4 Seguridad informática

El peligro de los ciberataques

El crecimiento exponencial del uso de las nuevas tecnologías en nuestra sociedad y la dependencia de los sistemas informáticos para la realización de actividades cotidianas son algunos de los aspectos que explican la importancia que la seguridad de la información ha adquirido en la actualidad.

Constantemente, se producen, en todo el mundo, millones de ciberataques cuyo objetivo es la intrusión en dispositivos con el fin de controlarlos de forma remota, obtener información de los mismos o, simplemente, dañarlos. Acciones tan simples como abrir un documento o responder a un correo electrónico pueden ser suficientes para que un virus infecte un equipo sin que el usuario sea consciente del grave peligro al que, por ello, ha quedado expuesto.

Teniendo esto en cuenta, la seguridad en los sistemas de información se considera una prioridad tanto para el entorno empresarial como para el personal, por lo que es necesario contar con medios y técnicas adecuados para preservar la protección de los sistemas.

Cuestiones sobre la lectura

1. Gran parte de las amenazas a las que un usuario está expuesto en Internet se producen por no respetar una serie de normas básicas de seguridad. ¿Qué tipo de amenazas relativas a la seguridad informática conoces?
2. La mayoría de usuarios tiene algún antivirus instalado en su equipo. ¿Qué otras herramientas de seguridad informática existen? ¿Las utilizas?
3. La seguridad informática no solo trata de prevenir incidentes, sino, también, de ofrecer soluciones cuando estos ocurren. En caso de que tu teléfono inteligente o tu ordenador personal dejara de funcionar como consecuencia de un ciberataque, ¿qué medidas adoptarías para recuperar la información alojada en el mismo?

1 La seguridad de la información

El término «seguridad» remite a la ausencia de peligro, daño o riesgo. Se considera que un sistema informático es seguro cuando es infalible, es decir, cuando funciona tal como se espera que lo haga.

Por otro lado, se denomina «información» al conjunto organizado de datos que constituye un mensaje. Este conjunto organizado de datos se trata digitalmente para ser procesado por dispositivos electrónicos, para ser almacenado en soportes informáticos o para ser transmitido a través de las redes de comunicación.

Así, si se unen ambos conceptos, la «seguridad de la información» se puede definir como el conjunto de medidas de prevención, detección y corrección orientadas a proteger la confidencialidad, la integridad y la disponibilidad de la información de un sistema.

1.1. Principios de la seguridad informática

Un sistema seguro es aquel conjunto de componentes de hardware y de software que mantiene un «nivel aceptable» de protección del usuario y de la información del mismo. Dicho nivel se alcanza al realizar ciertas acciones sobre dicho sistema que aseguren los siguientes principios básicos de seguridad:

- **Confidencialidad de la información.** Necesidad de que la información solo sea conocida por las personas autorizadas. La pérdida de confidencialidad puede revelar secretos empresariales, comprometer la seguridad de organismos públicos, atentar contra el derecho a la privacidad de las personas, etc. Por ejemplo, al realizar una transacción monetaria con una tarjeta de débito por Internet, los sistemas tratan de cifrar la información para que esta no pueda ser leída por otros usuarios.
- **Integridad de la información.** Característica que posibilita que el contenido permanezca inalterado (a menos que sea modificado por usuarios autorizados). La pérdida de integridad puede desembocar en fraudes, fomentar errores o dar lugar a otros ciberataques. Por ejemplo, se dice que se viola la integridad de la información de un sistema cuando un usuario que no debería tener acceso a cierta información modifica o borra datos.
- **Disponibilidad de la información.** Capacidad de permanecer accesible en el lugar, en el momento y en la forma en qué los usuarios autorizados lo requieran. El sistema, tanto el hardware como el software, debe mantenerse en funcionamiento de manera eficiente y ser capaz de restablecerse rápidamente en caso de que se produzcan errores. Este principio es fundamental en sistemas críticos cuyo fallo puede ocasionar pérdidas económicas significativas, daños físicos o, en el peor de los casos, amenazas para la vida humana. Por ejemplo, el ataque a una compañía aérea podría paralizar los vuelos o poner en riesgo la seguridad de los viajeros.

Como conclusión, la seguridad informática se define como el conjunto de procedimientos, estrategias y herramientas que permiten garantizar la confidencialidad, la integridad y la disponibilidad de la información.

1.2. Pero ¿qué hay que proteger?

El objetivo de la seguridad informática es proteger los recursos valiosos de una organización, tales como la información, el hardware o el software. Para ello, se establecen planes de seguridad que ayudan a identificar las vulnerabilidades e implantar los planes de contingencias adecuados.

Fig. 1. Aspectos clave de la seguridad informática.

Actividades

1. Para garantizar la confidencialidad de un sistema, es necesario disponer de mecanismos de autentificación, autorización, cifrado y no repudio. Investiga y explica en qué consiste cada uno de ellos.
2. ¿Qué es una «vulnerabilidad informática»? ¿Afecta al hardware, al software, a los datos o a los usuarios?

2 Amenazas a la seguridad

Las amenazas a la seguridad de un sistema informático son todos aquellos elementos o acciones capaces de atentar contra la seguridad de la información.

2.1. Tipos de amenazas

Las amenazas a la seguridad más importantes se pueden clasificar en humanas, lógicas y físicas.

Amenazas humanas

La mayoría de las acciones contra los sistemas informáticos provienen de personas que, de manera accidental o intencionada, pueden causar enormes pérdidas. Estas acciones se clasifican en dos grandes grupos:

- **Ataques pasivos.** Su finalidad es obtener información sin alterarla. Son muy difíciles de detectar, ya que, al no modificar los datos, no dejan muchos rastros. Algunos de los más habituales suelen ser los siguientes:
  - **Usuarios con conocimientos básicos.** Acceden a los sistemas de información accidentalmente o utilizando técnicas muy sencillas. Por ejemplo, un empleado que lee el correo de su compañero porque se ha dejado la sesión iniciada.
  - ***Hackers.*** Informáticos expertos que emplean sus conocimientos para comprobar las vulnerabilidades de un sistema y corregirlas. Las razones pueden ser laborales o, simplemente, por desafíos personales. En la mayoría de casos, no causan daños.
- **Ataques activos.** Persiguen dañar el objetivo o manipular la información para obtener beneficios, por ejemplo:
  - **Antiguos empleados de una organización.** Aprovechan las debilidades que conocen del sistema para atacarlo, ya sea por venganza o por otras razones.
  - ***Crackers* y otros atacantes.** Expertos informáticos que burlan los sistemas de seguridad, accediendo a ellos para obtener información, perjudicar un sistema informático o realizar cualquier otra actividad ilícita. En algunos casos, lo hacen simplemente con el objetivo de causar daños.

Fig. 2. Mapa de ataques informáticos en tiempo real (http://map.norsecorp.com).

Amenazas lógicas

El software que puede dañar un sistema informático es, generalmente, de dos tipos:

- **Software malicioso.** Programas, diseñados con fines no éticos, entre los que se encuentran los virus, los gusanos, los troyanos y los espías, los cuales atacan los equipos comprometiendo su confidencialidad, su integridad y su disponibilidad.
- **Vulnerabilidades del software.** Cualquier error de programación en el diseño, la configuración o el funcionamiento del sistema operativo o de las aplicaciones puede poner en peligro la seguridad del sistema si es descubierto por un atacante o provoca un fallo.

Amenazas físicas

Las amenazas físicas están originadas habitualmente por tres motivos:

- **Fallos en los dispositivos.** Las averías de discos, roturas en el cableado, sobrecargas eléctricas, apagones, etc., pueden provocar la caída de un sistema informático.
- **Accidentes.** Sucesos provocados de forma involuntaria por descuidos, malas prácticas o desconocimiento (por ejemplo, que un líquido se vierta sobre el equipo).
- **Catástrofes naturales.** Desastres como incendios, inundaciones o terremotos.

2.2. Conductas de seguridad

Las conductas de seguridad que se emplean en el uso de sistemas informáticos pueden ser de dos tipos: activas y pasivas.

- **Seguridad activa.** Conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos. Algunas de las principales medidas de seguridad activa son las siguientes:
  - **Control de acceso.** Limita el acceso únicamente al personal autorizado. Para ello, se utilizan contraseñas seguras, listas de control, certificados digitales, técnicas biométricas, etc.
  - **Encriptación.** Codifica la información importante para que, en caso de ser interceptada, no pueda descifrarse.
  - **Software de seguridad informática.** Previene del software malicioso y de ataques de intrusos al sistema informático. Para ello, se suelen utilizar antivirus, antiespías, cortafuegos, etc.
  - **Firmas y certificados digitales.** Permiten comprobar la procedencia, autenticidad e integridad de los mensajes.
  - **Protocolos seguros.** Protegen las comunicaciones, por medio del cifrado de la información, para garantizar su seguridad y confidencialidad.
- **Seguridad pasiva.** Conjunto de medidas que reparan o minimizan los daños causados en sistemas informáticos. Las prácticas de seguridad pasiva más recomendables son estas:
  - **Herramientas de limpieza.** En caso de infección, hay que realizar un escaneado completo del equipo y utilizar herramientas específicas para eliminar el *malware*. Una de las causas de infección puede tener que ver con el hecho de que el software de seguridad no funcione correctamente o, incluso, que pueda estar infectado, por lo que es recomendable iniciar el equipo con un disco de arranque libre de virus o analizarlo con un antivirus online.
  - **Copias de seguridad.** Restauran los datos utilizando copias de los datos originales que se realizan periódicamente. Emplean soportes de almacenamiento externos al equipo o en la nube, para que, en caso de fallo del equipo, estén disponibles.
  - **Sistemas de alimentación ininterrumpida (SAI).** Dispositivos que incorporan una batería para proporcionar corriente al equipo con el fin de que siga funcionando en caso de fallo eléctrico.
  - **Dispositivos NAS.** Permiten, como sistemas de almacenamiento a los que se tiene acceso a través de la red, que cualquier equipo autorizado pueda almacenar y recuperar la información.
  - **Sistemas redundantes.** Duplican componentes críticos, como los procesadores, los discos duros (RAID) o las fuentes de alimentación, para seguir funcionando aunque se produzca el fallo de un componente.

