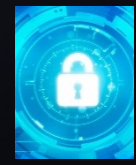
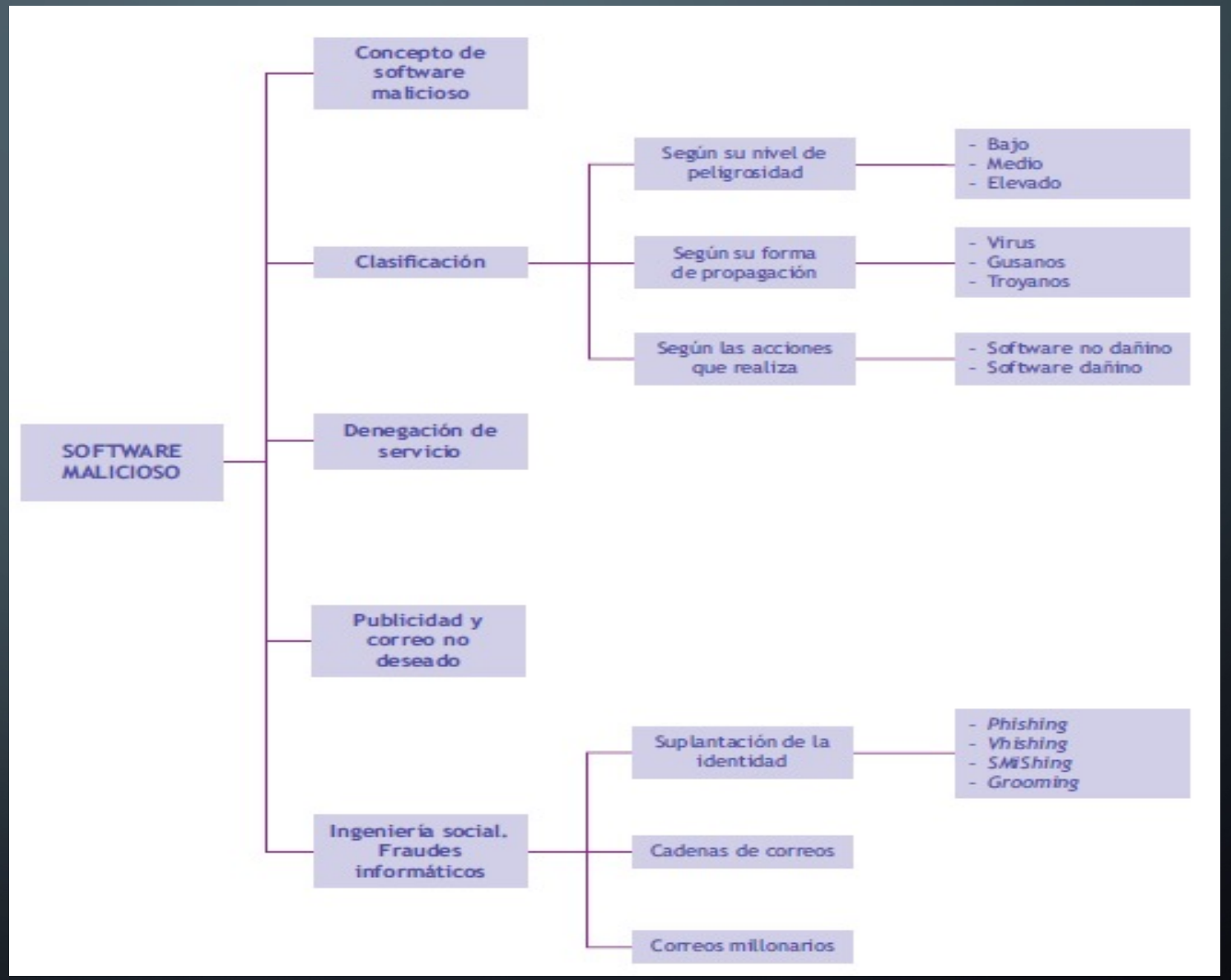
