Seguridad (informática) en redes corporativas

Algunos aspectos de la seguridad informática en departamentos de salud

Joan Pau García Úbeda – Informática Hospital Lluís Alcanyís – Departament Xàtiva-Ontinyent - AVS

Objetivos

- Revisar conceptos sobre **redes** y **seguridad**
- Enumerar las **dimensiones** o servicios de la seguridad en redes.
- Presentar **aspectos de seguridad** dentro de proyectos recientes en hospitales
- Reconocer **buenas prácticas** del profesional en entorno corporativo.

Índice

- Introducción y conceptos
  - Seguridad. Riesgo. Amenaza. Servicio
- Aspectos en proyectos recientes
  - Organización de la seguridad
  - Implantación del Modelo de red de hospital
  - Gestión del puesto de trabajo (Antivirus)
- Buenas prácticas.

Introducción y conceptos

- Red informática
  - Construcción de una red
- Seguridad
  - Seguridad en redes ó Informática

Seguridad

- “Se aplica también a ciertos mecanismos que aseguran algún bien fundamental, precaviendo que este falle, se frustre o se violente”

Red informática / telemática

conjunto de equipos conectados
mediante un medio de transmisión de datos,
que permite acceder a
información, recursos y servicios,
con intención de proporcionar
un valor añadido
a la organización.

Construcción de una red

- Protocolo: reglas para la comunicación entre al menos dos entidades para ofrecer un servicio.
- Elementos de interconexión
  - Electrónica de red: Routers, switches, tarjetas de red

Esto posibilita construir desde una red (domestica o de empresa) hasta el propio Internet

  - Algo practico pero complejo, que podemos utilizar sin conocimiento técnico.

Riesgos

Pero implica riesgos

- Uso inapropiado. Circulación de información sensible. Intentos de acceso ilegitimo. Caídas.

Las redes son vulnerables, no hay una seguridad total y absoluta.

Es necesario medir y priorizar los riesgos para su posterior tratamiento.

Gestión de riesgos

- Identificar los Riesgos
- Valorar los Riesgos
  - Probabilidad de ocurrencia
  - Consecuencia sobre los objetivos
  - Plazos de respuesta al problema/oportunidad
  - Tolerancia al riesgo de los implicados
- Tratamiento y control de Riesgos
  - Priorizar y actuar

Seguridad en redes

- Complejo, con multiples matices.
- La Seguridad (en redes) es el proceso de la organización que conduce a minimizar sus vulnerabilidades.
- La Seguridad en redes es el conjunto de técnicas, mecanismos, procedimientos y servicios destinados a minimizar las vulnerabilidades de bienes y servicios

Seguridad en redes

Mecanismos de seguridad:

- en base a sistemas como la criptografía permiten construir protocolos de seguridad