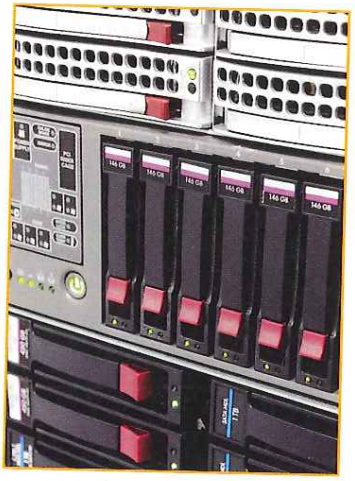


Fig. 3. Un sistema RAID es un conjunto de varios discos en los que se graba la información de manera simultánea. Las implementaciones más comunes son RAID 1, RAID 5 y RAID 10. Se utilizan en sistemas críticos de seguridad como, por ejemplo, los servidores.

Actividades

1 *Un informático en el lado del mal* es el blog del *hacker* español Chema Alonso. Lee algunas de sus publicaciones para obtener información sobre él y sobre las actividades que realiza.

2 Investiga la diferencia entre los diferentes niveles RAID y explica cómo se recupera la información en un sistema RAID 5 con cuatro discos cuando falla uno de ellos.

3 Malware

Malware, del inglés, es el acrónimo de «*malicious*» y «software», por lo que, en español, se traduce como 'programa malicioso'. Su peligrosidad se establece sobre la base de dos criterios principales: por un lado, su capacidad de hacer daño a un equipo y, por otro, su posibilidad de propagación. Los ciberataques suelen combinar varios tipos de *malware*.

3.1. Tipos de *malware*

Desde la aparición de los virus informáticos, a comienzos de la década de los ochenta, los códigos maliciosos han evolucionado mucho, por lo que su clasificación es cada vez más amplia. A continuación, se presentan los tipos de *malware* más conocidos:

- **Virus.** Un virus es un programa informático creado para producir daños en un equipo. Posee dos características particulares: actúa de forma transparente para el usuario y tiene la capacidad de reproducirse a sí mismo. La denominación genérica «virus» se utiliza para aludir a los programas que infectan archivos ejecutables; «virus *boot*», para los que atacan el sector de arranque de un equipo; «virus *script*», para los escritos en lenguajes de *scripting*, y «virus macro», para los que se incrustan en documentos que contienen macros.
- **Gusano.** Programa independiente que tiene por objetivo multiplicarse y propagarse de forma autónoma, infectando, valiéndose de las vulnerabilidades de los sistemas, los equipos. Los medios de infección habitual suelen ser la mensajería instantánea, el correo electrónico y la copia por memorias USB. Su capacidad de propagarse por las redes posibilita que puedan expandirse por todo el mundo en cuestión de pocos minutos.
- **Troyano.** Código malicioso que se oculta dentro un archivo inofensivo y útil para el usuario. Al igual que los gusanos, no infectan archivos, aunque, a diferencia de estos, requieren la intervención de sus víctimas para propagarse. Existe una gran variedad de troyanos, en función de sus acciones y utilidades: Downloader (descarga otros códigos maliciosos), Clicker (busca beneficio económico a través de clics en publicidad), Keylogger (registra las actividades que se realizan en el sistema), Backdoor (abre puertos en el sistema), Bot (controla el equipo de forma remota), etc.
- ***Spyware.*** Programa espía que almacena información personal (como los datos personales, las búsquedas realizadas, el historial de navegación, la ubicación, las descargas...) del usuario sin su consentimiento. En la mayoría de casos, la información obtenida es facilitada a empresas de publicidad para el envío de *spam* o correo basura.
- ***Adware.*** Programa malicioso que se instala en el sistema, aprovechando que el usuario acepta sus términos de uso, al instalar otras aplicaciones. Suele utilizar información recopilada por algún *spyware* para mostrar publicidad personalizada para el usuario.
- ***Ransomware.*** Aplicación que secuestra un dispositivo, por medio de la codificación o del bloqueo al acceso a la información, mostrando un mensaje a la víctima en el que se solicita el pago para liberarlo.
- ***Rogue.*** Programa malicioso que simula ser *antimalware* pero que ocasiona los efectos contrarios. Muestra en la pantalla advertencias de falsas infecciones, tratando de engañar al usuario para que pague por la supuesta desinfección.
- ***Rootkit.*** Software con permiso de administrador *(root)* que se oculta entre las herramientas *(kit)* del sistema operativo para proporcionar acceso remoto al atacante. Suspende su actividad al detectar escaneo, por lo que puede pasar desapercibido durante mucho tiempo.

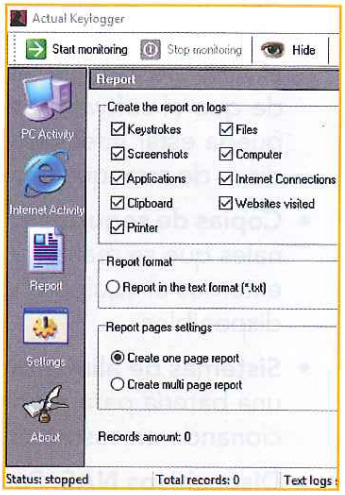


Fig. 4. Opciones de un Keylogger. Keylogger es un tipo de troyano que graba todo lo que el usuario escribe a través del teclado para enviarlo al atacante o almacenarlo a la espera de ser recuperado. Incluye opciones como la captura de pantalla, el historial de páginas web visitadas, los ficheros abiertos, etc.

3.2. Otras amenazas *malware*

Además del *malware*, existen otras amenazas:

- ***Phishing.*** Técnica para obtener información de un usuario de forma fraudulenta. El atacante se hace pasar por una persona o por una empresa de confianza, a través de un correo electrónico, de un mensaje instantáneo o de una red social, para enviar un enlace a una página web maliciosa con el fin de obtener sus credenciales, cuentas bancarias, números de tarjetas de crédito, etc.
- ***Pharming.*** Técnica que aprovecha la vulnerabilidad de los servidores DNS para redireccionar la dirección web de un sitio de confianza a otro fraudulento con la intención de robar datos personales y claves para cometer fraudes económicos.
- ***Spam.*** Mensajes de correo electrónico «no deseado» o «basura» enviados masivamente, ya sea con fines publicitarios o para la propagación de códigos maliciosos. Algunos estudios afirman que más del 80% de correo es *spam*, por lo que, además de ser molestos, consumen recursos innecesariamente (ancho de banda, almacenamiento,...).
- ***Hoax.*** Mensajes de correo, distribuidos en formato de cadena, cuyo objetivo es realizar engaños masivos. Algunos ejemplos característicos de *hoax* son las alertas falsas sobre virus, las historias solidarias inventadas y los mensajes que afirman traer mala suerte si no se reenvían.

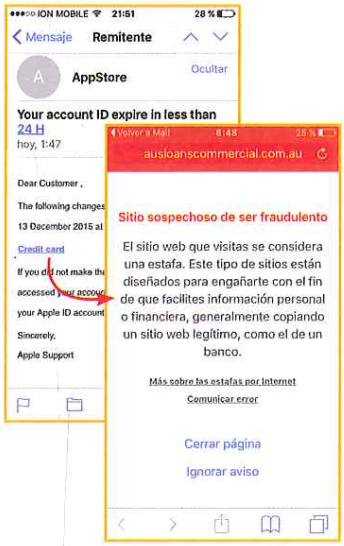


Fig. 5. Detección de *phishing*.

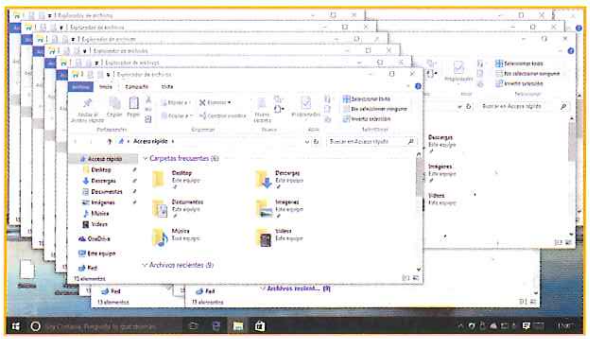
Actividades

1 Las siguientes aplicaciones son inofensivas, aunque ilustran lo indefenso que puede ser cualquier usuario al abrir un archivo desconocido, incluso aunque no se detecte ninguna amenaza al analizarlo con un antivirus.

a) Escribe el siguiente código en un editor de textos y guárdalo con el nombre **Virus.bat**:

```
@echo off
:inicio
start explorer.exe
goto inicio
```

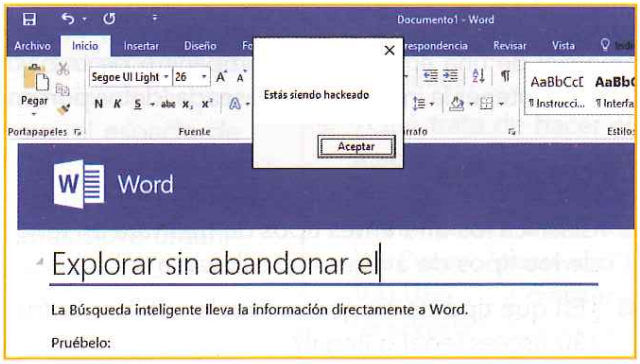
Al ejecutarlo, se abrirá el programa lanzado (explorer.exe) constantemente hasta agotar los recursos del equipo y dejarlo bloqueado:



b) Escribe el siguiente código en un editor de textos y guárdalo con el nombre **Virus.vbs**:

```
MsgBox "Estás siendo hackeado"
Set wshShell =
wscript.CreateObject("WScript.Shell") do
   wscript.sleep 600
   wshshell.sendkeys "{bs}"
loop
```

Al ejecutarlo, se activa la tecla de retroceso cada 600 milisegundos por lo que, en función de la ubicación del cursor, tendrá distintos efectos, como, por ejemplo, el de borrar el texto anterior:



4 Ataques a los sistemas informáticos

Tradicionalmente, la mayoría de ataques a sistemas informáticos se han dirigido al sistema operativo Windows, aunque, en la actualidad, se han extendido por todas las plataformas, con una tendencia creciente de ataques a dispositivos móviles. Todos ellos comparten un nexo común: las redes de comunicaciones y, en concreto, Internet.

