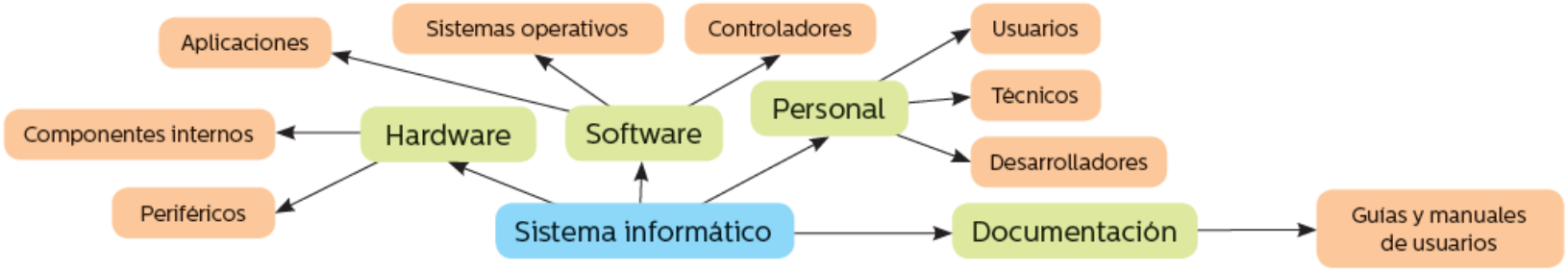
Seguridad informática

1. El sistema informático y sus elementos sensibles

Sistema informático



Elementos sensibles de un sistema informático

Integridad

- Mantiene su estructura y el ciclo de funcionamiento.

Confidencialidad

- El flujo de información es controlado.

Disponibilidad

- El elemento está disponible cuando se necesita y el tiempo previsto.

Seguridad informática

2. Seguridad y tipos de amenazas

2.1 Tipos de amenazas

La **seguridad informática** se encarga de que un sistema sea lo mas seguro posible y que las vulnerabilidades que pueda tener se solucionen de forma rápida y efectiva.

Tipos de amenazas

Amenazas físicas	Amenazas lógicas
• Afectan a la parte física del sistema: hardware. • Pueden estar originadas por el hombre, voluntaria o involuntariamente. • Fáciles de predecir. • Medidas de prevención y protección eficaces y contundentes.	• Afectan fundamentalmente a la parte lógica del sistema: software. • Funcionamiento anómalo del software instalado, intencionado o no. • Difíciles de prever, y no se suelen eliminar hasta que no se detectan. • Producen daños difíciles de reparar.

Seguridad informática

2. Seguridad y tipos de amenazas

2.2.1 Tipos de amenazas lógicas

Virus

- Altera el funcionamiento del sistema sin el consentimiento del usuario.
- **Origen:** archivos ejecutables o que pueden abrirse directamente.
- **Como evitarlos:** no instalar programas ni abrir archivos desconocidos.

Spyware

- Aplicación espía que se instala en el equipo y recopila información para transmitirla al exterior.
- **Origen:** programas gratuitos, portables, descargas directas no fiables.
- **Como evitarlos:** mantener actualizados tanto SO como navegador.

Gusanos

- Malware que trata de colapsar los equipos y redes de comunicación.
- **Origen:** archivos ejecutables o que pueden abrirse directamente.
- **Como evitarlos:** extremando las precauciones en los intercambios de archivos.

Ransomware

- Malware que restringe el acceso al sistema y a los archivos y exigiendo un pago por su rescate.
- **Origen:** a través de correos electrónicos en los que se encuentra adjunto o al visitar una web infectada.
- **Como evitarlos:** tener actualizado el software del equipo.

Seguridad informática

2. Tipos de amenazas

2.2.1 Tipos de amenazas lógicas

Troyanos

- Introduce sin consentimiento del usuario una aplicación para controlar el equipo remotamente.
- **Origen**: archivo ejecutable con capacidad para ejecutarse directamente.
- **Como evitarlos**: no abrir archivos desconocidos adjuntos al correo electrónico o de sitios de dudosa fiabilidad, y tener actualizado antivirus y cortafuegos.