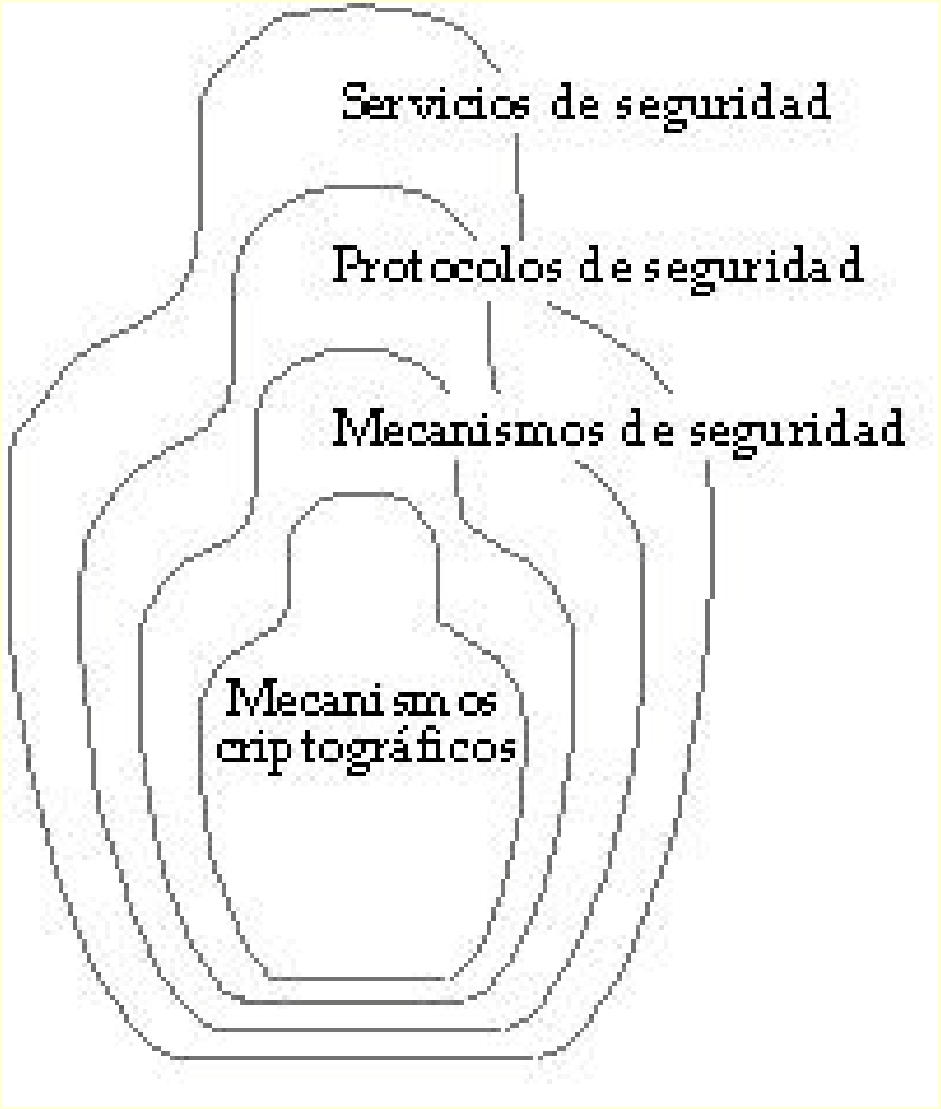
Protocolo de seguridad:

- reglas para la comunicación entre al menos dos entidades para ofrecer un servicio de seguridad

Los **servicios de seguridad:**

- protegen las comunicaciones de los usuarios frente a, ataques, amenazas o riesgos:

Servicios de seguridad



Amenazas sobre los servicios

Los **servicios de seguridad** protegen las comunicaciones de los usuarios frente a los distintos **ataques, amenazas o riesgos**:

- **sobre la identidad de las entidades**
  - (interceptación y suplantación),
- **sobre la información**
  - (intromisión, escucha, revelación, reenvío, manipulación y repudio de datos) y
- **sobre los servicios**
  - (negación del servicio y apropiación).

servicios de seguridad al usuario (dimensiones)

- la disponibilidad
- el control de acceso,
- la confidencialidad de datos,
- la integridad de datos,
- la autenticación de entidades,
- el no repudio,
- el anonimato o privacidad

servicios de seguridad al usuario (dimensiones) 1

- Disponibilidad
  - Estado correcto de un recurso, accesible y usable.
- Control de acceso
  - Los recursos de red son usados solo por usuarios autorizados
- Confidencialidad
  - Los datos solo serán usados por los usuarios autorizados.
- Integridad
  - Los datos no han sufrido cambios ni inconsistencias.

servicios de seguridad al usuario (dimensiones) 2

- Autentificación
  - Garantiza que una entidad o usuario es quien dice ser.
- No repudio
  - Adquisición de una prueba irrefutable de: el origen de los datos, el momento del envío, de la entrega al destinatario
- Anonimato y Privacidad
  - Cuando es necesario se respetará la ocultación de identidad imposibilitando la identificación

Cifrado Asimétrico

Que proteger, capas.

- Los equipos y conexiones de la red
- Los servicios
- Las aplicaciones
- La información

La fortaleza de la red es la de su eslabón mas débil.