4.1. Tipos de ataques

Los principales ataques a los que están expuestos los sistemas informáticos se dividen en los siguientes grupos:

- **Interrupción.** Ataque contra la disponibilidad de un sistema. El resultado de estos ataques es que un recurso sea destruido, quede inutilizable o no disponible. Estos ataques se llevan a cabo, por ejemplo, al destruir un disco duro, al cortar el cable de una red o al deshabilitar el sistema de gestión de archivos.
- **Interceptación.** Ataque contra la confidencialidad de un sistema a través del que un programa, proceso o usuario consigue acceder a recursos para los que no tiene autorización. Es el incidente de seguridad más difícil de detectar, ya que, por lo general, no produce una alteración en el sistema. Algunos ejemplos característicos de este tipo de ataque son el acceso a una base de datos o el acceso remoto al equipo de otra persona.
- **Modificación.** Ataque contra la integridad de un sistema a través del cual, además de acceder a un recurso, se manipula. Estos ataques suelen ser los más dañinos, ya que pueden eliminar parte de la información, dejar algunos dispositivos inutilizables, crear inconsistencias e introducir errores, alterar los programas para que funcionen de forma distinta, etc.
- **Suplantación o fabricación.** Ataque contra la autenticidad mediante el cual un atacante inserta objetos falsificados en el sistema. Con esto, se puede realizar una suplantación de identidad, de una dirección IP, de una dirección web, de un correo electrónico, etc.

4.2. Ingeniería social

La ingeniería social es una técnica ampliamente utilizada que no explota las vulnerabilidades a nivel tecnológico de un sistema, sino ciertos comportamientos y conductas de los seres humanos. Por lo general, estas técnicas de ataque buscan canalizar la atención de los usuarios aprovechando aspectos de su personalidad (curiosidad, deseos...) para que realicen actos involuntarios sin sospechar que están colaborando con el atacante para que logre sus objetivos.

Esta técnica se utiliza para conseguir información, privilegios o acceso a sistemas. En la práctica, se utilizan, principalmente, el teléfono e Internet para engañar a los usuarios por medio de la simulación, por ejemplo, de ser un empleado de un banco, el comercial de una empresa, un compañero de trabajo, un técnico o un cliente, con el fin de obtener la información deseada (datos personales, números de cuenta, etc.).

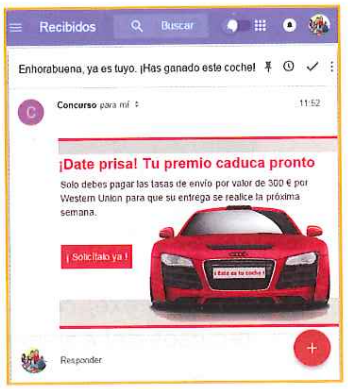


Fig. 6. Ejemplo de fraude realizado a través de *e-mail*.

Actividades

1. Clasifica los diferentes tipos de *malware* en función de los tipos de ataques que llevan a cabo.
2. ¿En qué tipo de ataques se suelen utilizar *botnets*? ¿Su uso es legal o ilegal?
3. Elabora una lista de las técnicas de ingeniería social que suelen utilizar los estafadores.
4. Averigua en qué consiste la ingeniería social inversa y proporciona algunos ejemplos.

4.3. Ataques remotos

Un ataque remoto es aquel que utiliza un conjunto de técnicas para acceder a un sistema informático a distancia. Por lo general, utiliza software malicioso que aprovecha las vulnerabilidades de seguridad en las aplicaciones, sistemas operativos y protocolos de red.

Algunos de los ataques que comprometen la seguridad de un sistema remoto son:

- **Inyección de código.** Añade o borra información en sitios remotos que no están bien protegidos. Por ejemplo, las bases de datos asociadas a los sitios web suelen utilizar instrucciones del lenguaje SQL para seleccionar datos (SELECT), insertarlos (INSERT), borrar tablas (DROP), etc., separadas por «;». Si el programador no filtra la entrada de datos correctamente, el atacante podría lanzar la comprobación de una contraseña al azar para, en la misma instrucción, borrar una tabla.

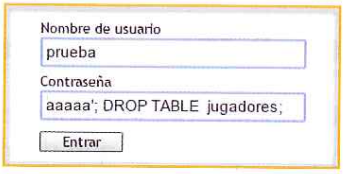


Fig. 8. Ejemplo de ataque por inyección SQL.

- **Escaneo de puertos.** Averigua qué puertos de un equipo en la red se encuentran abiertos para determinar los servicios que utiliza y, posteriormente, lanzar el ataque.
- **Denegación de servicio (DoS).** Satura los recursos de un equipo o de una red para que deje de responder o lo haga con tal lentitud que se considere no disponible. Los objetivos habituales de este tipo de ataques son servidores web. Cuando el ataque se lanza desde varios puntos de conexión, se denomina «DDoS».
- **Escuchas de red.** Captura e interpreta el tráfico de una red, aplicando distintos tipos de filtros. Los atacantes utilizan programas *sniffer* para interceptar toda la información que pasa por la red espiada, ya sea pinchando un cable con un *switch* o utilizando antenas. Una vez capturada, se utilizan analizadores para recolectar datos sin cifrar que han sido enviados a través de protocolos no seguros, como HTTP (web), SMTP (envío de *e-mail*), POP3 (recepción de *e-mail*), Telnet (acceso remoto), FTP (archivos), etc.
- ***Spoofing.*** Suplanta la identidad de un usuario, red, equipo o aplicación, falsificando su dirección de IP, DNS, URL, *e-mail*, GPS, ARP, etc. Por medio de esta técnica, el atacante adquiere privilegios para acceder a redes autentificadas por MAC, para hacerse pasar por otras personas, etc.

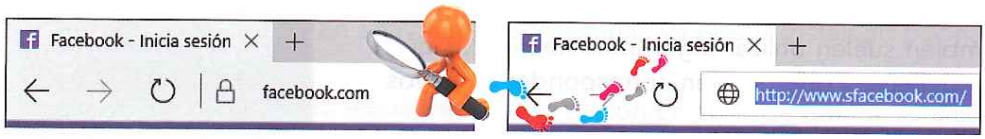


Fig. 7. Ejemplo de ataque DNS *spoofing*, a través del cual el usuario es redireccionado a una web falsa.

- **Fuerza bruta.** Vulnera mecanismos de autenticación basados en credenciales del tipo usuario y contraseña. Se basa en probar todas las combinaciones posibles del espacio de claves de un sistema. Pero, a medida que el espacio de claves y su longitud crecen, la capacidad de cálculo actual se vuelve insuficiente para probar todas las claves en tiempos razonables. Por esta razón, se combina la fuerza bruta con el uso de diccionarios que contienen palabras clave organizadas por medio de algún criterio en particular (datos de la empresa, lugares, familiares, claves populares, etc.).
- **Elevación de privilegios.** Aumenta los permisos del atacante a administrador o *root* para obtener un acceso total al sistema.

Actividades

1. Investiga qué comando puedes utilizar para averiguar cuáles son los puertos abiertos de tu equipo.
2. Busca una web que te permita realizar un diagnóstico visual de tu red con Traceroute.
3. ¿Para qué sirve el protocolo WHOIS? Utilízalo con alguno de tus dominios.
4. ¿Qué trata de hacer el atacante web al probar esta contraseña: **noclaves'; INSERT INTO tabla ('user', 'password') VALUES ('cracker', 'cracker');**? ¿Cómo podrías evitarlo?

5 Protección contra el *malware*

El uso de Internet, el correo electrónico, las aplicaciones, los dispositivos y los soportes de almacenamiento constituye una de las bases de la actual sociedad del conocimiento. Sin embargo, a su vez, estas herramientas son las principales fuentes de infección de *malware*. Para mantener la información y los dispositivos protegidos, es necesario utilizar diversas herramientas de seguridad (antivirus, cortafuegos, *antispam*, etc.), así como adoptar políticas de seguridad para gestionar contraseñas, cifrar la información, etc.

5.1. Políticas de seguridad

La política de seguridad de un sistema informático es el conjunto de normas y procedimientos que definen las diferentes formas de actuación recomendadas, con el fin de garantizar un cierto grado de seguridad.

Es imposible hablar de sistemas cien por cien seguros porque, entre otros aspectos, el coste de la seguridad total es muy alto. Por esta razón, muchas empresas, además de utilizar herramientas de seguridad, crean planes de acción en sus políticas de seguridad, con el propósito de concienciar a cada uno de los miembros de la organización sobre la importancia y la sensibilidad de la información, ya que una de las piezas clave para preservar la seguridad de una empresa son las actuaciones de sus empleados.

Además de las políticas de seguridad propias, la legislación establece medidas de carácter legal de obligado cumplimiento, como la LSSICE, la LOPD, la ley de *cookies*, etc.

