrar un 40% en el coste anual de energía.

Climatización in-row / climatización falso suelo

Estos son dos sistemas principales de climatización utilizados en CPD grandes:

- **Climatización por Falso Suelo (Impulsión de aire frío):** Es el sistema más frecuente en CPD. Requiere un suelo técnico. El aire frío se impulsa por las rejillas instaladas en los pasillos fríos, atraviesa los servidores y retorna caliente por la parte superior para ser enfriado de nuevo.
- **Climatización In-Row (Entre Racks):** Los equipos de refrigeración (tipo *splits*) se instalan entre los racks (en filas). Estos aspiran el aire del pasillo caliente, lo filtran y enfrían, impulsándolo al pasillo frío, creando un **flujo de aire horizontal**. Esta solución evita la necesidad de falsos suelos altos.

Protección frente a robos

Se requiere un férreo control de acceso al CPD. Las soluciones incluyen:

- Puertas bajo llave, puertas blindadas en lugares críticos.
- Servicio de Vigilancia (personal de seguridad).
- Detectores de metales y escáneres de control de pertenencias.
- Sistemas de **protección electrónica** (cámaras de videovigilancia, sensores de movimiento, alarmas).
- Sistemas electrónicos de acceso (teclados con contraseña, tarjetas de proximidad o banda magnética).
- Utilización de **sistemas biométricos** (huellas, iris).
- Para equipos individuales (portátiles, ordenadores de alto coste) instalados en lugares públicos: cadenas o candados antirrobo (cerraduras Kensington).

Soluciones ante problemas de fallos de suministro eléctrico

Los fallos de suministro eléctrico (cortes, subidas/bajas de tensión, ruido) pueden causar corrupción de datos, fallos permanentes en el equipo, o "muerte lenta".

Medidas preventivas y correctivas:

- **Instalación eléctrica:** Debe tener potencia suficiente, elementos homologados y cumplir con normativas. Se recomienda contar con líneas de fuerza dedicadas a equipos que más consumen (ej. refrigeración).
- **Toma de tierra:** Obligatoria, evita el riesgo de electrocución de personas y averías.
- **Estabilizadores de corriente:** Aislan el servidor de las fluctuaciones de la corriente.
- **Acometidas redundantes:** En CPD críticos se recomienda instalar dos o más acometidas de red eléctrica de diferentes compañías.
- **Recursos provisionales/correctivos: Sistemas de Alimentación Ininterrumpida (SAI/UPS)**, **grupos electrógenos** (generadores eléctricos) y luces de emergencia.

CPD: Tipos de CPD respaldo

Los Centros de Proceso de Datos (CPD) de respaldo (DRS - *Disaster Recovery Sites*) son réplicas del CPD principal diseñadas para tomar el control del sistema y evitar la pérdida de datos y disponibilidad si el CPD principal queda fuera de servicio por un desastre.

Tipología	Descripción	Tiempo de Puesta en Funcionamiento	Coste
Cold Site (Sala Fría)	Instalación externa con infraestructura básica (climatización, potencia) pero sin servidores instalados. Requiere trasladar los servidores y reinstalar el	Más de una semana.	El más barato.

	sistema desde copias de seguridad.		
Hot Site (Sala Caliente)	CPD con sistemas, comunicaciones y software análogo al principal (aunque puede tener menor capacidad). Solo requiere restaurar los datos desde el último *backup*.	Menos de un día.	Mayor coste de mantenimiento.
Mutual Backup	Acuerdo con otra organización para usar mutuamente un espacio reservado para servidores de respaldo. Pueden estar apagados o encendidos.	Variable. Similar a Cold o Hot Site.	Moderado.
Mirror Site (Centro Espejo)	Evolución de la Sala Caliente donde los datos se replican en **tiempo real**.	Muy rápido, sin restauración de datos.	Alto.
Configuración Activo-Activo	Los sistemas están en **clústeres geográficos** en ambos CPD. Los usuarios trabajan indistintamente con ambos, y la caída de uno no afecta el servicio porque el otro funciona autónomamente.	Instantáneo (sin parada).	El más alto.

SAI: Tipos, características, y cálculo y selección de un SAI

Un **SAI** (Sistema de Alimentación Ininterrumpida) o **UPS** (*Uninterruptible Power Supply*) es un dispositivo que, gracias a sus baterías, proporciona energía tras un apagón por un tiempo limitado, permitiendo el guardado de datos y el cierre ordenado de equipos. También actúa como un estabilizador, mejorando la calidad de la energía eléctrica al filtrar ruido y estabilizar subidas/bajadas de tensión.