Dimensiones y capas

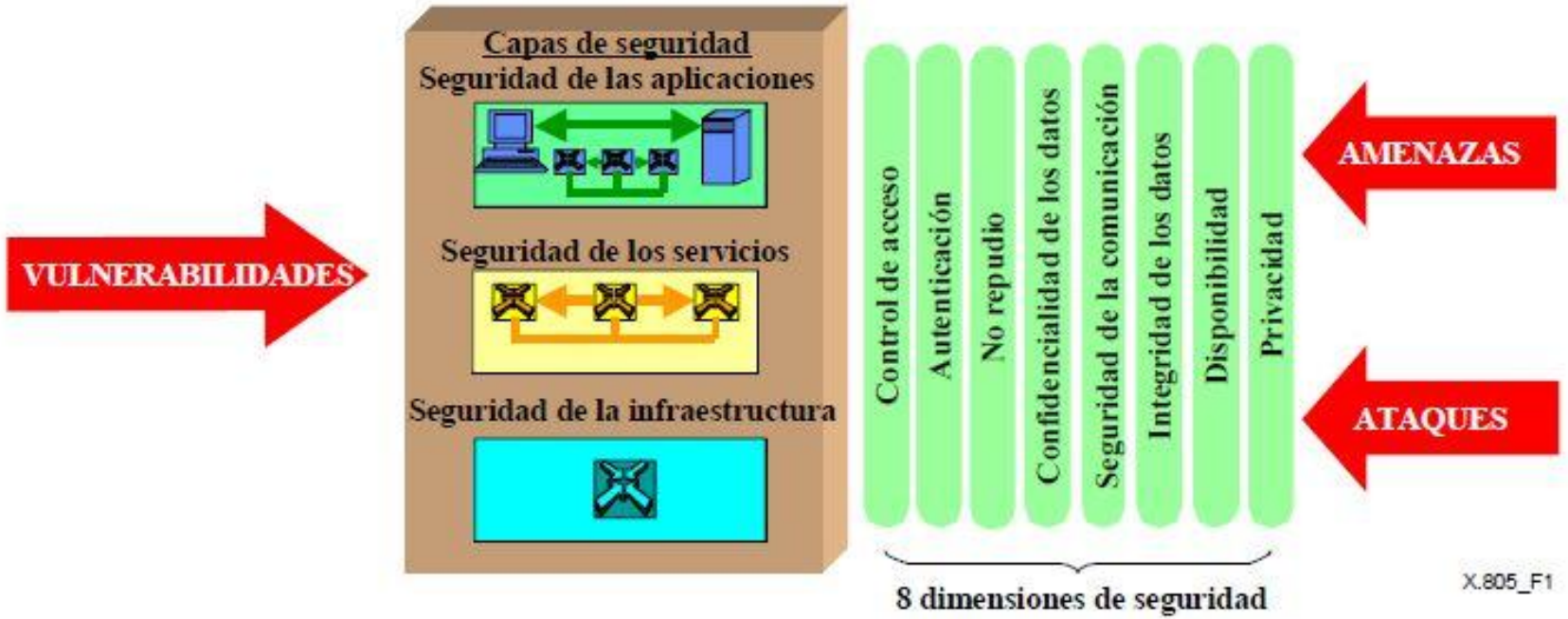


Figura 1/X.805 – Aplicación de las dimensiones de seguridad a las capas de seguridad

“Seguridades”

- Seguridad Física
- Seguridad Lógica
- Seguridad Técnica
- Seguridad Administrativa

Aspectos en proyectos recientes

- Organización de la seguridad
- Implantación del Modelo de red de hospital
- Gestión del puesto de trabajo (Antivirus)

Políticas de seguridad

La mejor forma de proteger la red de una organización es mediante la:

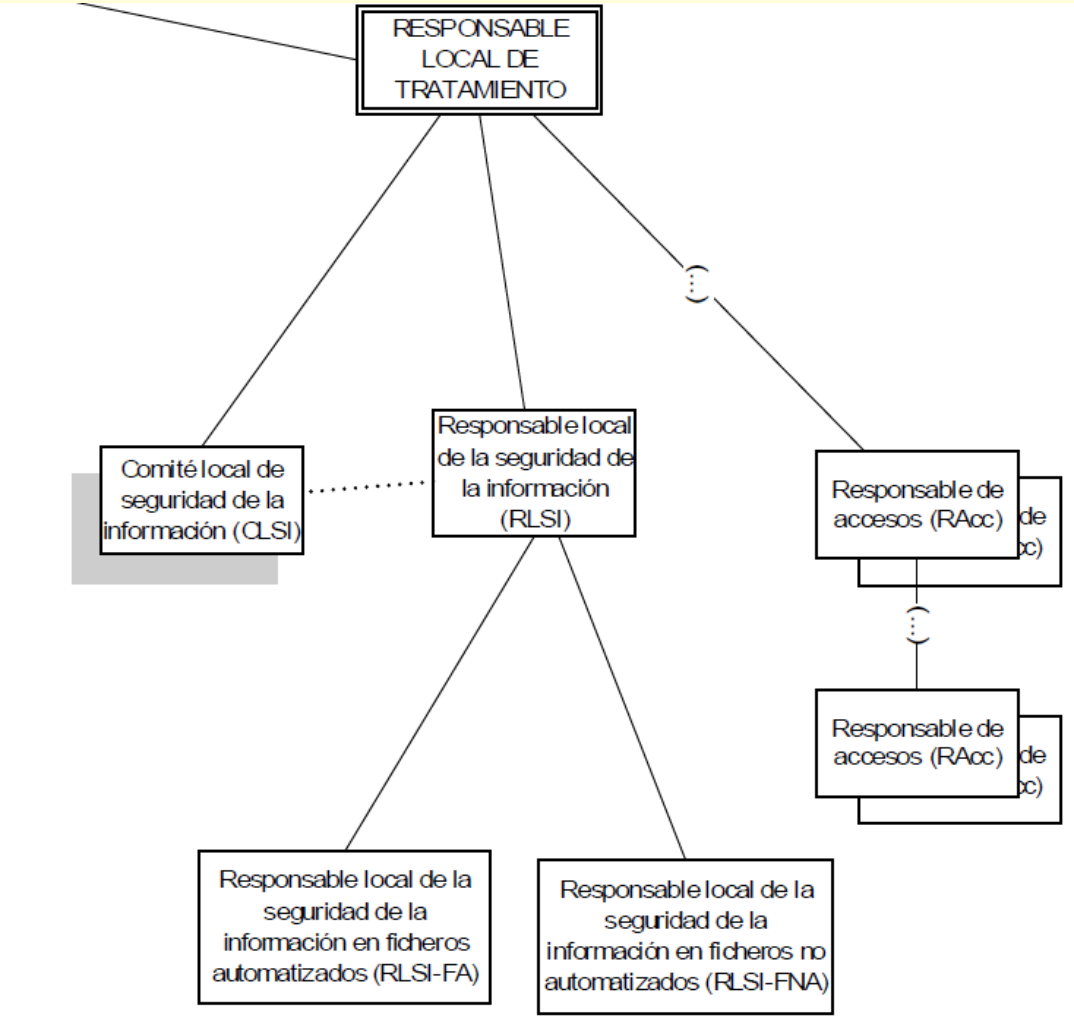
- **definición de políticas de actuación claras** (*políticas de seguridad*) **y**
- **la concienciación en seguridad informática.**

Organización de la seguridad

Impulsada por la USO bajo la Subdir. de SI

- Propuesta de orden sobre Organización de la Seguridad en la AVS
  - Organización jerárquica, roles y funciones
- Empuje a la implantación de la LOPD
  - documentos de seguridad en aplicaciones.
  - auditorias externas de seguridad (realizado)
  - Implantación de procedimientos
  - Información y sensibilización