5.2. Soluciones antivirus

Un antivirus es un software que tiene como finalidad prevenir, detectar y eliminar virus, software malicioso y otros ataques en el sistema. Reside en la memoria, analizando constantemente los archivos ejecutados, los correos entrantes, las páginas visitadas, las memorias USB introducidas, etc.

En caso de amenaza, los antivirus muestran un mensaje al usuario con las posibles acciones que puede llevar a cabo: omitir el aviso, desinfectar el archivo, moverlo a la cuarentena o eliminarlo. Para detectar un software malicioso, estos programas utilizan una base de datos de firmas o definiciones de virus con la que comparan el código de los archivos. También suelen utilizar algoritmos heurísticos que advierten de comportamientos sospechosos que pueden corresponder a nuevos virus no reconocidos.

Los antivirus actualizan constantemente sus definiciones de virus incluyendo nuevas amenazas que van apareciendo; por esta razón, es imprescindible que estén instalados en equipos con conexión a Internet.

Algunos de los antivirus más populares son Avast, Avira, Bitdefender, ESET, GData, Kaspersky, McAfee y Norton. Sus desarrolladores también ofrecen *suites* de seguridad que, además del antivirus, incluyen prestaciones adicionales, como cortafuegos, control parental, *antispam*, protección de pagos, cifrado de datos de entrada, monitor de red, etc. Un ejemplo de este tipo de desarrolladores es Kaspersky Internet Security.

Otra opción interesante (especialmente, en caso de infección) es utilizar antivirus en línea gratuitos, que permiten analizar el ordenador con la garantía de no estar infectados y, por tanto, que ofrecen gran fiabilidad en sus resultados.

Fig. 9. Análisis con el antivirus gratuito AVG.

5.3. Síntomas de una infección

La mayoría de las infecciones son detectadas por las herramientas de seguridad; no obstante, existe una serie de indicadores que los usuarios deben tener en cuenta para estar alerta y recurrir a las herramientas adecuadas.

Algunos de los principales síntomas de una infección son los siguientes:

- Ralentización del equipo durante el arranque, el funcionamiento o la conexión a Internet.
- Desaparición de carpetas o archivos, o distorsión de sus contenidos.
- Aparición de publicidad, mensajes de error o sonidos no habituales.
- Movimiento automático del ratón, de los menús o de las ventanas.
- Fallos o comportamientos extraños en las aplicaciones y los dispositivos.
- Intentos de conexión a Internet inesperados o redireccionamientos no deseados.
- Secuestro de la página de inicio del navegador y cambio del buscador predeterminado.
- Aparición de barras de herramientas extrañas en el navegador web.
- Envío de correos electrónicos o de mensajes a los contactos de una lista.
- Aumento de la actividad en el equipo y del tráfico en la red.

5.4. Pasos que se deben seguir en caso de infección

Cuando se ha detectado una infección o hay una sospecha razonable de que pueda haberla, es posible adoptar las siguientes medidas:

- **Restaurar el sistema a un estado anterior.** Algunos sistemas operativos, como Windows, crean puntos de restauración periódicamente permitiendo devolver al equipo a un estado seguro anterior sin que se pierda información.
- **Actualizar la base de datos del antivirus y realizar un análisis completo del equipo.** En caso de que no se detecte o elimine el *malware*, se puede optar por utilizar aplicaciones de otros fabricantes o por realizar un análisis en línea.
- **Arrancar el equipo con un Live CD o Live USB.** Esta opción permite:
  - Analizar el equipo con un antivirus sin contaminar, ya que el instalado podría estar infectado.
  - Extraer los archivos para recuperar la información en caso de que el sistema operativo del equipo haya sido dañado y no permita iniciar el sistema.
- **Ejecutar utilidades de desinfección específicas, que actúan como antídotos de virus o eliminan amenazas concretas.** Una vez conocida la amenaza, dichas utilidades se pueden descargar desde sitios web seguros, desarrolladores de antivirus, foros de seguridad, etc.

Cuando se tiene conocimiento de que el equipo ha sido atacado o está infectado, es muy importante no utilizar la red ni introducir ningún dato de carácter personal o confidencial hasta que el equipo esté completamente limpio.

En el peor de los casos, habrá que formatear el equipo y reinstalar el sistema operativo y las aplicaciones. Si se ha utilizado una política adecuada de copias de seguridad, el daño debería ser mínimo; en otro caso, la información del usuario o la empresa podría sufrir daños irreparables.

Actividades

1. Averigua qué antivirus son más efectivos basándote en comparativas de laboratorios como Virus Bulletin o AV-Comparatives.
2. ¿Para qué se utiliza la aplicación AdwCleaner?
3. El origen de la infección de la mayoría de teléfonos inteligentes suele deberse a la instalación de aplicaciones maliciosas. ¿De qué herramientas dispones si se infecta tu teléfono?
4. Sigue los ataques informáticos a tiempo real con el mapa interactivo de Kaspersky (https://cybermap.kaspersky.com) y propón herramientas para protegerte de las actuales amenazas.

6 Cifrado de la información

El cifrado de la información es un procedimiento, casi tan antiguo como la escritura, imprescindible para garantizar la confidencialidad e integridad de la misma, especialmente, cuando esta se envía a través de redes no seguras.

6.1. Orígenes

El uso de la criptografía se remonta al origen del lenguaje, cuando los primeros hombres tuvieron que desarrollar herramientas para asegurar la confidencialidad en determinadas comunicaciones.

Hacia el siglo v a. C., los griegos utilizaban un cilindro o bastón, denominado «skytálē», alrededor del cual se enrollaba una tira de cuero. Al escribir un mensaje sobre el cuero y desenrollarlo, se observaba una ristra de caracteres sin sentido. Así, para leer el mensaje, era necesario enrollar el cuero de nuevo en un cilindro del mismo diámetro.

Fig. 11. Skytálē.

Durante el Imperio romano, los ejércitos utilizaron el cifrado César, consistente en desplazar cada letra del alfabeto un número determinado de posiciones.

El primer libro europeo que describe el uso de la criptografía, *Epístola sobre las obras de arte secretas y la nulidad de la magia*, fue escrito en el siglo XIII por el monje franciscano Roger Bacon, quien describió siete métodos para mantener en secreto los mensajes.

Durante la Segunda Guerra Mundial, los alemanes utilizaron la máquina Enigma para cifrar y descifrar los mensajes. Alan Turing, en el bando de los aliados, fue uno de los artífices del descifre del primer mensaje y del cambio de rumbo de la guerra, de la historia y de la seguridad informática actual. Hoy en día, Turing es considerado uno de los padres de la informática.

Fig. 12. Máquina de cifrado Enigma.

No obstante, la era de la criptografía moderna comienza realmente con Claude Elwood Shannon, quien, con sus publicaciones sobre la teoría de la información y la comunicación, estableció las bases de la criptografía y el criptoanálisis modernos.

6.2. Criptografía

La criptología es la disciplina científica dedicada al estudio de la escritura secreta. Está compuesta por dos técnicas antagonistas: la criptografía y el criptoanálisis. Estos términos tienen sus orígenes en la Grecia clásica. Así, «criptografía» (del griego *criptos*, 'oculto', y *graphos*, 'escritura') se puede traducir como 'escritura oculta'.

Según la Real Academia Española, la criptografía es el «arte de escribir con clave secreta o de un modo enigmático». Para ello, se utilizan claves y procedimientos matemáticos para cifrar el texto, esto es, para transformarlo con el fin de que solo pueda ser leído por las personas que conozcan el algoritmo utilizado y la clave empleada.

El criptoanálisis estudia los sistemas criptográficos para encontrar sus debilidades y quebrantar la seguridad con el fin de descifrar textos sin conocer las claves.

Fig. 10. Esquema de cifrado de un mensaje en el que el emisor y el receptor se encuentran en ubicaciones distintas.

Criptografía de clave simétrica

La criptografía simétrica emplea la misma clave para cifrar y descifrar los mensajes. Es una técnica muy rápida pero insegura, ya que el remitente tiene que enviar tanto el mensaje cifrado como la clave, por lo que si un atacante consigue hacerse con ambos, podrá descifrar el mensaje.

Fig. 13. Carla escribe un mensaje a David cifrándolo con una clave. David lee el mensaje utilizando la clave que le ha comunicado Carla en otro envío.

Criptografía de clave asimétrica

La criptografía asimétrica utiliza dos claves, una pública y una privada. Cada usuario posee una clave pública que es conocida por todos los usuarios y otra privada que únicamente puede conocer su propietario. Cuando se cifra un mensaje con la clave pública de una persona, solo puede descifrarse utilizando la clave privada de dicha persona.

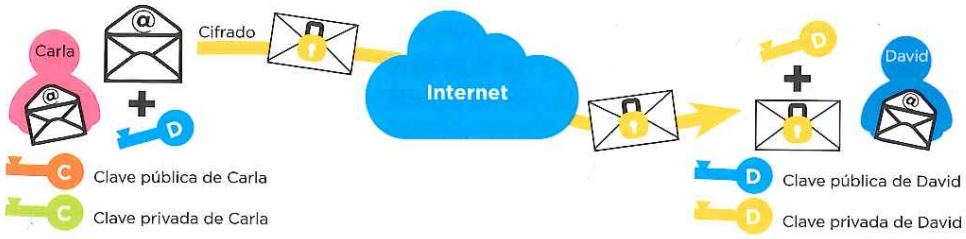


Fig. 14. Carla escribe un mensaje cifrándolo con la clave pública de David. David lee el mensaje con su clave privada, que únicamente él conoce.

Criptografía de clave pública

La criptografía simétrica no es completamente segura y la asimétrica, por su parte, ralentiza el proceso de cifrado. Para solventar estos inconvenientes, el proceso habitual pasa por utilizar un cifrado de clave pública que combine ambas criptografías con el objetivo de obtener una garantía plena de confidencialidad.

