Fundamentos Tecnológicos para el Tratamiento de Datos

Profesor: Serhiy Lyalkov

Tema 8

Seguridad en los sistemas de información

unir
LA UNIVERSIDAD
EN INTERNET

La Universidad en Internet

Índice de la sesión

Esquema

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

- La navegación por la web está sujeta a numerosos riesgos, vulnerabilidades y peligros.
- La seguridad en los sistemas de información afecta tanto al usuario final como a los propios oferentes de servicio.
- Actualmente supone uno de los pilares básicos de la propia actividad de una empresa. Ninguna empresa es ajena a esta problemática.
- Básicamente dos son las vulnerabilidades fundamentales de cualquier sistema de información: el *software* malicioso y los robos de identidad.

SOFTWARE MALICIOSO

El *software* malicioso o *malware* es un tipo de software cuyo objetivo es infiltrarse en un equipo o sistema informático sin el consentimiento del usuario.

Robos de identidad

Tratan de suplantar la identidad del usuario para, una vez obtenida, tener acceso total a la red de comunicación. Destacan *el phishing, pharming, ransomware* o *keyloggers*.

- **Virus informático.** Son programas informáticos que se instalan e infiltran en los dispositivos informáticos de forma que la información pueda quedar expuesta.
- ***Spyware***. Es un programa que se instala en el ordenador para espiar toda la información existente en el dispositivo.
- **Gusanos informáticos**. Son similares a los virus informáticos, pero no necesitan de intervención humana.
- ***Troyanos***. Es un tipo de *software* que intenta crear puertas o entradas al sistema para que otros programas maliciosos puedan entrar.

HERRAMIENTAS PARA LA SEGURIDAD

Las empresas disponen de una amplio abanico de herramientas para proteger sus sistemas de información. Se dividen si están orientados a garantizar el acceso al usuario.

Pilares de la seguridad de la información

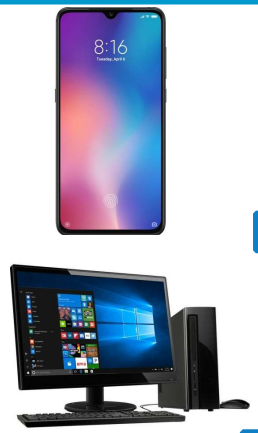
Tres son los grandes pilares de la seguridad de la información en la empresas: la **confidencialidad**, la **disponibilidad** y la **integridad de los datos**.

- **Autenticación biométrica.** Uso de rasgos humanos para autenticarse.
- **Certificados digitales.** Permite identificarse, con plena validez jurídica.
- ***Token***. Dispositivo físico que garantiza el acceso autorizado o a impedir dicho acceso a usuarios no autorizados.
- ***Firewall***. Protege a una computadora o una red de computadoras evitando las intrusiones de usuario con acceso no autorizados.
- **Antivirus.** Software que ayuda a proteger a nuestra computadora contra la mayoría de los virus, gusanos, troyanos y otros programas que puedan infectar nuestra PC.

8.1 Introducción y Objetivos

8.1 Introducción y objetivos

Usuario

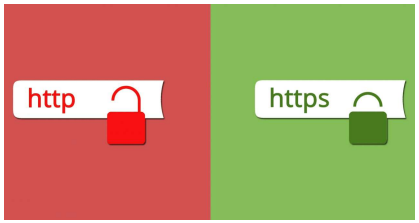


Red / Internet

Robo o brechas de datos o información

Objetivo:
- Riesgo
+ Seguridad

Medidas:
- Equipo de ciberseguridad
- Formación al usuario
- Oferentes de servicios



Objetivos:

- Principios básicos Seguridad
- Protección de la información
- Herramientas

8.2 Seguridad en los sistemas de información

8.2 Seguridad en los sistemas de información

RED

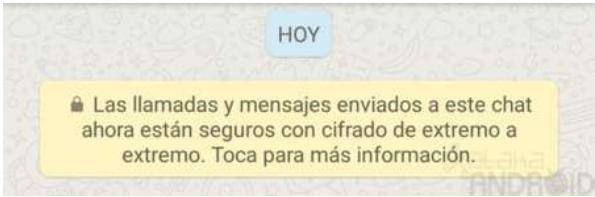
+ Interconexiones → + Vulnerabilidades

Redes públicas

- + Tamaño + Aberturas + Riesgos
- ADSL o Fibra vía router
- Redes inalámbricas

Mensajería

- Datos personales
- Archivos adjuntos
- Información confidencial



Redes P2P

- Peer to Peer
- Ordenadores interconectados
- sin clientes/servidores FIJOS

8.2 Seguridad en los sistemas de información

Tipologías de vulnerabilidades

Software Malicioso

- Infiltración en sistema
- Sin consentimiento
  - Virus
  - Gusanos
  - Spyware
  - Troyanos

