



TEMARIO

IFCT106PO

Protección de equipos en la red

TEMA 1. LA NECESIDAD DE PROTEGERSE EN LA RED

TEMA 2. LOS PELIGROS POSIBLES: LOS VIRUS INFORMÁTICOS

TEMA 3. LAS SOLUCIONES: EL ANTIVIRUS

TEMA 4. OTROS CONCEPTOS SOBRE SEGURIDAD INFORMÁTICA

TEMA 5. ACTUALIZACIONES DEL SOFTWARE

OBJETIVO GENERAL

- Prevenir los ataques de la red en equipos.



TEMA 1

La necesidad de protegerse en la red

- ▶ La necesidad de protegerse en la red
- ▶ Causas de la inseguridad
- ▶ Tipos de amenazas existentes
- ▶ Cómo protegernos

OBJETIVOS:

- Comprender las necesidades de protegerse en la red y aprender conceptos principales de seguridad.
- Reconocer cuáles son las consecuencias de la falta de seguridad y los problemas que se derivan.
- Aprender las causas de inseguridad de los equipos informáticos y del software.
- Identificar las amenazas existentes.
- Aprender a proteger los equipos de las amenazas y ataques.

INTRODUCCIÓN

Estamos en la era de la conectividad electrónica universal. De la presencia de virus, hackers, filtraciones de información, redes sociales a las que se sube información personal, nubes para guardar todos nuestros archivos, informatización de los procesos administrativos, de los negocios... que hace que sea un momento en el que la seguridad cobra mayor importancia, para proteger los datos, los recursos, garantizar la autenticidad de los datos y mensajes y proteger los sistemas de ataques en la red.

1. LA NECESIDAD DE PROTEGERSE EN LA RED

Cada vez estamos más rodeados de sistemas, es decir, de máquinas y programas interconectados me-

TOMA NOTA

Un ordenador se compone principalmente de dos elementos:

- El software es el conjunto de programas, instrucciones y reglas informáticas que hacen posible la realización de tareas específicas.
- El hardware es el conjunto de los componentes físicos de los que está hecho el equipo, es decir, la parte que puedes ver del ordenador, los componentes de su estructura física.

dianete redes donde se almacena información y que se transmite mediante estos sistemas. Un sistema está compuesto por varias máquinas controladas por componentes que se denominan software, que son lo que conocemos como programas de ordenador.

Los ordenadores, dispositivos de red, teléfonos, tabletas... forman redes interconectadas unas con otras que se comunican mediante otro sistema que es el hardware, que es gestionado por distintas aplicaciones bajo un protocolo de comunicaciones.

Uno de los problemas a la hora de aplicar la seguridad, es que muchas de las medidas que se emplean suponen una disminución del rendimiento de los equipos y aplicaciones, como es el caso de los sistemas criptográficos que consumen muchos recursos y el ancho de banda en las conexiones a internet, por lo que las organizaciones y empresas no dedican muchos recursos a este problema.

Hay que tener en cuenta que muchas veces estos problemas de seguridad no solo se producen por fallos en los equipos, sino también por un mal uso por parte del personal, es decir, por el factor humano. Por lo que es importante dedicar tiempo y recursos a la adecuada formación de los empleados, a la implicación de los responsables y directivos.

1.1 La seguridad: conceptos

Cuando hablamos de seguridad podemos referirnos a términos diferentes:

- Seguridad informática: es el conjunto de herramientas diseñadas con el fin de proteger los datos almacenados en un equipo.
- Seguridad de la información: consiste en proteger la información y los sistemas de información de un

acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados.

- Seguridad de la red: es el conjunto de herramientas diseñadas para proteger los datos durante su transmisión a través de una red de telecomunicación.
- Seguridad en internet: son las herramientas diseñadas para proteger los recursos de una red privada frente a usuarios de otras redes.

La diferencia entre estos términos se basa en el ámbito en el que se centran. Mientras que la seguridad de la información tiene que ver con la confidencialidad, integridad y disponibilidad de los datos, independientemente de su formato, la seguridad informática se orienta a garantizar la disponibilidad y el correcto funcionamiento de un sistema informático; por su parte, la seguridad en la red se centra en la protección de los datos durante su transmisión.

1.2 La red, Internet

La red Internet es un sistema compuesto por millones de ordenadores interconectados mediante una red física, muy compleja y que crece a gran velocidad. Cada ordenador contiene programas que interactúan entre sí y que a la vez interactúan con otros programas alojados en ordenadores de otra red, lo que hace que Internet tenga que ser capaz de procesar a la vez la información de millones de personas.

Las primeras investigaciones que se hicieron sobre la seguridad del software se basaban en establecer unas reglas de acceso a una cantidad elevada de usuarios que compartían un sistema, que consistía en establecer permisos que regulaban lo que hacían o los datos que veían. Las preguntas que se plantean a la hora de resolver este problema de seguridad son:

- ¿Cómo se puede mantener una base de datos en la que diferentes usuarios tienen diferentes privilegios de acceso?
- ¿Cómo se puede asegurar que las aplicaciones que se utilizan son correctas y que no han sido modificadas?
- ¿Se puede estar seguro de que los datos no han sido modificados?
- ¿Puede fácilmente una compañía hacer cumplir una determinada política de licencias para su software?

1.3 Consecuencias de la falta de seguridad

La ausencia o deficiencia de unas medidas de seguridad adecuadas puede causar daños graves como:

- Pérdida de tiempo en reparar y reconfigurar los equipos y programas.
- Imposibilidad de usar los recursos ya que las aplicaciones y servicios informáticos no están disponibles.
- Robos de información confidencial y posible revelación de estos datos a terceras personas no autorizadas.
- Filtración de datos personales de usuarios registrados en el sistema como empleados, clientes, proveedores, contactos, violando la legislación de protección de datos personales de la Unión Europea.
- Impacto en la imagen de la empresa, pérdida de credibilidad, daño a la reputación, pérdida de la confianza por parte de los clientes, proveedores...
- Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del servicio, pérdida de oportunidades de negocio...
- Pago de indemnizaciones por daños y perjuicios a terceros, teniendo que afrontar responsabilidades legales.