Fig. 15. Carla escribe un mensaje a David cifrándolo con una clave. Dicha clave, a su vez, la ha cifrado con la clave pública de David. David utiliza su clave privada para descifrar la clave con la que puede leer el mensaje.

El estándar X.509

En criptografía, X.509 es un estándar para infraestructuras de clave públicas. Se utiliza para emitir certificados con los que se autentifica a los usuarios.

Actividades

1. Codifica un mensaje, utilizando el cifrado César, aplicando un desplazamiento de entre tres y ocho caracteres. Intercámbialo con un compañero y averigua quién lo descifra con mayor rapidez.
2. Diseña los esquemas de cifrado que representan el proceso que sigue la respuesta de David a Carla utilizando la criptografía de las tres claves.
3. Envía un texto codificado en binario o en hexadecimal a uno de tus compañeros. ¿Qué tipo de criptografía estáis utilizando?
4. Averigua qué cifrado utiliza tu gestor de correo (Gmail, Hotmail, Yahoo!, etc.) para preservar la confidencialidad y la integridad de los mensajes intercambiados con tus contactos.

7 Firma electrónica y certificado digital

En la sociedad de la información, los usuarios pueden realizar gran parte de las tareas cotidianas por medio de las nuevas tecnologías. Para ello, es preciso contar con mecanismos que garanticen la autenticidad, la integridad y la confidencialidad de las comunicaciones entre ciudadanos, empresas y otras instituciones públicas a través de las redes abiertas de comunicación. Los principales mecanismos que lo permiten son la firma electrónica y el certificado digital.

7.1. La firma electrónica

La firma electrónica se define como el conjunto de datos asociados a un documento electrónico que permite realizar las siguientes acciones:

- **Identificar al firmante de forma inequívoca.** Requiere el uso de una clave privada que únicamente conoce el firmante.
- **Asegurar la integridad del documento firmado.** Proporciona mecanismos para comprobar que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración ni manipulación algunas.
- **No repudio.** Certifica que los datos utilizados por el firmante para realizar la firma son únicos y exclusivos, y, por lo tanto, no puede argüir *a posteriori* que no ha firmado el documento en cuestión.

Al firmar digitalmente un documento electrónico, se le confiere una validez jurídica equivalente a la que proporciona la firma manuscrita, con la ventaja de que este procedimiento no requiere la presencia física del firmante y, además, no se puede falsificar. Este documento debe conservarse, y cualquier impresión debe contener un código seguro de verificación (CSV) que permita contrastar la copia impresa con el original electrónico.

Normativa legal de la firma electrónica

La Ley 59/2003, de 19 de diciembre, de Firma Electrónica regula el uso de este sistema.

Firma de documentos electrónicos

El firmante genera, mediante una función *hash*, un resumen que es utilizado como huella digital del mensaje. El resultado que se obtiene de este resumen, que se cifra con su clave privada, se denomina «firma digital» y se enviará adjunta al mensaje original.

Cualquier receptor del mensaje puede comprobar su autoría descifrando la firma digital con la clave pública del firmante, lo que dará como resultado el resumen del mensaje.

Para comprobar que el contenido no ha sido modificado desde su creación, se aplica la función *hash* al documento original por medio de la comprobación del resultado obtenido con el resumen cifrado que se ha recibido. Si ambos coinciden, el documento queda verificado; en caso contrario, se considera que el documento es erróneo o ha sido modificado.

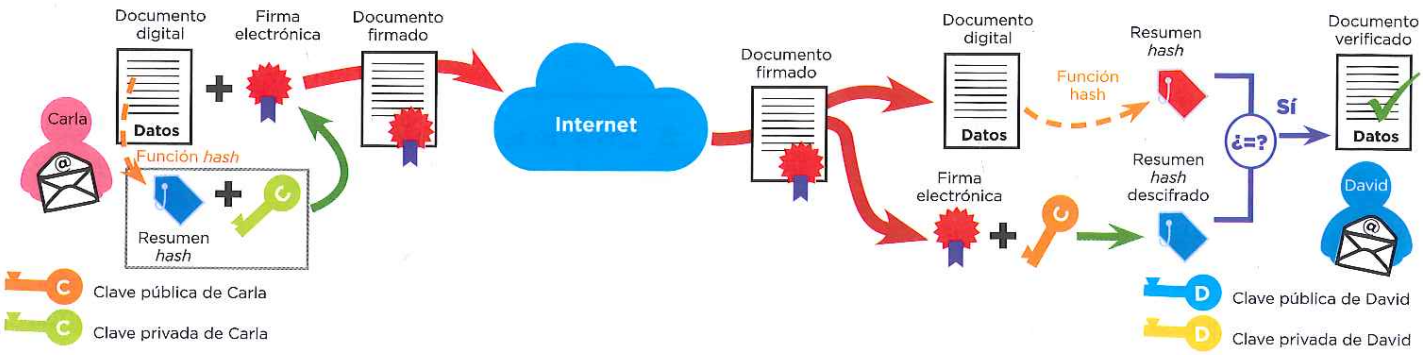


Fig. 16. Carla firma digitalmente el mensaje para que David pueda verificar que realmente es ella quien lo ha enviado.

¿Cómo se firma un documento?

Para realizar la firma electrónica de un documento, se pueden seguir dos métodos:

- **Utilizar una aplicación en el dispositivo.** Son aplicaciones de firma que se descargan en el equipo. Existen programas cotidianos, como Adobe Acrobat o Microsoft Office Word, que permiten firmar documentos, aunque es conveniente recurrir a aplicaciones ofrecidas por las Administraciones Públicas, como AutoFirma, eCoFirma y @firma.
- **Firmar directamente en Internet.** Esta opción se utiliza habitualmente al firmar formularios o solicitudes, por ejemplo, en relación con las Administraciones Públicas. El usuario también puede firmar sus propios documentos en Internet a través del servicio ofrecido en el sitio oficial de VALIDe (https://valide.redsara.es).

En cualquier caso, para firmar un documento, es necesario disponer de un certificado digital, por ejemplo, el que incluye el DNI electrónico.

El DNI electrónico

El DNI electrónico incorpora un pequeño circuito integrado o chip que contiene los mismos datos que aparecen impresos en la tarjeta junto con los certificados de autentificación y de firma electrónica.

7.2. El certificado digital

Un certificado digital es un documento electrónico, expedido por una autoridad de certificación, cuya misión es validar y certificar que una firma electrónica se corresponde con una persona, con una empresa o con un organismo público. Contiene la información necesaria para firmar electrónicamente e identificar a su propietario con sus datos (nombre y apellidos, NIF, algoritmo y claves de la firma, fecha de expiración y organismo que lo expide).

El certificado digital identifica a una persona o entidad con dos claves complementarias, una pública y otra privada, de modo que los datos cifrados con una solo se pueden descifrar con la otra. Se diferencian en que la clave privada está pensada para estar siempre bajo el control del firmante y, en cambio, la clave pública se puede repartir o enviar a otros usuarios.

Fig. 17. Firma de un documento utilizando el DNI electrónico.

Autoridades de certificación

Las autoridades de certificación son aquellas instituciones de confianza responsables de emitir y revocar los certificados digitales utilizados en la firma electrónica, ya que, de otro modo, no contarían con las garantías de seguridad para los que han sido diseñadas. La autoridad de certificación da fe de que la firma electrónica se corresponde con un usuario concreto, razón por la que los certificados están firmados, a su vez, por la autoridad de certificación.

Actualmente, en España, los certificados electrónicos emitidos por entidades públicas son el DNI electrónico y el de la Fábrica Nacional de Moneda y Timbre, Real Casa de la Moneda.

Actividades

1 Accede a la aplicación online VALIDe, utilizando un equipo con lector de tarjetas, para realizar las siguientes tareas con tu DNI electrónico:

a) Comprueba la validez de tu certificado digital.

b) Firma electrónicamente uno de los trabajos que has realizado.

2 Los navegadores de Internet disponen de varios certificados instalados.

a) ¿Cómo se puede acceder a ellos? ¿Para qué se utilizan?

b) ¿Qué entidades de certificación incluyen? ¿En qué pestaña aparecen los de clave privada?

8 Navegación segura

La navegación en páginas web, junto con el uso del correo electrónico, es uno de los servicios de Internet más utilizados. Sus ventajas, así como sus riesgos, son innumerables, ya que los usuarios pueden convertirse en víctimas de todo tipo de delitos informáticos que aprovechan las vulnerabilidades del software y la inexperiencia de los usuarios para la consecución de sus fines, ya sean lucrativos o de otro tipo. Ante estas amenazas presentes en la red, se deben seguir unas determinadas pautas de navegación que permitan hacer uso de los servicios que ofrece Internet de forma segura.

8.1. Buenas prácticas de navegación

El uso adecuado del navegador, de las herramientas de seguridad y del sentido común son las mejores armas para no convertirse en víctima de ciberataques.