Rootkits

- Programas que ocultan evidencias de infecciones en el sistema.
- Son introducidos por creadores de malware para que sus amenazas no sean detectadas.
- **Origen**: se introducen de muchas formas, incluso a través de productos comerciales de seguridad y extensiones de aplicaciones. No pueden propagarse automáticamente.
- **Como evitarlos**: se debe mantener todo el software de sistema actualizado.

Exploits

- Técnica o aplicación que aprovecha fallos de seguridad del sistema (bug) para infectar el equipo, controlarlo, sustraer información, etc.
- **Origen**: por errores en el proceso de desarrollo del software que suponen brechas de seguridad.
- **Como evitarlos**: para evitar expoits se instalan parches de seguridad o se actualizan las aplicaciones a la última versión.

Seguridad informática

3. Niveles de seguridad

Nivel D

Sistema informático sin protección para hardware ni autenticación para acceso a recursos.

Nivel C1

El hardware tiene cierta protección y hay autenticación de usuario y una cuenta de administrador.

Nivel C2

Con mecanismos para controlar el acceso al sistema y recursos. Operaciones auditadas y más de un administrador.

Nivel B1

Seguridad multinivel: permisos y usuarios.

Nivel B2

Introduce mecanismos para comunicar elementos del sistema con diferente nivel de seguridad.

Nivel B3

Introduce mecanismos de protección de hardware.

Nivel A

El sistema se controla y verifica desde su creación para asegurar procesos seguros.

Seguridad informática

4. Análisis y control del riesgo

El riesgo se calcula a partir de dos variables cualitativas:

- La **probabilidad** de amenaza.
- La **magnitud** del daño de dicha amenaza sobre el elemento.

Riesgo alto (11-16)

Riesgo medio (8-10)

Riesgo bajo (1-7)

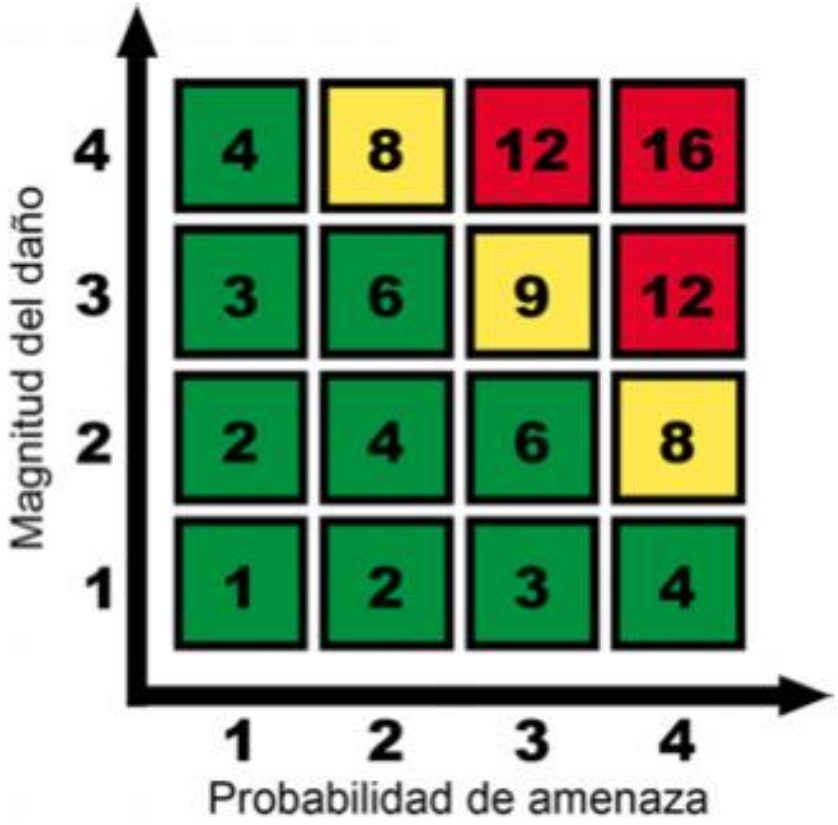
Valores

1→Insignificante

2→Bajo

3→Mediano

4→Alto



Seguridad informática

4. Análisis y control del riesgo

Del estudio de riesgos y magnitud se obtienen las medidas destinadas a prevenir y proteger el sistema. Se pueden clasificar en:

Medidas físicas y técnicas

- **Seguridad física**: protege elementos físicos.
- **Seguridad lógica**: protege accesos a la información.

Medidas personales

- Formación de usuarios del sistema.
- Sensibilización sobre seguridad e integridad del sistema.

Medidas organizativas

- Protocolos de actuación en caso de desastre.
- Auditoría y seguimiento de los elementos del sistema y accesos.

Seguridad informática

5. Mecanismos de seguridad física

Se encargan de la protección del hardware del sistema.
En sistemas empresariales hay un Centro de Proceso de Datos (CPD) donde se alojan los servidores y electrónica de red base del sistema.
En un CPD se utilizan los siguientes mecanismos:

Sistema antiincendios

- Desde un extintor a agua nebulizada o polvo.
- Pintura intumescente o antifuego.

Control inteligente

- Con la domotización pueden controlarse puertas, cámaras, etc.
- Integra diferentes mecanismos de seguridad difíciles de graduar.

Sistema de protección eléctrica

- Instalación preparada para evitar cortes y sobrecargas en el suministro.
- Sistemas de alimentación ininterrumpida (SAI) actúan como puente entre la línea eléctrica y los equipos.

Seguridad informática

5. Mecanismos de seguridad física

Sistema de control de accesos

- Restringe el acceso a zonas que no deben ser manipuladas por cualquier usuario.
- Hay varios tipos:
  - **Tarjetas**: chip PKI, banda magnética, de proximidad, con o sin contraseña.
  - **Sistemas biométricos**: firma, huella digital, voz o patrones oculares.

Sistema de climatización

- Controla la temperatura y humedad del entorno de los equipos.

Protección contra desastres naturales

- Depende de la ubicación del sistema.
- Se protege al CPD de terremotos, inundaciones, etc.

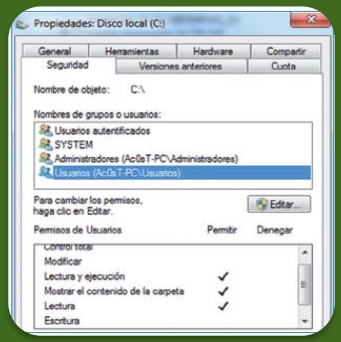
Seguridad informática

6. Mecanismos de seguridad lógica

Se encargan de la protección del software del sistema.
Los mecanismos más comunes son los siguientes:

Autenticación por contraseña

- Cada sistema se basa en su política de contraseña basada en:
  - Vigencia.
  - Complejidad.
  - Confidencialidad.



Permisos y políticas de usuario

- Los administradores diseñan una estructura de acceso a los usuarios a los recursos e información para los que están autorizados.

Seguridad informática

6. Mecanismos de seguridad lógica

Encriptación

- Acción de codificar un dato para que no sea accesible. Puede darse:
  - En el **almacenamiento y acceso a la información** con dos tipos de codificación:
    - **Reversible**: logaritmo que encripta los datos; el algoritmo inverso los desencripta.
    - **Irreversible**: no hay algoritmo inverso (ej. las contraseñas).
  - En el **tráfico de información** entre dos puntos. Los más comunes son:
    - Cifrado simétrico: una clave para cifrar y descifrar.
    - Cifrado asimétrico o de clave pública: utiliza dos claves, pública y privada.

Protección contra malware

- Evitar abrir ficheros sospechosos y usar el antivirus.
- Mantener el sistema operativo y aplicaciones actualizados.
- Hacer análisis del equipo periódicamente.