Tipos de SAI

1. **SAI modo espera o fuera de línea (Off-Line / SPS):** La corriente se suministra directamente al ordenador y el SAI solo actúa ante un corte. Apenas corrige imperfecciones. Produce un micro-corte (1-10 ms) al activarse. Es el más barato, utilizado en ordenadores personales. Sus baterías tienen una vida útil más corta.
2. **SAI modo line interactive (In-Line):** Suministra corriente directamente y actúa ante un corte. Incluye un circuito de filtración y estabilización (AVR: *Automatic Voltage Regulator*), pero puede dejar pasar algunas interferencias. Adecuado para ordenadores, centralitas y servidores de PYMES.
3. **SAI modo directo o en línea o de doble conversión (On-Line):** La corriente eléctrica alimenta continuamente a las baterías, y estas a su vez suministran energía constantemente al equipo, independientemente del suministro externo. Estabiliza totalmente la señal. Utilizado en CPDs y equipos críticos. Son más caros y de mayor calidad, aunque las baterías se deterioran más rápido.

Características

- **Autonomía:** Tiempo que el SAI puede seguir alimentando a los equipos conectados tras un fallo. Se mide en minutos. Los fabricantes suelen proporcionar este dato a media carga (50% de la potencia máxima).
- **Potencia:** La energía máxima que el SAI puede suministrar, medida en dos unidades:
    - **Vatios (W):** Potencia activa o real consumida.
    - **Voltiamperios (VA):** Potencia aparente o teórica, que el fabricante suele hacer figurar en las especificaciones.
- **Factor de Potencia (FP):** Relación entre Vatios y Voltiamperios (FP = W/VA), normalmente entre 0 y 1.

Cálculo y selección de un SAI

Para la selección del SAI, se debe determinar la potencia requerida y asegurarse de que el dispositivo pueda cubrirla:

1. **Calcular la potencia activa (W) total** de los equipos que se desea proteger.
2. **Aplicar un margen de seguridad** (ej. 20% más) a la potencia en W.
3. **Determinar la Potencia en VA** necesaria, usando el factor de potencia del SAI ($VA = W / FP$).
4. La carga total enchufada a la batería del SAI no debe sobrepasar el **70%** del total de su potencia máxima.

Nota: Si un SAI es de 1000 VA y su FP es 0.8, la potencia real (W) que puede soportar es $1000 \times 0.8 = 800$ W.

Sistemas biométricos de identificación. Ventajas y desventajas. Indicadores que deben tener.

Los **sistemas biométricos de identificación** abarcan métodos para reconocer de forma única a una persona basándose en sus rasgos físicos o conductuales, o factores genéticos. Se basan en "algo que se es" (característica personal) o "algo que se sabe hacer".

Ventajas

- **Mayor seguridad:** Son difíciles de duplicar o falsificar, ofreciendo mayor seguridad contra la suplantación de identidad.
- **Comodidad:** "La clave se lleva encima". No se pueden olvidar, perder o sustraer (a diferencia de contraseñas o tarjetas).

Desventajas

- **Coste y complejidad:** Son más caros de implementar y requieren hardware o software especializado.

- **Falsos resultados:** Uno de los principales problemas es la generación de **falsos positivos** (acceso a personas no autorizadas) o **falsos negativos** (denegación de acceso a personas autorizadas).
- **Aceptación Social/Privacidad:** Los usuarios pueden sentirse controlados. Ciertos métodos pueden comprometer información personal sensible (ej. ADN, consumo de estupefacientes) o generar recelo (ej. luz proyectada en el iris).

Indicadores que deben tener

Para que un control de acceso biométrico sea fiable, debe basarse en características humanas que cumplan los siguientes indicadores:

- **Universalidad:** Todos los individuos deben poseer esa característica.
- **Unicidad:** La característica debe ser distinta en cada individuo.
- **Permanencia:** La característica no debe modificarse con el tiempo (ni a corto ni a largo plazo).
- **Cuantificación:** Debe poder medirse con cualquier sistema (numérico, físico o matemático).

Ejemplos de sistemas comunes:

- **Iris y retina:** Alta fiabilidad, el iris es inalterable a lo largo de la vida.
- **Huellas dactilares:** Más utilizado, bajo coste, alta fiabilidad.
- **Reconocimiento facial:** Fiabilidad media-baja debido a variaciones por el paso de los años, disfraces o factor iluminación.
- **Manos:** Reconocimiento del entramado de venas de las palmas (alta fiabilidad) o geometría de la mano.

La seguridad informática puede verse como un castillo: la **Seguridad Física** son los muros, el foso y las torres que protegen la estructura; la **Seguridad Lógica** es la inteligencia interna que defiende los tesoros (los datos) que se encuentran dentro. Las medidas de **Seguridad Activa** son los vigías que previenen el ataque, mientras que las medidas de **Seguridad Pasiva** son los equipos de rescate y reconstrucción que actúan después del asalto.