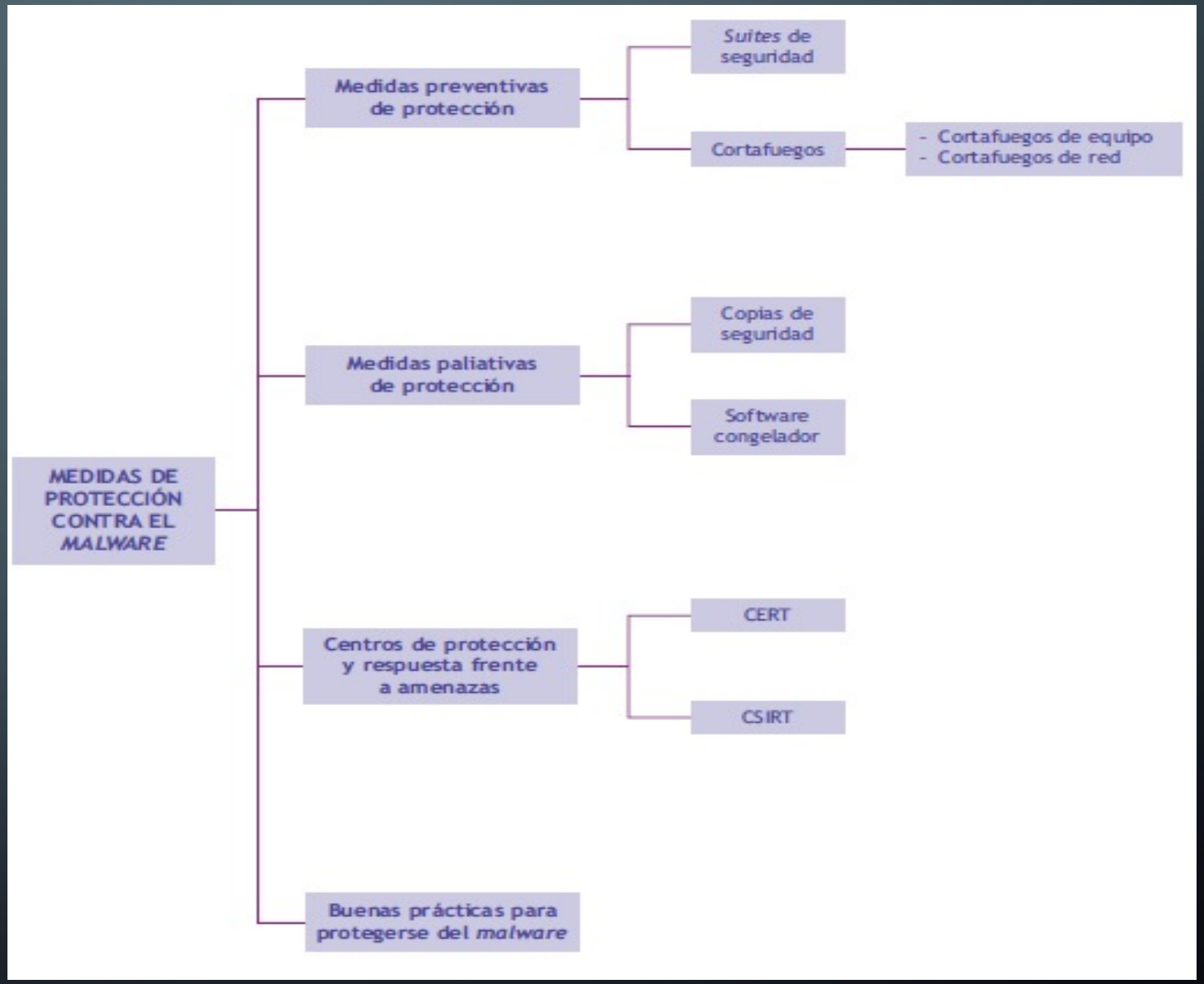
SEGURIDAD INFORMÁTICA