Seguridad informática

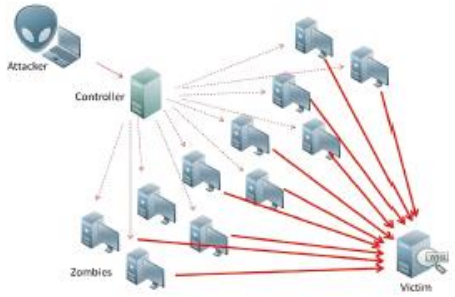
7. Ataques más comunes

DoS (Denegación de servicio)

- Infecta varios equipos para controlarlos y colapsarlos.

Spoofing

- Suplanta la identidad de un equipo o usuario haciendo acciones sobre un sistema en su nombre.



Phising

- Suplanta la identidad de un equipo o sitio web para que el usuario proporcione sus datos.

Sniffing

- Captura tráfico en el sistema y extrae datos, claves, etc.

Hijacking

- Sustituye la página de inicio del navegador.

Inyección de código

- Trata de conseguir acceso o información de servidores.

Seguridad informática

8. Buenas prácticas

El Instituto Nacional de Ciberseguridad (INCIBE) propone las siguientes prácticas de seguridad informática:

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

General

- Mantenerse informado sobre novedades y alertas de seguridad.
- Mantener actualizado el equipo.
- Hacer copias de seguridad de datos importantes con cierta frecuencia.
- Utilizar software legal.
- Utilizar contraseñas fuertes.
- Utilizar herramientas de seguridad para proteger el equipo.

Correo electrónico

- No abrir nunca ficheros adjuntos sospechosos.
- Utilizar un filtro anti-spam.
- Desactivar la vista previa del cliente de correo.
- No facilitar la cuenta de correo electrónico a desconocidos.
- No responder a falsos mensajes ni cadenas de correos.
- Borrar el historial de destinatarios al reenviar un correo.

Seguridad informática

8. Buenas prácticas

Navegación

- No descargar o ejecutar ficheros de procedencia sospechosa.
- Analizar con el antivirus todo lo que se descarga.
- Mantener el navegador actualizado.
- Configurar adecuadamente el nivel de seguridad del navegador.
- Instalar y configurar correctamente un cortafuegos.
- Descargar los programas desde los sitios oficiales.
- Evitar las ventanas emergentes.
- Borrar las cookies, los ficheros temporales y el historial al usar equipos ajenos.

Banca y comercio electrónico

- Comprobar que la dirección es segura (empieza por https y aparece un candado).
- Asegurarse de la validez de los certificados.
- Tener en cuenta que un banco nunca pide información confidencial por e-mail.
- Evitar el acceso a estos sitios web en equipos públicos.
- Desactivar la opción de autocompletar campos.
- Cerrar la sesión cuando se finalice la navegación o compra.

Seguridad informática

8. Buenas prácticas

Redes P2P

- Analizar todos los archivos que se descarguen antes de ejecutarlos.
- No compartir software ni contenido ilegal.
- Ejecutar el cliente P2P en una sesión de usuario con permisos limitados.

Juegos en línea

- Evitar compartir el usuario / contraseña fuera de la plataforma del juego.
- Mantener actualizado el software del juego.
- No adquirir créditos ni bonificaciones del juego fuera de las páginas oficiales.
- Vigilar los movimientos de la cuenta o tarjeta bancaria.

Dispositivos móviles

- Desactivar las conexiones inalámbricas (WiFi y Bluetooth) cuando no se usen.
- No aceptar conexiones de dispositivos desconocidos.
- Ignorar SMS y MMS de origen desconocido.
- Activar el acceso por PIN y proteger el acceso al dispositivo.
- Bloquear la tarjeta SIM es caso de pérdida o robo.
- No descargar software de sitios poco fiables o sospechosos.
- Leer los acuerdos de usuario y los permisos necesarios antes de instalar software.

Seguridad informática

En resumen