Algunas de las pautas que se deben seguir para realizar una navegación segura son las siguientes:

- **Configurar el navegador adecuadamente.** El navegador permite configurar diferentes niveles de seguridad, lo que posibilita, entre otras opciones, usar filtros contra la suplantación de la identidad, bloquear elementos emergentes y activar el control parental para la protección de menores. Aun así, es recomendable eliminar periódicamente la información que se almacena en el historial y en la memoria caché.
- **No acceder a sitios web de dudosa reputación y evitar enlaces sospechosos.** Numerosos sitios web fraudulentos suelen promocionarse con descuentos, regalos, programas gratuitos, material multimedia, etc., con el propósito de captar usuarios. Los vínculos contenidos en páginas web, mensajes de correo electrónico o mensajería instantánea, como WhatsApp, pueden direccionar a las víctimas a sitios maliciosos capaces de infectar el equipo del usuario.
- **Aceptar únicamente las *cookies* deseadas.** Las *cookies* son pequeños archivos de texto con metadatos de una visita: identificadores de sesión, procedencia de la visita, duración de la misma, etc. Por ejemplo, la *cookie* de Facebook permite dejar abierta la sesión sin necesidad de introducir el usuario y la contraseña cada vez que se desea acceder al sitio web.
- **Proteger los datos personales.** No se deben facilitar datos personales, como el nombre y los apellidos, la dirección o el número de tarjeta de crédito, en aquellas páginas que no sean de absoluta confianza y que no estén bajo protocolo seguro (HTTPS). Así, nunca se debe acceder a estos sitios haciendo clic en enlaces que se reciban, por ejemplo, en un correo electrónico.
- **Descargar aplicaciones de sitios web oficiales.** Es preciso desconfiar de los sitios desconocidos que ofrecen descargas, ya que constituyen una de las principales vías de propagación de virus. Aunque se utilicen sitios web fiables, cualquier archivo descargado de la red debe ser analizado con un antivirus antes de abrirse. Por otro lado, las copias de software pirata, además de no ser éticas ni legales, pueden contener virus, espías, troyanos, etc.
- **Revisar el correo electrónico.** Además de analizar el correo, hay que utilizarlo con cautela, sospechando de los mensajes no esperados. Por otro lado, es recomendable activar la carpeta de detección de *spam* y revisarla periódicamente para comprobar que no se ha introducido un mensaje válido en ella.
- **Actualizar el sistema operativo y sus aplicaciones.** Los ciberatacantes utilizan las vulnerabilidades detectadas en los programas informáticos para lanzar sus ataques. Por este motivo, es recomendable configurar las actualizaciones automáticas del equipo.

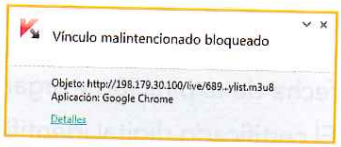


Fig. 18. Vínculo malicioso bloqueado por un antivirus.

Fig. 19. Sitio web malicioso detectado durante la navegación.

8.2. Navegación privada

La navegación privada es una medida de privacidad para que el navegador no almacene la información que se genera en relación con la navegación (*cookies*, usuarios y contraseñas, historial, memoria caché...), por lo que es recomendable su uso al compartir el equipo con otras personas o al utilizarlo en un lugar público. Esta medida de seguridad solo afecta al equipo, ya que no permite ocultar la actividad de navegación ni al servidor, ni al proveedor de servicios de Internet ni a los sitios web que se visitan, por lo que su uso permite alejar a curiosos, pero no a atacantes expertos. Para activarla, hay que utilizar la opción **Nueva ventana de incógnito, Navegación privada** o **Navegación inPrivate,** en función del navegador.

Fig. 20. Navegación privada.

8.3. Proteger la privacidad en la red con un *proxy*

Los servidores *proxy* actúan como intermediarios entre los equipos de los usuarios y los sitios web que visitan. El usuario accede al *proxy* y utiliza su buscador para navegar por Internet. De este modo, las páginas visitadas solo pueden captar datos del *proxy*, pero no del usuario.

Existen multitud de servidores *proxy* disponibles de forma gratuita, si bien suelen contar con algunas restricciones. Funcionan correctamente para consultar páginas web, pero para acceder a contenidos multimedia o para descargar ficheros son demasiado lentos. Algunos ejemplos de servidores *proxy* son Anonymouse o hide.me.

8.4. Navegación anónima

La navegación anónima evita el seguimiento de sitios web que intentan obtener información de los usuarios y mantener el anonimato en comunicaciones que requieren la máxima privacidad.

Uno de los navegadores anónimos más utilizados es Tor, un software libre que, junto con una red de ordenadores voluntarios, oculta la dirección de IP y asigna otra de cualquier parte del mundo, manteniendo la integridad y la confidencialidad de la información que viaja por la red. Otra opción pasa por instalar complementos de navegación anónima, como anonymoX para Firefox, que modifican la IP visible de los usuarios por una IP genérica de sus servidores.

Estas redes anónimas están diseñadas para proteger la privacidad de los internautas frente a las amenazas de la red. Sin embargo, no hay que olvidar que, aunque la web visitada no tenga acceso a los datos del usuario, estos quedan registrados en los servidores anónimos, del mismo modo que los operadores pueden identificar cualquier llamada oculta. Así, en caso de que un malhechor utilice estas redes para cometer un delito, este puede ser identificado por las autoridades con la misma facilidad con la que se haría si utilizase un sistema de navegación convencional.

El papel de la Policía

La Policía cuenta con unidades especializadas en la lucha contra los delitos informáticos.

Actividades

1. Los archivos infectados suelen ser documentos o programas ejecutables. ¿Crees que abrir la imagen **fondo.jpg** podría entrañar algún peligro?
2. Los sistemas operativos no muestran las extensiones de archivos conocidos por defecto (por ejemplo, **gimp.exe** aparece como **Gimp**). ¿Qué nombre aparece para el *script* **fondo.jpg.vbs**?
3. Imagina que te encuentras de viaje en China, donde el Gobierno restringe el uso de servicios como YouTube o Facebook a sus ciudadanos. ¿Qué harías para consultar tus redes sociales?
4. Elabora un decálogo de buenas prácticas de uso de la mensajería instantánea (a través de aplicaciones como WhatsApp) y del correo electrónico.

9 Privacidad de la información

Se considera «información privada» toda aquella información protegida por la LOPD (Ley Orgánica de Protección de Datos) o aquella que otros usuarios o entidades no desean que sea conocida (sitios visitados, correo electrónico, etc.).

La enorme cantidad de datos de carácter personal que circula por las redes, unida a la capacidad de los sistemas informáticos para combinar y procesar las información, supone amenazas a la privacidad de los individuos.

Fig. 21. Actividad de un usuario registrada por Google.

9.1. Amenazas a la privacidad

Las amenazas a la privacidad por el *malware* son unos de los mayores problemas de seguridad informática. Algunas de ellas son las siguientes:

- **Sistemas operativos.** La mayoría de dispositivos que se conectan a Internet utilizan un sistema operativo que, para funcionar, reúne la información confidencial del usuario, como sus datos de identificación biométrica, su idioma, su ubicación, sus búsquedas habituales... Los atacantes podrían aprovechar alguna vulnerabilidad en este software para obtener todos estos datos.
- **Contraseñas.** El método más extendido para la identificación de los usuarios es el uso de contraseñas. Para evitar que otros usuarios consigan apoderarse de esta información secreta, es importante utilizar autentificaciones biométricas o, en su defecto, generar contraseñas fuertes, con distintos tipos de caracteres y con una longitud mínima de ocho caracteres.
- **Registro de visitas web**. Cada vez que se accede a una página web, el navegador proporciona datos sobre el navegador, el sistema operativo, los dispositivos, la dirección IP, etc. Estos datos pueden ser utilizados fraudulentamente para obtener información de los usuarios y lanzar ciberataques.
- **Sesiones del navegador.** Algunos navegadores permiten gestionar el historial o los marcadores desde cualquier lugar. En algunos casos, como en Google Chrome, la sesión permanece abierta aunque el usuario cierre la aplicación.
- ***Cookies.*** Algunos sitios web utilizan *cookies* para obtener información acerca de los hábitos de navegación del usuario o sus datos personales, para realizar seguimientos de compras en línea, etc. En la mayoría de casos, esta información se utiliza para fines publicitarios, aunque, en otras ocasiones, las *cookies* pueden ser manipuladas con intenciones fraudulentas.
- **Formularios.** La web 2.0 ofrece multitud de servicios online, que, en la mayoría de casos, requieren que el usuario se registre a través de un formulario. En caso de contener campos con información confidencial, es necesario verificar la legitimidad del sitio. Una buena estrategia es corroborar el dominio y el uso del protocolo HTTPS.
- **Redes sociales.** Las publicaciones en redes sociales, como Instagram, Twitter o Facebook, esconden más peligros de lo que la mayoría de usuarios sospechan. Para los ciberatacantes, las redes sociales constituyen un método sencillo y rápido con el que acceder a todo tipo de información personal (fotografías, vídeos, datos personales...).
- **Google.** La principal fuente de ingresos de Google está relacionada con la publicidad adaptada a los gustos y necesidades del usuario. Esta compañía ofrece gran parte de los servicios que se utilizan habitualmente en Internet en sus diferentes aplicaciones (Chrome, Maps, Picasa, YouTube, Store, Google+, Books, etc.), por lo que es capaz de reunir una gran cantidad de información sobre cada uno de sus usuarios. Una medida de protección consiste en configurar las opciones de privacidad de los servicios de Google.

9.2. Antiespías

El espionaje se define como la obtención encubierta de datos o de información confidencial. Para llevarlo a cabo, se utilizan diversas técnicas con el fin de obtener información confidencial o privada, práctica que se considera un delito y que está penada por la ley.

Los programas espías o *spyware* se introducen en los dispositivos en forma de pequeñas aplicaciones que recopilan información del sistema y de los usuarios para enviarla a los ciberatacantes.

Los programas antiespía funcionan de manera similar a los antivirus, a saber: comparan los archivos analizados con una base de datos de software espía. Algunas de las aplicaciones antiespías más populares son CCleaner, Ad-Aware, Windows Defender, Malwarebytes y SpyBot.

Creepware

El *creepware* o la *webcam* espía es el espionaje informático que activa la *webcam* y el micrófono de forma remota, sin el consentimiento del usuario. Los expertos coinciden en tapar las *webcams*, como norma de seguridad, cuando no se utilizan.