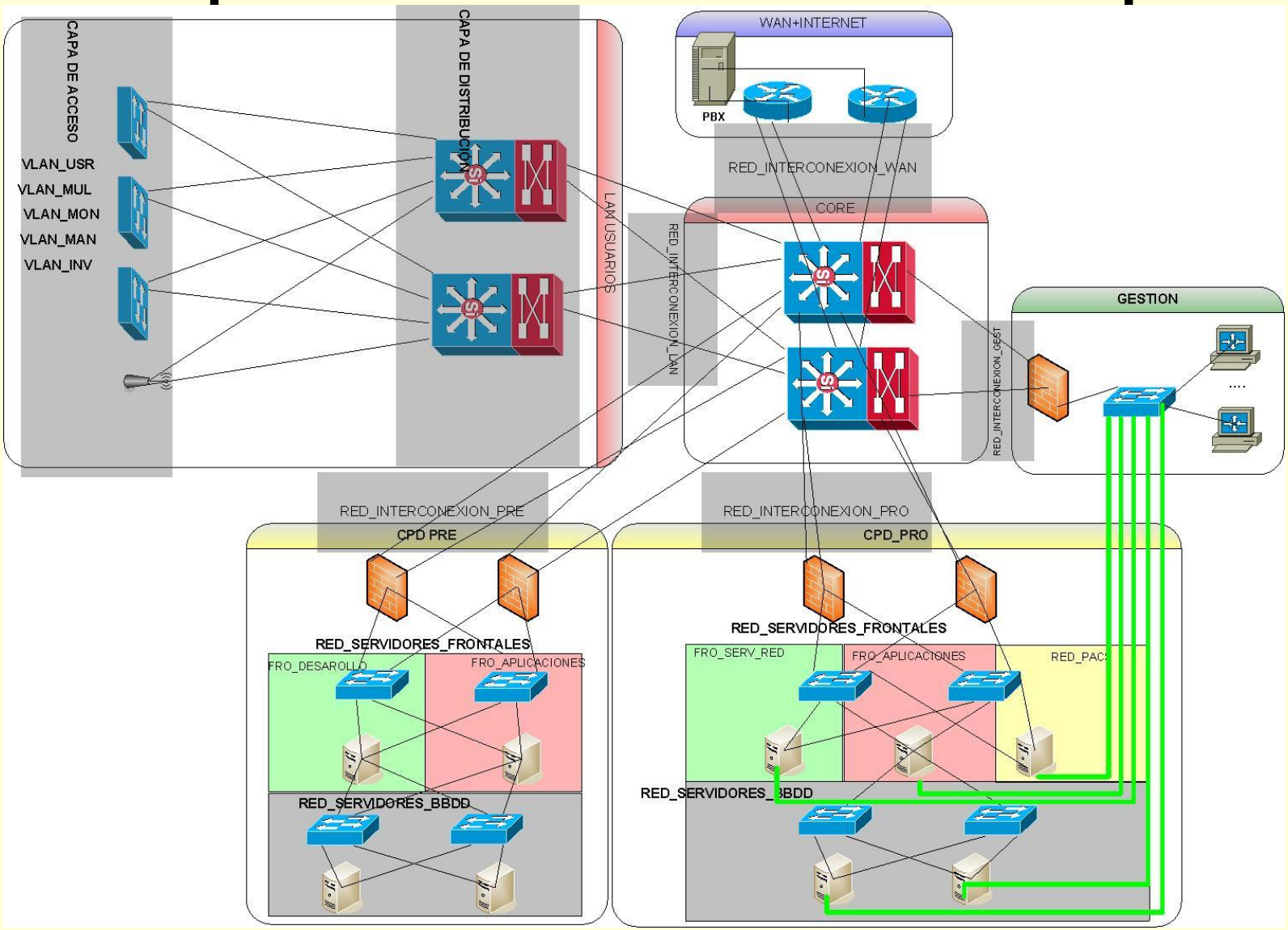
Organización de la seguridad



Modelo de red de hospital

- Red Arterias
- Proyecto de mejora de la red
  - Implantación de medidas técnicas de seguridad en dispositivos de red
  - Ampliación de protección perimetral por bloques (firewalls internos)
  - Mejora de tráficos legítimos de red
  - Protección de elementos sensibles (servidores de datos y aplicaciones)

Bloques de red de un hospital



Gestión del puesto de trabajo.

Es el responsable de todo lo relacionado con los puestos de trabajo de los profesionales, y también de las medidas de seguridad como la protección Antivirus.

Amenazas

New malware detections by country

1		United States	26%	3 Estados Unidos	315.791.000	4,49
2		South Korea	9%	26 Corea del Sur	48.588.000	0,69
3		China	7%	1 China	1.353.601.000	19,26
4		Great Britain	5%	23 Reino Unido	62.798.000	0,89
5		Germany	5%	16 Alemania	81.991.000	1,17
6		Brazil	4%	5 Brasil	198.361.000	2,82
7		India	3%	2 India	1.258.351.000	17,90
8		Spain	3%	28 España	46.772.000	0,67
9		France	2%	21 Francia	63.458.000	0,90
10		Mexico	1%	11 México	116.147.000	1,65

Amenazas (lógicas)

- BOTS y BOTNET
- PHISING
- MALWARE
- TROYANOS
- PHARMING
- CARDING
- DIALERS
- SPAM
- EXPLOITS
- ROOTKIT
- SQL INJECTION
- CROSS-SITE SCRIPTING
- LDAP INJECTION
- SPOOFING
- SNIFFING
- BUFFER OVERFLOWS
- HIJACKING
- CROSS-SITE REQUEST FORGERY (CSRF)

Antivirus Corporativo

Integra avanzadas tecnologías de:

- antivirus,
- cortafuegos y
- prevención de intrusos

para proteger el entorno de

- malware,
- infracciones de acceso,
- vulnerabilidades de desbordamiento del búfer y
- ataques mezclados.