UNIDAD 6: SOFTWARE MALICIOSO Y MEDIDAS DE PROTECCIÓN CONTRA EL MALWARE

SEGURIDAD INFORMÁTICA




SOFTWARE MALICIOSO
Concepto de software malicioso
Clasificación
Según su nivel de peligrosidad
- Bajo
- Medio
- Elevado
Según su forma de propagación
- Virus
- Gusanos
- Troyanos
Según las acciones que realiza
- Software no dañino
- Software dañino
Denegación de servicio
Publicidad y correo no deseado
Ingeniería social. Fraudes informáticos
Suplantación de la identidad
- Phishing
- Vhishing
- SMiShing
- Grooming
Cadenas de correos
Correos millonarios


MEDIDAS DE PROTECCIÓN CONTRA EL *MALWARE*
Medidas preventivas de protección
Suites de seguridad
Cortafuegos
- Cortafuegos de equipo
- Cortafuegos de red
Medidas paliativas de protección
Copias de seguridad
Software congelador
Centros de protección y respuesta frente a amenazas
CERT
CSIRT
Buenas prácticas para protegerse del *malware*

ÍNDICE DE CONTENIDOS

1. CONCEPTO DE SOFTWARE MALICIOSO

- El **software malicioso o malware** puede modificar el funcionamiento de un equipo informático o alterar la información que procesa, ya sea borrándola, modificándola o enviándola sin nuestro conocimiento a terceras personas.
- Por lo tanto, el término software malicioso tiene un ámbito más amplio que el de virus informático y se utiliza para designar a cualquier software que pueda representar una amenaza al sistema o resultar molesto para el usuario.
- Así, un virus informático es una variedad más de software malicioso, como lo son los troyanos, el spyware, el adware, etc.

1. CONCEPTO DE SOFTWARE MALICIOSO

Generalmente, el malware se propaga a través de dos vulnerabilidades:

- **Vulnerabilidades del software:**

Se trata de explotar debilidades del sistema operativo o de algún programa. Algunos especímenes de malware son capaces de copiarse a sí mismos y enviarse automáticamente a través de la red para infectar a la mayor cantidad posible de equipos.

- **Vulnerabilidades asociadas a las personas:**

En la mayoría de ocasiones son los propios usuarios quienes, con su desconocimiento o exceso de confianza, contribuyen a la propagación del software malicioso.

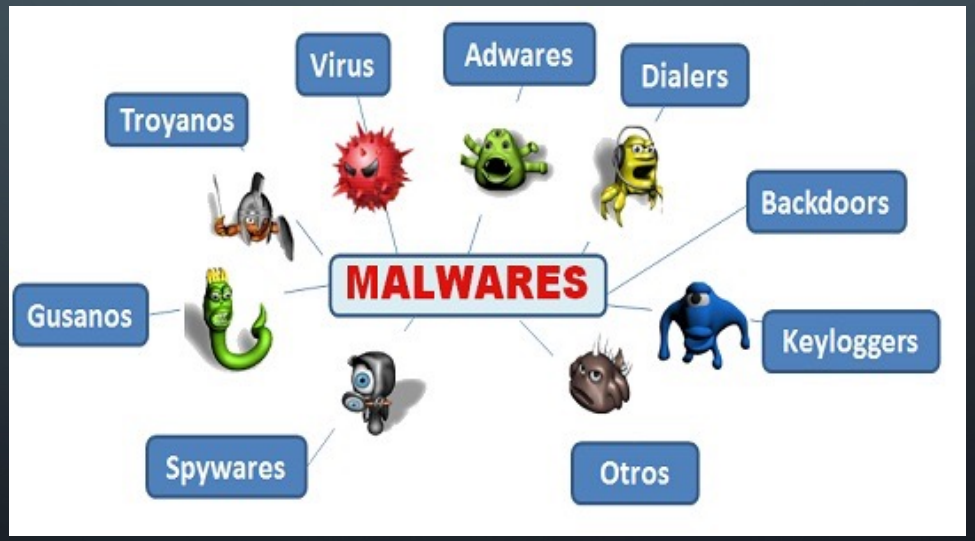
1. CONCEPTO DE SOFTWARE MALICIOSO

Otro aspecto a tener en cuenta sobre el software malicioso es su difusión.

- Prácticamente la mayoría del malware desarrollado en la actualidad afecta a sistemas Microsoft, que son los más extendidos.
- Es un error muy común pensar que estamos protegidos por el simple hecho de no utilizar un sistema operativo de Microsoft, ya que existen variedades de malware diseñadas específicamente para aprovechar vulnerabilidades de otras plataformas, como macOS y GNU/Linux.
- Por otro lado, el malware no solo afecta a los equipos informáticos y en la actualidad es fácil encontrar especímenes creados para dispositivos móviles que afectan a sistemas como Android o iOS.