9.3. Borrar archivos de forma segura

Cuando se elimina un archivo de la papelera, es posible recuperarlo si se emplea el software adecuado. Esto garantiza que los documentos importantes no se pierdan en caso de que se borren accidentalmente o, incluso, al formatear un disco. Sin embargo, esto compromete la privacidad cuando el usuario quiere eliminar archivos sin que nadie pueda tener acceso a ellos.

De la misma manera que existen programas para recuperar archivos, otros garantizan la eliminación segura de archivos para que sean irrecuperables. Otras aplicaciones, como CCleaner, incluyen, además, la posibilidad de borrar el espacio libre para evitar la recuperación de cualquier archivo eliminado previamente.

Limpiador. Elimina el *spyware* y los archivos innecesarios del sistema operativo y de las aplicaciones, con lo que se mejora el rendimiento del equipo.

Registro. Borra las entradas inválidas del registro de Windows fruto de la desinstalación de aplicaciones que van dejando rastro. Ofrece la posibilidad de crear una copia de seguridad previamente.

Herramientas. Permite desinstalar programas, desactivar los programas que se inician automáticamente con el arranque de Windows, buscar duplicados, restaurar el sistema y borrar de forma segura algunos archivos o el espacio libre del disco.

Opciones. Configura el idioma, las funciones de la aplicación, las *cookies*, etc.

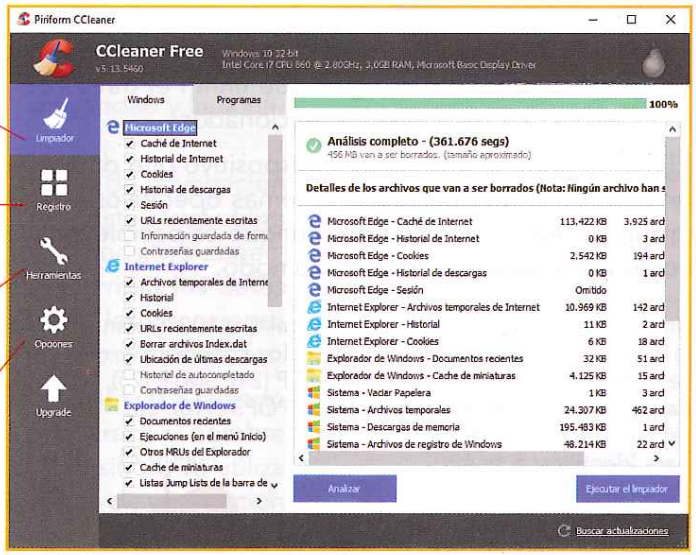


Fig. 22. Interfaz de CCleaner.

Actividades

1. ¿Consideras que WhatsApp es una aplicación segura? Investiga en Internet si presenta vulnerabilidades de seguridad o privacidad.
2. ¿En qué consiste la verificación en dos pasos de Google? ¿Cómo puedes acceder a tus cuentas cuando tu teléfono se queda sin batería?
3. Averigua cuáles son las aplicaciones más populares para recuperar archivos borrados y para eliminar archivos de forma segura.
4. Configura las opciones necesarias en el navegador para proteger tu privacidad, borra los datos de navegación y desactiva el seguimiento de tu tráfico.

10 Protección de las conexiones en red

En la actualidad, las redes de ordenadores están presentes en todas partes, desde los hogares hasta las grandes empresas. Estas redes proporcionan servicios tan variados como el acceso a Internet, el intercambio de datos, el comercio electrónico, la conexión entre dispositivos, los servicios de VoIP, la gestión de la domótica de un hogar, etc.

Un equipo conectado en red ofrece innumerables ventajas, aunque sus riesgos también se multiplican, ya que cualquier vulnerabilidad puede convertirse en una amenaza.

Para asegurar una red informática, hay que establecer, entre otros aspectos, políticas de seguridad que se ajusten al diseño de la red, asignar *firewalls*, limitar el acceso a *routers*, inmunizar los equipos con soluciones antivirus adecuadas y mantener el software actualizado.

10.1. Cortafuegos

El cortafuegos, también denominado *«firewall»*, es un dispositivo hardware o software cuya finalidad es controlar la comunicación entre un equipo y la red, por lo que se ha convertido en una de las principales defensas contra ataques informáticos y en una pieza clave para bloquear la salida de información del ordenador a Internet. El origen del término tiene que ver con la seguridad industrial, donde se utilizaban paredes gruesas con cámaras de aire en aquellos lugares con peligro de incendio para aislar rápidamente los espacios y minimizar los daños.

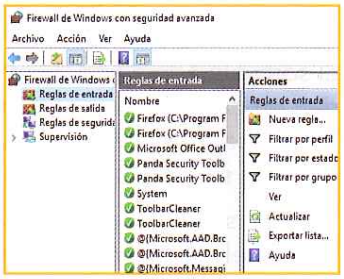


Fig. 24. Reglas de entrada en *firewall* de Windows.

Todos los mensajes que entran o salen por el cortafuegos son examinados, de modo que aquellos que no cumplen los criterios de seguridad especificados son bloqueados, con el propósito de evitar los ataques de intrusos, los accesos de empleados a sitios no autorizados, la descarga de software dañino o que los equipos infectados de *malware* envíen datos sin autorización fuera de la red. Para ello, es necesario configurar las reglas que filtran el tráfico por los puertos, aceptando o bloqueando los paquetes inspeccionados.

El cortafuegos se instala en el dispositivo que da acceso a Internet, que suele ser un servidor o un *router*. Los sistemas operativos y las soluciones antivirus suelen incluir su propio cortafuegos, aunque es posible instalar herramientas específicas como ZoneAlarm, Outpost o Comodo.

Un puerto de red es la interfaz con la que se comunica una aplicación a través de la red. Están numerados para identificar a qué aplicación van destinados los datos recibidos por cada uno.

Los puertos del 0 al 1023 están asignados a los protocolos conocidos y más utilizados, como FTP (21), SMTP (25), HTTP (80), HTTPS (443), POP3 (110), etc.

Los puertos comprendidos entre el 1024 y el 49 151 están registrados y pueden ser usados por cualquier aplicación.

Los puertos del 49 152 al 65 535 son dinámicos o privados, y se utilizan habitualmente en conexiones P2P.

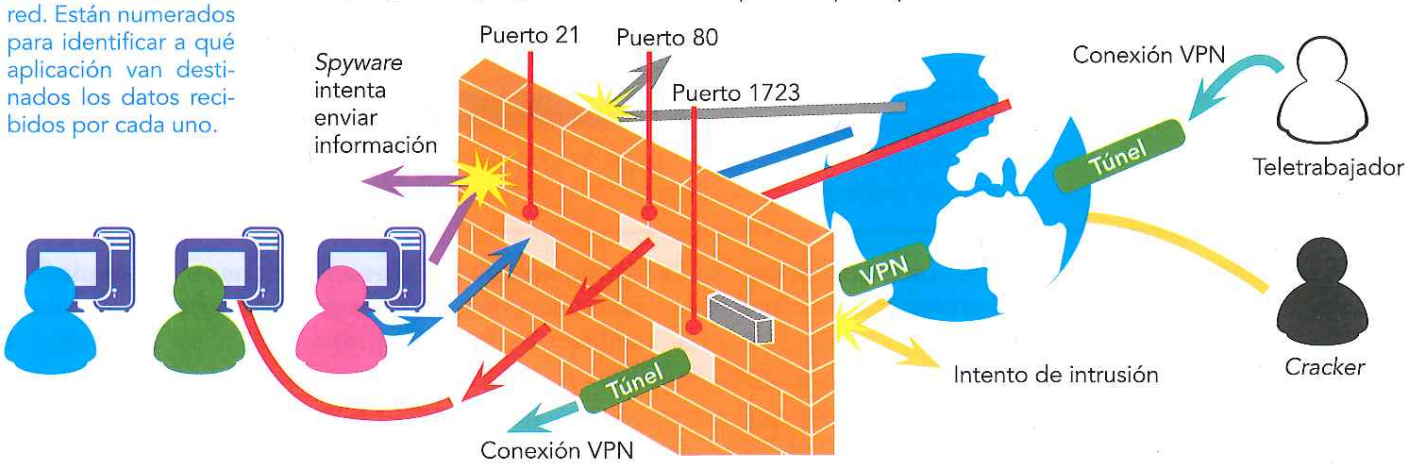


Fig. 25. El cortafuegos controla las conexiones de la red local con Internet.

10.2. Redes privadas virtuales

Las redes privadas virtuales (VPN) son conexiones punto a punto a través de una red privada o pública insegura, como Internet. Los clientes usan protocolos especiales basados en TCP/IP, denominados «protocolos de túnel», para realizar conexiones con una red privada. Una vez que el servidor VPN autentifica al usuario, se establece una conexión cifrada. Existen dos tipos de conexiones a este tipo de redes:

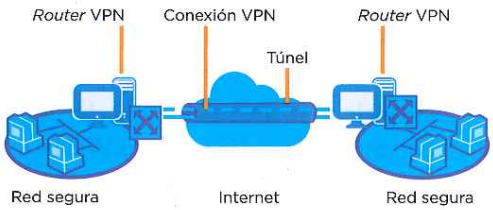


Fig. 26. VPN de sitio a sitio.

- **VPN de acceso remoto.** Se utilizan para que los usuarios tengan acceso a un servidor de una red privada con la infraestructura proporcionada por una red pública. Es el caso de las personas que trabajan a distancia, de los alumnos que acceden a la red de una universidad o de los usuarios que desean obtener una conexión segura desde lugares públicos (cafeterías, hoteles, bibliotecas, etc.).
- **VPN de sitio a sitio.** Permiten a las organizaciones conectar redes a través de Internet utilizando comunicaciones entre ellas. Algunos ejemplos de sus aplicaciones son la conexión entre oficinas, sucursales, empresas o Administraciones Públicas.