Dispone de respuestas avanzadas para la gestión de brotes para reducir el daño y el coste de los mismos.

Modulos

- Protección de acceso
  - Proteje el equipo frente a cambios no deseados mediante reglas de protección de acceso.
- Protección de desbordamiento del búfer
  - Impide que las vulnerabilidades de desbordamiento del búfer ejecuten código arbitrario en el equipo.
- Directiva de programas no deseados
  - Impide que programas potencialmente no deseados, como software espía y software publicitario accedan al equipo.

Protección de acceso

- es la primera línea de defensa contra el malware
- compara las acciones solicitadas con una lista de reglas configuradas para bloquear y/o informar de infracciones de acceso.
- Los métodos más comunes: macros, ejecutables, correo, secuencias de comandos web, archivos de ayuda.

Protección de acceso - Ejemplos

Se definen mediante reglas de acceso como:

- Evitar la desactivación o el cambio en procesos críticos, como el propio antivirus.
- Evitar la falsificación de procesos de Windows.
- Evitar que los gusanos de envío masivo de correo envíen ningún correo.

Desbordamiento de buffer

- un intruso envía demasiados datos o códigos a un búfer de un programa y éste se desborda.
- Un defecto de diseño permite al intruso ejecutar código arbitrario con privilegios.

Programas no deseados

- Software desarrollado por compañías legítimas que puede alterar el estado de seguridad o la directiva de privacidad del equipo en el que se encuentra instalado.
- Este software puede incluir, aunque no necesariamente, software espía, software de publicidad y software de marcación.
- Estos programas se pueden descargar junto con un programa que el usuario desea obtener.