2. CLASIFICACIÓN DEL MALWARE

- Existe una gran variedad de software malicioso y cada día se descubren nuevos programas de este tipo, por lo que no es fácil realizar una clasificación del malware.
- Por ello, se pueden establecer distintas clasificaciones, en función del criterio usado para realizarlas:



2. CLASIFICACIÓN DEL MALWARE

2.1. SEGÚN EL IMPACTO PRODUCIDO SOBRE LA VÍCTIMA

- Atendiendo a este criterio, distinguimos **tres niveles de peligrosidad**: bajo, medio o elevado.
- Para evaluar el grado de peligrosidad de un espécimen, se estudia la **gravedad de las acciones** que produce sobre un equipo infectado, su **velocidad** y **facilidad** de **propagación** y la cantidad de infecciones producidas **recientemente**.

2. CLASIFICACIÓN DEL MALWARE

2.2. SEGÚN SU FORMA DE PROPAGACIÓN

Según la forma de propagarse, los tipos de malware más importantes son:

VIRUS:

- Un software malicioso que tiene por finalidad alterar el funcionamiento de un equipo informático sin el conocimiento o consentimiento de su usuario, corrompiendo o destruyendo archivos.

2. CLASIFICACIÓN DEL MALWARE

2.2. SEGÚN SU FORMA DE PROPAGACIÓN

Según la forma de propagarse, los tipos de malware más importantes son:

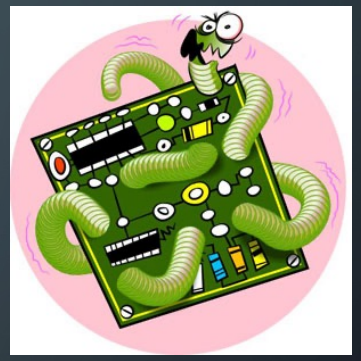
VIRUS:

- El funcionamiento de los virus es simple: cuando se ejecuta el software malicioso, el virus se instala en la memoria RAM del ordenador, desde donde infecta archivos ejecutables y graba los archivos infectados en el disco duro del equipo. De este modo, una vez en el disco, el virus se ejecutará cada vez que se utilice el programa infectado. Si se reinstala el programa afectado sin apagar el ordenador, el virus volverá a infectarlo (ya que sigue estando en la RAM).
- En cuanto a sus efectos, en algunos casos las acciones resultantes de la ejecución de un virus parecen inofensivas, como cambiar carpetas por accesos directos ocultando los archivos originales, pero en otras ocasiones pueden llegar a modificar el registro de Windows con la finalidad de evitar el cortafuegos, permitiendo a un atacante controlar a su antojo el equipo de la víctima.

2. CLASIFICACIÓN DEL MALWARE

2.2. SEGÚN SU FORMA DE PROPAGACIÓN

Según la forma de propagarse, los tipos de malware más importantes son:



GUSANO:

- Es un tipo de malware que se propaga automáticamente sin necesidad de infectar otros archivos, ya que puede duplicarse a sí mismo.
- Por tanto, puede extenderse sin necesidad de intervención de los usuarios de los equipos infectados.
- Su finalidad no es destruir archivos o equipos, sino que están pensados para consumir recursos de un sistema o red de comunicaciones hasta saturarlo y provocar su caída.
- Sus principales formas de difusión son: los recursos compartidos, las redes P2P y el correo electrónico.

2. CLASIFICACIÓN DEL MALWARE

2.2. SEGÚN SU FORMA DE PROPAGACIÓN

Según la forma de propagarse, los tipos de malware más importantes son:

TROYANO:

- Es un software malicioso que se introduce en un ordenador y se instala en él, aparentando ser un programa inofensivo, pero su finalidad es permitir a un usuario no autorizado tomar el control de la máquina infectada.
- A diferencia de los virus, los troyanos ni infectan o corrompen archivos o programas y, a diferencia de los gusanos, no tienen capacidad de propagarse automáticamente, únicamente buscan permitir la administración remota del equipo a usuarios ilegítimos.

2. CLASIFICACIÓN DEL MALWARE

2.2. SEGÚN SU FORMA DE PROPAGACIÓN

Según la forma de propagarse, los tipos de malware más importantes son:

TROYANO:

- Un troyano, normalmente, está constituido por dos programas: un cliente en el equipo atacante y un servidor que se instala en el ordenador infectado.
- Los tipos más comunes son: backdoor, keylogger, downloader y proxy. Este tipo de malware es especialmente dañino por las consecuencias que puede ocasionar para los usuarios infectados.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso NO dañino.

