¿POR QUÉ?

- Auge de Internet
  - Operaciones bancarias
  - Compras
  - Negocios de empresas
- Fallos en seguridad
  - Pérdidas económicas
  - Problemas legales
- Debemos conseguir un nivel de seguridad aceptable
  - Evitar fallos
  - Recuperarnos de los fallos, rápido y eficientemente.

ACTIVOS

- El objetivo de la seguridad informática es proteger los activos informáticas:
  - Información contenida.
  - Infraestructura física.
  - Los usuarios.

OBJETIVOS

- Confidencialidad: información almacenada o transmitida por la red sólo disponible para las personas autorizadas.
- Disponibilidad: Tanto el sistema como los datos deben estar disponibles para el usuario en todo momento.
- Integridad: Información válida y consistente. No ha sido modificada sin autorización.
- Autenticación: verificar que un documento ha sido elaborado o pertenece a quien el documento refleja.
- No repudio: Garantiza la participación de las partes en una comunicación:
    - **En origen:** El emisor no puede negar que lo es.
    - **En destino:** El receptor no puede negar que lo ha recibido.

CLASIFICACIÓN DE SEGURIDAD

- En función del activo a proteger:
  - Física → Hardware
  - Lógica → Software
- En función del momento de actuación:
  - Activa: Antes del percance, para evitar los fallos.
  - Pasiva: Después del percance, para minimizar los efectos.

SEGURIDAD FÍSICA

- Trata de proteger el hardware de posibles desastres naturales.

Amenaza	Defensa
Incendios	Mobiliario ignífugo. Evitar localización peligrosa Sistemas antiincendios, detectores de humo...
Inundaciones	Evitar plantas bajas. Impermeabilización de paredes, techos, sellado de puertas...
Robos	Puertas con medidas biométricas, cámaras, vigilantes...
Señales electromagnéticas	Evitar lugares con radiaciones electromagnéticas Filtros o cableado especial. La fibra óptica no es sensible a esto.
Apagones	SAI
Sobrecargas eléctricas	SAI. También estabilizan la señal eléctrica
Desastres naturales	Estar en contacto con los organismos que proporcionan información sobre terremotos o desastres meteorológicos.

SEGURIDAD LÓGICA

- Complemento a la seguridad física. Protege el software de virus, ataques de la red...

Amenaza	Mecanismo de defensa
Robos	Cifrado. Contraseñas Sistemas biométricos
Pérdida de información	Copia de seguridad (distintas ubicaciones) Sistemas tolerantes a fallos Discos redundantes
Pérdida de integridad de la información	Programas de chequeo del equipo. Firma digital Comando sfc
Entrada de virus	Antivirus
Ataques desde la red	Firewall Programas de monitorización Proxys
Modificaciones no autorizadas	Contraseñas Listas de control de acceso Cifrar documentos

SEGURIDAD ACTIVA

- Previenen e intentan evitar el daño.

Técnicas	¿Qué previene?
Contraseñas	Previene el acceso a recursos a usuarios no autorizados
Listas de control de acceso	Previene acceso a ficheros a usuarios no autorizados
Encriptación	Evita a personas no autorizadas interpretar la información
Software de seguridad	Evita virus y accesos no deseados al sistema
Firmas y certificados digitales	Comprueba la procedencia, autenticidad e integridad de los mensajes
Sistemas de ficheros tolerantes a fallos	Previene fallos de integridad
Cuotas de disco	Previene el uso excesivo de disco por parte de algún usuario

SEGURIDAD PASIVA

- Complementa a la seguridad activa, trata de minimizar los daños.

Técnicas	Resultado
Discos redundantes	Restaurar datos que han quedado inconsistentes
SAI	Proporcionan energía durante un periodo de tiempo.
Copias de seguridad	Podemos recuperar información en caso de pérdida de datos.

Vulnerabilidad, malware y exploit

- **Vulnerabilidad:** Defecto de una aplicación que puede ser aprovechado.
- **Malware:** Programa malicioso que aprovecha vulnerabilidades para introducirse en el sistema.
- **Exploit:** Pieza de software que provoca una acción no deseada en el sistema invadido.

Tipos de Vulnerabilidades

- Vulnerabilidades reconocidas y con solución. Se instala parche.
- Vulnerabilidades reconocidas y sin solución de momento. Recomendable desactivar el servicio afectado.
- Vulnerabilidad no reconocida. Estamos en peligro sin ser conscientes de ello.

TIPOS DE ATACANTES

- **Hackers**: Atacan sistemas por curiosidad.
- **Crackers**: Hacker que quiere causar daño u obtener beneficio.
- **Script kiddie:** Se descargan scripts maliciosos y los utilizan sin conocer sus efectos ni sus consecuencias.
- **Sniffers**: Analizan el tráfico de la red para obtener información de los paquetes trasmitidos.
- **Lammers**: Se consideran Hackers pero no tienen suficientes conocimientos para ello.
- **Newbie**: Hacker novato.
- **Ciberterrorista**: Experto informático que trabaja para países u organizaciones como espías o saboteadores.
- **Programadores de virus:** Crean programas dañinos para los sistemas o aplicaciones.
- **Carders:** Atacan sistemas de tarjetas de crédito.

OTRA CLASIFICACIÓN DE ATAQUES

- **Spoofing:** Suplanta la identidad de un PC
- **Sniffing**: Analiza el tráfico de red para hacerse con información.
- **Conexión no autorizada:** Se busca un agujero de seguridad y se entra en el sistema.
- **Malware:** Se introducen programas malintencionados en nuestro sistema.
- **Keyloggers:** Almacenan lo que se teclea e incluso hacen capturas de pantalla para averiguar contraseñas.
- **Denegación de servicio:** Interrumpe el servicio de servidores o redes.
- **Ingeniería social:** Se obtiene información confidencial de una persona para utilizarla con fines maliciosos.
- **Phishing:** Se engaña al usuario para obtener su información confidencial suplantando la identidad de un organismo o página web.

PROTECCIÓN

- No instalar nada innecesario
- Actualizar parches de seguridad
- Formar a los usuarios
- Instalar Firewall
- Copias de seguridad
- Gestionar y revisar los logs del sistema.

LEY DE PROTECCIÓN DE DATOS

- La gestión de datos personales está regulada por la Ley de Protección de Datos de Carácter Personal.(LO 15/1999).
- Cuando se vaya a crear un fichero con datos personales se debe solicitar la aprobación de la Agencia de Protección de Datos.
- Niveles de seguridad en función de los datos almacenados
  - Básico → Datos personales
  - Medio → infracciones, gestión tributaria, datos fiscales y financieros.
  - Alto → Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

NORMATIVA DE LOS SISTEMAS DE INFORMACIÓN Y COMERCIO ELECTRÓNICO

- Regulado por la Comisión del Mercado de las Telecomunicaciones. Ley 34/2002.
    - Las empresas deben proporcionar información con nombre, domicilio, dirección de correo electrónico, número de identificación fiscal y precio de los productos.
    - Exculpa de responsabilidad siempre que no tengan conocimiento de la información contenida en sus servidores.
    - Los contratos realizados por vía electrónica son válidos.