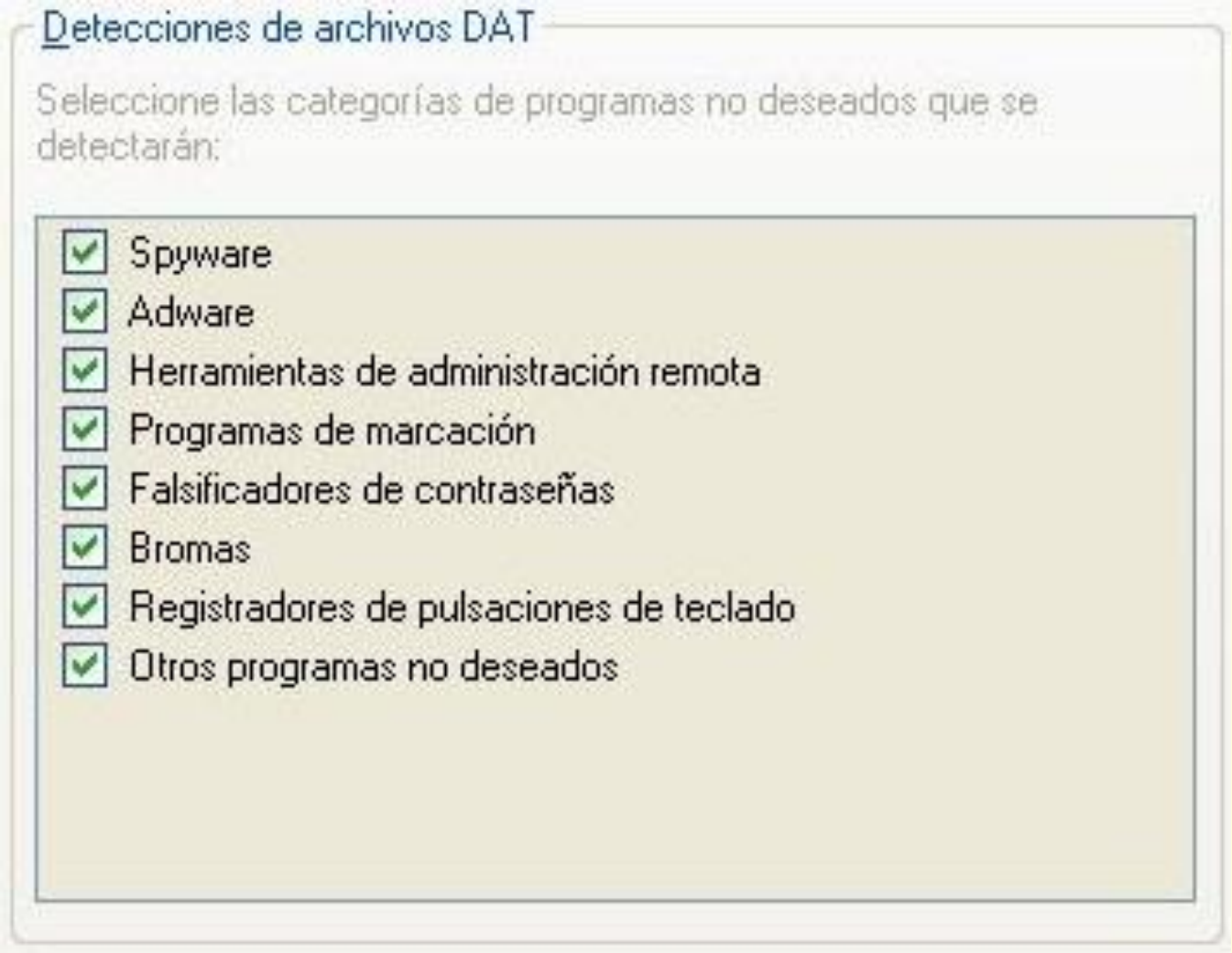
Anti Spyware

Módulo AntiSpyware amplia la capacidad de detectar y bloquear determinado software antes de que supongan una amenaza para el entorno de:

- Publicidad,
- Software espía y
- otros programas potencialmente no deseados

.

Categorias de programas no deseados



Antivirus (final)

- Estos elementos se configuran de modo general para cada puesto de trabajo de usuario final.
- Para cada servidor se particulariza su configuración con objeto de garantizar los servicios que ofrece.

Buenas practicas

Buenas practicas

- El primer antivirus es el sentido común.
- Cuidado con los desconocidos:
  - No abra nunca mensajes electrónicos o ficheros de origen desconocido.
  - No facilite nunca sus datos personales ni ningún tipo de códigos de acceso.

Buenas practicas

- No hay que responder a los mensajes que soliciten información confidencial aunque sea de forma urgente. El banco o las administraciones nunca le solicitarán por correo ningún dato personal.

Buenas practicas (corporativas)

- Tener instalado y actualizado algún software contra virus y espías y un firewall
- Mantenga actualizado con los diferentes parches o actualizaciones de seguridad tanto el sistema operativo de su equipo como su navegador de Internet y en general todos los programas, empezando por los de uso mas corriente.
- Haga copias de seguridad con frecuencia para evitar la pérdida de datos importantes.
- Usar una cuenta sin privilegios de administrador para las tareas cotidianas. Reservar la cuenta de administrador para instalaciones, actualizaciones o cambios de configuración.

Buenas practicas (corporativas)

- Tanto el acceso al ordenador como a las distintas aplicaciones corporativas será identificado (mediante usuario y contraseña, u otro mecanismo) y previamente autorizado por el responsable correspondiente.
- La custodia de la contraseña es responsabilidad del usuario. Nunca debe utilizarse la cuenta de usuario asignada a otra persona. Las contraseñas no deben anotarse sino que deben recordarse, y deben cambiarse periódicamente. Esto garantiza el uso privado de las mismas.

Buenas practicas (corporativas)

- No apunte sus contraseñas en ningún documento, ni las comparta con otros usuarios.
- No deben utilizarse contraseñas cortas o fáciles de deducir. No utilice las mismas contraseñas en Sistemas de Alta Seguridad que en Sistemas menos seguros.

Buenas practicas (corporativas)

- Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al responsable correspondiente
- Al abandonar el puesto de trabajo deben cerrarse las sesiones con las aplicaciones establecidas, y apagar los equipos al finalizar la jornada laboral.

Preguntas

Muchas Gracias