- No todo el software malicioso realiza acciones dañinas para las víctimas.
- Se consideran no dañinas acciones tales como mostrar publicidad no deseada a los usuarios, mostrar información falsa o asustar a los usuarios mediante algún tipo de broma.
- Es el denominado ***grayware***.
- Los principales tipos son: Spyware, Adware, Hijacking, Jokes y Bulos (Hoaxes).

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso NO dañino: SPYWARE

- El término spyware proviene de la unión de dos palabras inglesas: spy (espía) y software.
- Por tanto, es un tipo de software que trata de conseguir información del usuario.
- A veces únicamente se trata de conseguir estadísticas de navegación (tiempo que un usuario está en una página o páginas visitadas), pero cuando trata de obtener un beneficio de la información conseguida para realizar alguna acción dañina dejará de ser grayware para convertirse en malware.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso NO dañino: ADWARE

- El término adware proviene de la unión de dos palabras inglesas: ad (abreviatura de anuncio) y software.
- Este malware muestra publicidad al usuario de forma intrusiva, por ejemplo, en forma de ventanas emergentes (pop up).
- Aunque este tipo de software no representa una amenaza directa para el usuario, suele ser frecuente su utilización para camuflar la acción de otro malware.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso NO dañino: ADWARE

- Es frecuente encontrar este tipo de programas combinado con spyware para conseguir información y enviársela a terceras personas.
- Otras veces, al instalar un programa legítimo de pago, se ofrece la posibilidad de usarlo gratuitamente instalando adicionalmente un programa de adware.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso NO dañino: HIJACKING

- Cambian la configuración del navegador, por ejemplo, modificando la página de inicio por una página web, que contendrá anuncios o publicidad.
- También pueden modificar los enlaces de la carpeta Favoritos o añadir nuevas barras de herramientas.
- La finalidad de este malware suele ser aumentar la cantidad de visitas que recibe una página web.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso NO dañino: JOKES o Bromas

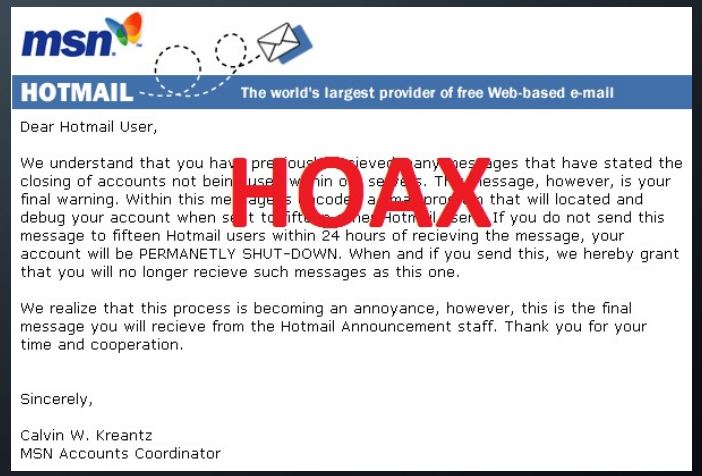
- Consisten en un software malicioso que no realiza ninguna acción dañina sobre el equipo infectado.
- En algunos casos, su acción se limita a hacer creer al usuario que se va a borrar el contenido del disco o a enviar información personal por la red, pero no lo hace.
- Este software se considera un tipo de grayware porque no realiza ninguna acción dañina sobre el equipo, salvo tratar de asustar al usuario.
- Es muy frecuente confundir este término con algún otro tipo de malware como ***rogueware o ransomware***.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso NO dañino: BULOS o Hoaxes

- Son un tipo de malware que suele propagarse por correo electrónico y alerta a los usuarios de alguna amenaza no real, como, por ejemplo, un virus, una estafa, un fallo de seguridad, etc.
- Utilizan técnicas de ingeniería social para lograr que los usuarios reenvíen el correo a otras personas.