Robos de identidad

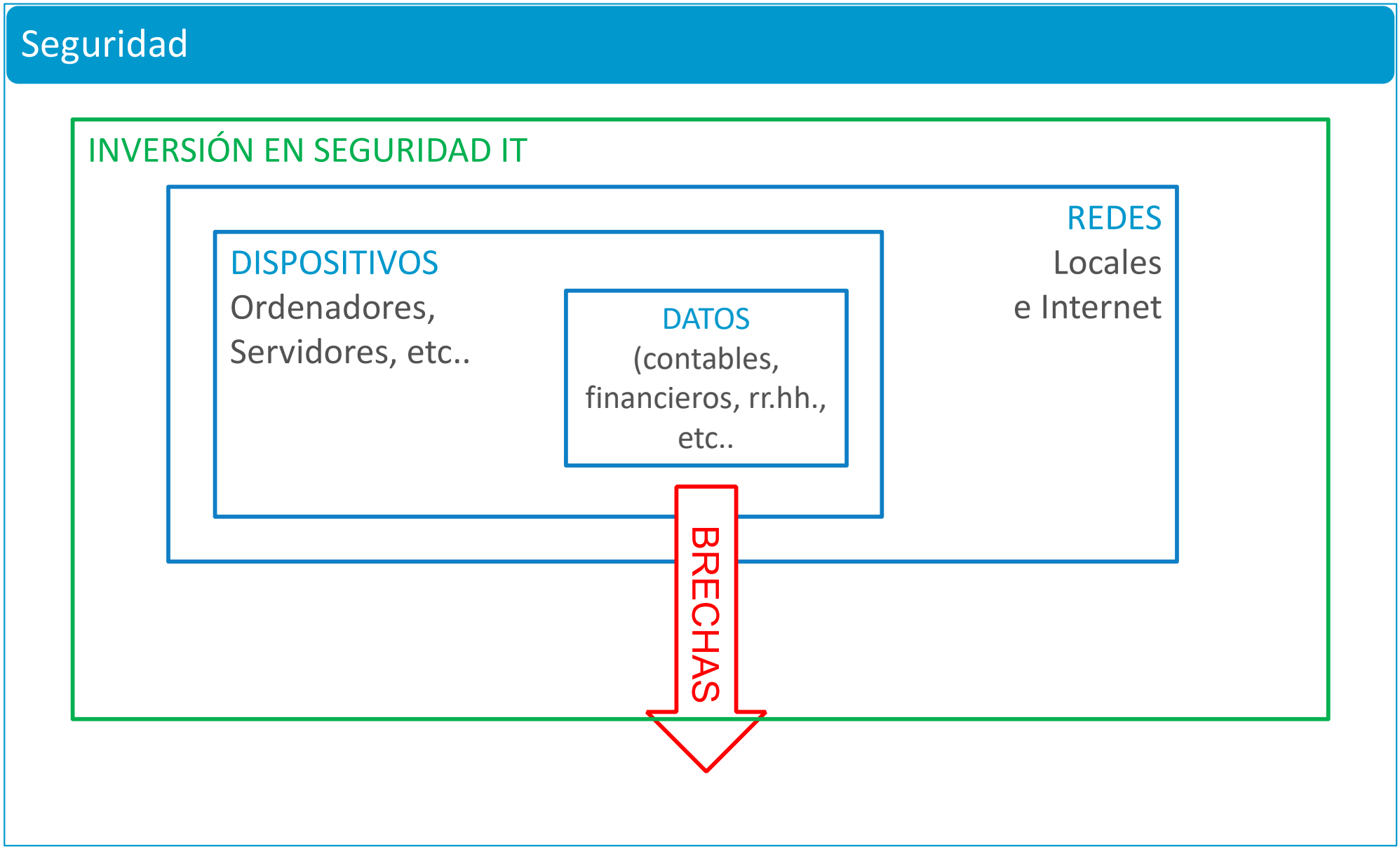
- Suplantación
- Acceso a la red de comunicación
  - Phishing
  - Pharming
  - Ransomware
  - Keylogger

Redes inalámbricas

- Cable vs Wifi
- Redes públicas abiertas
- WEP
- WPA
- WPA2

8.3 Seguridad de la información en la empresa

8.3 Seguridad de la información en la empresa



8.3 Seguridad de la información en la empresa

Seguridad

INVERSIÓN EN SEGURIDAD IT

ASPECTOS BÁSICOS DE SEGURIDAD

CONFIDENCIALIDAD	DISPONIBILIDAD	INTEGRIDAD
• √ Autorizado • × No autorizado	• Acceso ágil • Acceso seguro	• Reales • Correctos

RIESGOS:

- Almacenamiento móvil:
  - SW Malicioso
  - Contraseñas y permisos
  - Accesibilidad no autorizada
- Correo Electrónico
  - Difusión a listas de distribución
  - Phishing y SPAM
  - Datos sensibles
- Software Pirata
  - Origen desconocido
  - “Gratuitos”

8.3 Seguridad de la información en la empresa

Seguridad

INVERSIÓN EN SEGURIDAD IT

Medidas:

- **Formación de empleados**
  - Ética y concienciación
  - Buenas practicas
  - Preguntar en caso de duda

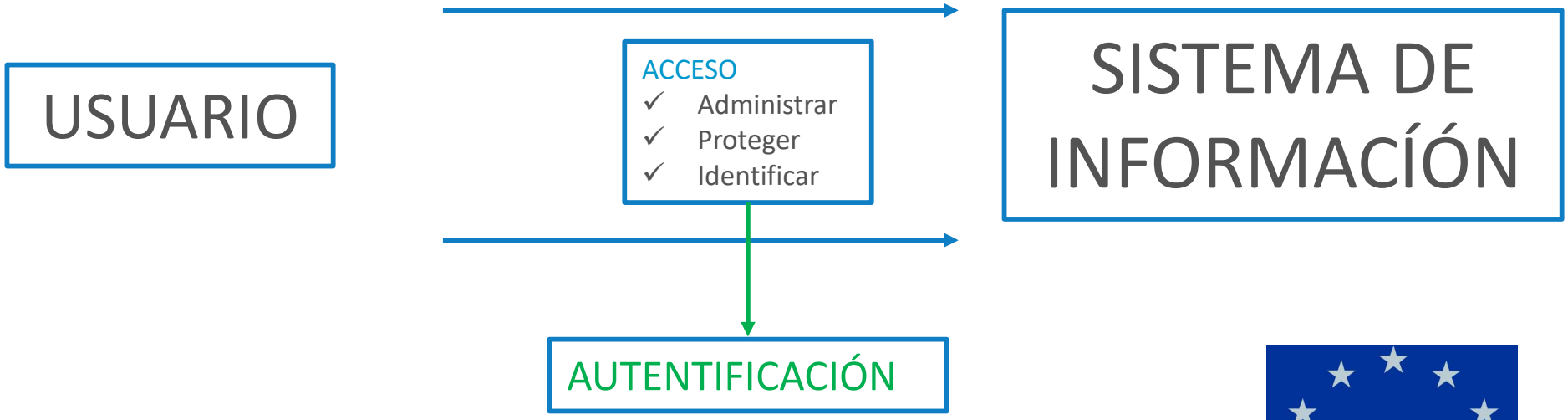
- **Software Original**
  - Actualizaciones
  - Garantía del proveedor
  - Gestión optima de contraseñas y permisos
  - ↓ Accesos no autorizados

- **Políticas y permisos**
  - Asignación y gestión de contraseñas
  - Políticas de uso
  - Permisos por roles o usuarios
  - Copias de seguridad

8.4 Tecnologías y herramientas para proteger la información

8.4 Tecnologías y herramientas para proteger la información

Autentificación



- Autentificación biométrica: huella o escáner de retina
- Certificados digitales: persona física o jurídica | validez jurídica
- Token: almacenan claves, PINs, firmas digitales, datos biométricos, etc…
- Mensajería bidireccional: claves por SMS o correo

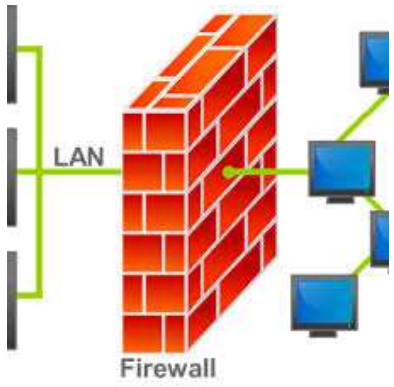
Autenticación de 2 pasos

PSD2

Microsoft Authenticator

8.4 Tecnologías y herramientas para proteger la información

Herramientas de protección



Firewall

Antivirus

Antispyware

Antispam

SI

Windows Defender

panda

kaspersky

avast
Internet Security
avast.com

A fondo

- Oficina de seguridad del internauta (OSI). https://www.incibe.es/

- Asociación española para el fomento de la seguridad de la información. https://www.ismsforum.es/index.php

Resumen

- Conocer los principios básicos de la seguridad.

Amenazas como software malicioso, robos de identidad y vulnerabilidad inalámbrica

- Saber como proteger la información en la empresa.

"Confidencialidad, disponibilidad e integridad"

Formación de empleados, software original, contraseñas, políticas de uso, etc…

- Diferenciar entre los distintos tipos de herramientas

Autentificación: biométrica, certificados, dos pasos, etc…

Protección: firewall, antivirus, antispyware y antispam


unir
LA UNIVERSIDAD
EN INTERNET