Los sistemas operativos incluyen su propio servidor VPN, aunque existe una gran variedad de aplicaciones para ello; por ejemplo, VPNBook, que ofrece servidores alojados en distintos países, de modo que, introduciendo el usuario y la contraseña facilitados, es posible navegar a través de ellos.

10.3. Certificados SSL/TLS de servidor web y HTTPS

El SSL *(secure sockets layer)* es un protocolo criptográfico desarrollado por Netscape hasta la versión 3.0, cuando fue estandarizado y pasó a denominarse TLS *(transport layer security)*. No obstante, hoy en día el término SSL está muy extendido, por lo que se suele aludir a ambos indistintamente.

Dichos estándares se utilizan para emitir certificados de sitios web, por lo que son una pieza fundamental en la seguridad, ya que garantizan la integridad y la confidencialidad de las comunicaciones.

Cuando se utiliza el cifrado basado en SSL/TLS junto al protocolo de navegación web HTTP, se crea un canal cifrado seguro denominado «HTTPS». Este canal utiliza una clave de 128 bits de longitud, conocida únicamente por el dispositivo conectado y por el servidor que facilita la conexión, de modo que encripta los datos convirtiéndolo en un medio seguro para el comercio electrónico, las conexiones bancarias, el correo electrónico, los trámites con las Administraciones Públicas, etc.

Fig. 27. HTTPS está basado en los protocolos HTTP y SSL.

El navegador alerta a los usuarios de la presencia de un certificado SSL/TLS cuando se muestra un candado y la dirección se convierte en HTTPS. Si aparece el nombre de la empresa u organización en color verde, esto significa que el sitio web utiliza un certificado de validación extendida (EV) que requiere un proceso de verificación de identidad mucho más riguroso, lo que aporta una mayor seguridad.

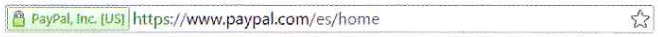


Fig. 25. Sitio web con certificado EV.

Actividades

1. Comprueba las reglas de entrada y salida del cortafuegos para averiguar qué puerto y qué protocolo se utiliza para compartir impresoras.
2. Crea una regla para bloquear la conexión a Internet a una de las aplicaciones instaladas en tu equipo y comprueba si ha surtido efecto.
3. Establece una conexión segura para navegar por Internet utilizando los servidores de VPNBook (puedes conocer los datos de conexión en la pestaña PPTP).
4. Conéctate a varias páginas que utilicen el protocolo HTTPS y comprueba su certificado y cifrado.

11 Seguridad en las comunicaciones inalámbricas

Las redes inalámbricas ofrecen soluciones para compartir información sin hacer uso de cables, posibilitando, así, las transferencias de datos. Utilizan el aire como medio de transmisión, al alcance de cualquier usuario, por lo que, al utilizarlas, se deben adoptar medidas de protección específicas para evitar potenciales amenazas.

La seguridad en la comunicación inalámbrica de tecnologías de largo alcance, como móviles (3G, 4G y LTE) y WiMAX, suele estar gestionada por las operadoras. Pero, en el caso de las redes locales y de las redes de área personal, donde los estándares de comunicación más utilizados son Bluetooth y wifi, la seguridad depende, en gran medida, de los usuarios.

11.1. Seguridad en Bluetooth

Bluetooth es la especificación que define un estándar global de comunicaciones inalámbricas para redes de área personal y que permite la transmisión de voz y de datos entre diferentes equipos por medio de un enlace por radiofrecuencia en entornos de comunicación móviles.

La tecnología Bluetooth tiene un alcance de unos diez metros, por lo que se ha integrado en dispositivos de la vida cotidiana que forman parte de las redes personales (PAN), como teléfonos y relojes inteligentes, manos libres, dispositivos GPS, etc.

Los ciberatacantes que emplean estas comunicaciones suelen utilizar antenas que amplían considerablemente el campo de acción de la señal Bluetooth. Algunos de los ataques que se realizan por medio de estas comunicaciones son los siguientes:

- ***Bluejacking.*** Consiste en el envío de *spam* al usuario por medio del intercambio con este de una vCard, de una nota o de un contacto en cuyo nombre aparezca el mensaje de *spam*. En algunos casos, se utiliza el propio nombre del dispositivo como *spam*, por lo que la víctima recibe como mensaje de aviso (por ejemplo, «OBTÉN CUPONES DE DESCUENTO EN www.paginaweb.com») que determinado usuario está tratando de conectarse con su dispositivo.
- ***Bluesnarfing.*** Aprovecha las vulnerabilidades del protocolo para sustraer información del dispositivo atacado.
- ***Bluebugging.*** Utiliza técnicas de ingeniería social para que la víctima acepte una conexión inicial para infectar el dispositivo con *malware* de control remoto. A partir de entonces, el usuario dispondrá de acceso remoto al teléfono del usuario y podrá utilizar sus funciones: escuchar llamadas, enviar mensajes, acceder a los contenidos o, incluso, utilizar el dispositivo para lanzar otros ciberataques, etc.

La adopción de algunas medidas de seguridad sencillas puede evitar los ataques. Por esta razón, deberían formar parte de la conducta habitual de un usuario de dispositivos Bluetooth. Algunas de ellas son:

- Activar Bluetooth cuando sea necesario realizar algún tipo de comunicación a través de este medio y desactivarlo cuando se deje de utilizar.
- Cambiar el nombre del dispositivo para que no desvele datos personales y configurarlo para que permanezca oculto.
- No emparejar ni aceptar conexiones entrantes de dispositivos desconocidos, ya que la información transferida podría estar infectada de software malicioso.
- Verificar periódicamente la lista de dispositivos de confianza para eliminar los que no se utilizan habitualmente o sean desconocidos.

Fig. 28. Ejemplo de ataque *bluejacking*.

Actividades

1. Revisa la configuración Bluetooth de tu dispositivo y adopta las medidas propuestas para protegerlo.
2. Indica cuáles son las diferencias entre Wi-Fi Direct y Bluetooth a la hora de compartir información con otros dispositivos.
3. La tecnología inalámbrica NFC de corto alcance se utiliza, entre otras cosas, para realizar pagos a través del móvil y de tarjetas *contactless*. Investiga en qué consiste y el grado de seguridad que proporciona.

11.2. Seguridad en redes wifi

Las redes wifi utilizan una tecnología inalámbrica que realiza la conexión entre dispositivos situados en un área relativamente pequeña, como una habitación, una oficina, una casa o un edificio, a través de ondas electromagnéticas. La señal en abierto suele tener un alcance de unos 100 metros, aunque cualquier atacante podría captar la señal a varios kilómetros de distancia utilizando una antena alineada.

El dispositivo que autentifica a los usuarios y que emite la señal suele ser un *router* o punto de acceso, por lo que la seguridad de las redes inalámbricas depende casi exclusivamente de ellos. Para acceder a la configuración del *router,* es necesario teclear su dirección de IP en el navegador; a continuación, se muestra una web en la que hay que introducir el nombre del usuario administrador y la clave de acceso.

Algunas de las medidas de seguridad básicas que se pueden configurar en el *router* para mantener una red wifi segura son las siguientes:

- **Personalizar la contraseña de acceso.** Las contraseñas por defecto de algunos *routers* suelen ser muy vulnerables (admin/admin, admin/1234…) o se pueden averiguar rápidamente en Internet al introducir el modelo de *router.*
- **Cambiar el SSID.** El nombre de la red (SSID) es el identificador con el que se etiqueta la red inalámbrica para que cada usuario pueda localizarla, por ejemplo, Wifi_Ana3C. La mayoría de *routers* vienen preconfigurados con el nombre de fábrica, por lo que es fundamental cambiarlo por uno genérico que no revele datos personales, de ubicación ni del modelo de *router* e, incluso, es recomendable ocultarlo.
- **Revisar el cifrado.** La señal inalámbrica puede ser interceptada más fácilmente que una red cableada, por lo que es necesario utilizar estándares de cifrado como WPA2. Este sistema utiliza diferentes versiones para autentificar a los usuarios con una sola clave (WPA2-Personal) o utilizando claves privadas para cada usuario (WPA2-Enterprise o Radius). Los sistemas anteriores, como WEP o WPA, no se deben utilizar, ya que son vulnerables y se pueden descifrar fácilmente.
- **Desactivar el acceso por WPS.** El estándar WPS (Wi-Fi Protected Setup) facilita la configuración de una red segura con WPA2 a sus usuarios. Sin embargo, gran parte del software malicioso basa sus ataques en el acceso por WPS, por lo que es recomendable desactivarlo.
- **Filtrar las MAC.** Las direcciones MAC son establecidas por el fabricante y únicas para cada dispositivo de red. Al configurar la autentificación por MAC, es posible añadir los dispositivos que pueden tener acceso a la red wifi y bloquear el resto.
- **Actualizar el *firmware*.** El *firmware* es el software que controla los circuitos de los dispositivos electrónicos. Los fabricantes suelen liberar actualizaciones que subsanan errores de seguridad, mejoran el rendimiento, etc., para evitar que los atacantes se aprovechen de estas vulnerabilidades.
- **Comprobar el historial de actividad.** La actividad del *router* puede desvelar información sobre posibles intrusiones, ya que muestra los datos de los equipos conectados, los horarios, la duración de la sesión, etc.
- **Utilizar software de auditoría.** En el mercado existen herramientas diseñadas para evaluar la seguridad de una red y detectar sus posibles vulnerabilidades. Una de las más populares es Nmap.

Si estos intentos para evitar que los intrusos accedan a la red wifi no funcionan, la forma más efectiva de recuperar el control de la misma pasa por reiniciar la configuración de fábrica y volver a configurarlo todo desde el principio.

Fig. 29. Botón WPS de un *router.*

Fig. 30. Opciones de configuración de un *router* inalámbrico.