2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso dañino:

- Otras variedades de software malicioso representan una amenaza real y atentan contra la seguridad de los equipos, realizando acciones como, por ejemplo, obtener información privada (claves de las cuentas de correo electrónico o de las tarjetas de crédito), modificar o borrar información almacenada en el disco duro o incluso, amenazar a los usuarios para obtener un beneficio económico.
- Aquí es donde los desarrolladores de malware muestran todo su ingenio para sacar provecho de las vulnerabilidades de los sistemas y las aplicaciones instaladas.
- Algunas variedades de malware consideradas como dañinas son: Ransomware, Rogueware, Password Stealer, Bombas lógicas, Keylogger, …

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso dañino: RANSOMWARE

- Este término proviene de la unión de las palabras inglesas ransom (rescate) y software.
- Este tipo de malware cifra archivos importantes del disco duro para exigir el pago de dinero a cambio de la contraseña para descifrarlos.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso dañino: ROGUEWARE

- El término rogueware proviene de rogue, que en inglés significa falso, y software.
- Esta variedad de malware hace creer al usuario que su equipo está infectado por algún virus (sin estarlo realmente) y que la única forma de desinfectarlo es adquiriendo una solución antivirus, por la que habrá que pagar una cantidad de dinero.
- En ocasiones, se indica al usuario que la única forma de eliminar el virus ficticio del equipo es descargar una solución antivirus entrando en un enlace que se visualiza por pantalla.
- Al descargar ese supuesto antivirus, se podría estar dando el control total a un atacante remoto, que podría ver todo lo que visualiza por pantalla la víctima o darle acceso a su disco duro.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso dañino: PASSWORD STEALER

- Los navegadores son la herramienta utilizada para crear o usar cuentas de correo o redes sociales.
- Existen algunos especímenes de malware que se aprovechan de esta situación y modifican el navegador para que capture y envíe las contraseñas cuando la víctima las introduce, obteniendo los datos de sesión.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso dañino: BOMBA LÓGICA

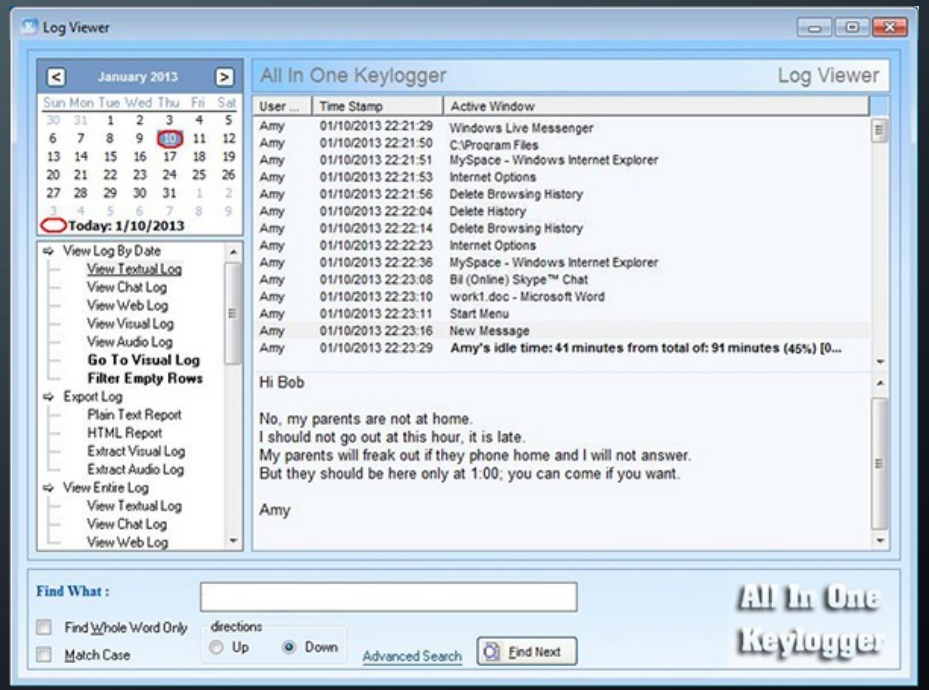
- Se trata de un malware que se pone en marcha cuando se cumple alguna condición, como que sea un día concreto, que se cambie algún dato en una base de datos o que se modifique un archivo del disco duro.

2. CLASIFICACIÓN DEL MALWARE

2.3. SEGÚN LAS ACCIONES QUE REALIZA

Software Malicioso dañino: KEYLOGGERS y BACKDOORS

- Un **Keylogger** es un "registrador de pulsaciones", y un **Backdoor** abre una brecha de seguridad en el sistema infectado, posibilitando la entrada de terceros en el equipo.



3. DENEGACIÓN DE SERVICIO

- Imaginemos por un momento que en nuestro equipo hemos recibido un correo de un conocido que nos invita a ejecutar un archivo que contiene código malicioso.
- Como desconocemos este dato, ejecutamos el archivo y al hacerlo nuestro equipo deja de responder, por lo que la única solución es reiniciarlo.
- Estamos ante un ataque de denegación de servicio, y lo peor es que hemos sido nosotros quienes hemos realizado el ataque sobre nuestro propio equipo.
- Una **denegación de servicio (DoS, Denial of Service)** se define como la *imposibilidad de acceder temporal o permanentemente a un recurso o servicio por parte de un usuario legítimo*. Los ataques de denegación de servicio tratan, pues, de conseguir una degradación de un servicio o recurso.
- Por lo tanto, un **ataque de denegación de servicio** es un ataque a un sistema de computadoras o red que causa que un recurso o servicio sea inaccesible a los usuarios legítimos.

3. DENEGACIÓN DE SERVICIO

Según el origen de los ataques de denegación de servicio efectuado, distinguimos los siguientes:

- **Ataques internos:** son provocados por usuarios legítimos de la organización que, ya sea por desconocimiento o de forma intencionada, provocan la degradación de un recurso o servicio.

- **Ataques externos:** el atacante es una entidad ajena a la organización, es decir, se trata de usuarios ilegítimos que no deberían tener acceso a los equipos que hay en ella. En este tipo de ataques se aprovechan vulnerabilidades existentes en el sistema, como bugs de los programas o la no autenticación de los usuarios, para acceder a él.

3. DENEGACIÓN DE SERVICIO

Una **ampliación** del ataque DoS es el llamado **ataque de denegación de servicio distribuido**, también llamado **DDoS** (por sus siglas en inglés, Distributed Denial of Service) el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión hacia un mismo punto de destino. La forma más común de realizar un DDoS es a través de una **red de bots.**

4. PUBLICIDAD Y CORREO NO DESEADO

- Llamamos **correo no deseado** a todo **correo no esperado** por el usuario que lo recibe.
- Este correo puede resultar muy molesto porque se trata de correo no solicitado que en algunos casos se envía de forma masiva, llegando a **saturar la bandeja de entrada** de nuestra cuenta de correo de información no deseada.
- El correo electrónico es una forma de comunicación rápida, gratuita y fácil de utilizar, por lo que muchas **empresas** lo utilizan masivamente para **darse a conocer** al público o presentar algún producto, constituyendo una nueva variedad de correo no deseado, el **correo basura** o **spam**.

4. PUBLICIDAD Y CORREO NO DESEADO

- Con frecuencia, se confunden los términos ***correo no deseado y correo basura (spam)***, llegando a utilizarse indistintamente, pero es conveniente distinguirlos correctamente.
- Ambos están integrados por mensajes enviados al destinatario sin su consentimiento, pero aplicamos el término **spam** para el correo no deseado que tiene **fines publicitarios o económicos**.

4. PUBLICIDAD Y CORREO NO DESEADO

- Para facilitar el trabajo de los usuarios, algunos antivirus y servidores de correo ofrecen un servicio de detección de correo no deseado, redirigiendo este tráfico a una carpeta especial o eliminándolo directamente.
- En España, el correo electrónico no deseado está prohibido por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE).

Sanciones en materia de correo no deseado

Las sanciones previstas por la Ley 34/2002 para el supuesto de envíos de correo no deseados pueden ser de hasta los 600 000 €.

5. INGENIERÍA SOCIAL. FRAUDES INFORMÁTICOS.

- La mayor parte de las veces, los piratas informáticos no necesitan desarrollar complejos programas para conseguir las contraseñas o los datos bancarios de los usuarios, ya que son estos los que facilitan esta información a los atacantes.
- **La ingeniería social** es una forma de fraude informático muy utilizado por piratas informáticos y **consiste en manipular el comportamiento natural de los usuarios mediante engaños y mentiras.**

5. INGENIERÍA SOCIAL. FRAUDES INFORMÁTICOS.

- Los argumentos utilizados son muy convincentes y conviene estar muy alerta.
- Para extender estas estafas o fraudes, los atacantes utilizan una gran variedad de herramientas o técnicas.
- Aunque el **correo electrónico** es el método más empleado, también se suelen utilizar **mensajes de texto, redes sociales o llamadas de teléfono**.

5. INGENIERÍA SOCIAL. FRAUDES INFORMÁTICOS.

5.1. SUPLANTACIÓN DE IDENTIDAD O SPOOFING

- Es un tipo de fraude que consiste en hacerse pasar por otra persona.
- Un tipo es el **phising**, en el que el atacante crea una página web falsa idéntica a la de una empresa que requiere autenticación para que el usuario introduzca los datos de entrada y estos pasen a poder del atacante.
- Otro tipo es el **vishing**, similar al anterior pero el engaño se realiza a través de una llamada telefónica. El término deriva de la unión de dos palabras en inglés: ''voice'' y ''phishing''.
- Por otro lado, el **smishing** engaña a las víctimas a través del envío de mensajes SMS o mensajería instantánea (como WhatsApp) para conseguir sus contraseñas.
- Otro tipo es el **grooming**, que consiste en el acoso a menores por parte de un adulto.

5. INGENIERÍA SOCIAL. FRAUDES INFORMÁTICOS.

5.2. CADENA DE CORREOS

- Son **mensajes** en los que se incita a su destinatario a difundirlos al mayor número de personas posible **bajo promesas o amenazas**, con el ánimo de **conseguir direcciones de correo**.
- Los argumentos utilizados por parte del emisor del mensaje son muy variados, pero todos persiguen el mismo objetivo: conseguir que el destinatario acepte formar parte del juego o de la trama planteada y que reenvíe el mensaje al mayor número de usuarios posibles para, de este modo, aumentar la difusión del mismo.
- Detrás de estos correos suele haber una persona u organización interesada en obtener direcciones de correo válidas para posteriormente enviarles spam.

5. INGENIERÍA SOCIAL. FRAUDES INFORMÁTICOS.

5.3. CORREOS MILLONARIOS

- Otra forma de estafa informática muy común es la denominada "estafa nigeriana", que consiste en el envío de correos prometiendo a los usuarios que pueden hacerse ricos fácilmente.
- Recibe ese nombre porque, en un principio, eran mensajes que simulaban proceder de Nigeria.
- Actualmente, los reclamos son muy diversos: desde un millonario que ha fallecido sin dejar herederos y de cuya herencia las víctimas recibirán una parte si pagan una cantidad de dinero, hasta un premio de lotería que se ha ganado (sin haber participado), pasando por el envío de dinero a un familiar que está en el extranjero, etc.

6. MEDIDAS DE PROTECCIÓN CONTRA EL MALWARE

- En la actualidad podemos encontrar especímenes que aprovechan **vulnerabilidades** que presentan los dispositivos **móviles**, las **tablets** o incluso **televisores** de última generación que utilizan Internet.
- Muchas personas son conscientes de la importancia de utilizar algún mecanismo que les proteja contra las acciones de personas no autorizadas y, aunque muchos conocen la existencia de los **antivirus** y tienen uno **instalado** en sus equipos, pocos son conscientes de que es vital mantenerlos **actualizados** o de que existen otros mecanismos que contribuyen a mejorar la seguridad.
- Hay que **establecer mecanismos** que protejan a los equipos informáticos contra los efectos del malware.

6. MEDIDAS DE PROTECCIÓN CONTRA EL MALWARE

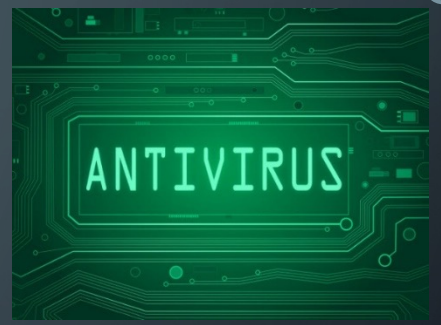
- Existe una gran variedad de herramientas desarrolladas con esta finalidad. **Según su momento de actuación**, distinguimos dos grupos de medidas contra el malware:
  - **Medidas preventivas**, que tratan de evitar infecciones por malware.
  - Y **medidas paliativas**, que minimizan el impacto producido por una infección.

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

- Son el **conjunto de acciones** que los usuarios realizan para evitar infecciones por malware.
- **Detectan y previenen** un incidente de seguridad.
- Además, no solo son las medidas que **previenen contra el malware**, sino también las medidas que previenen **contra otras amenazas** como **accesos no autorizados** o la utilización inadecuada de **recursos** del sistema.
- Nos ocuparemos de las herramientas que evitan que los sistemas se infecten con malware, como **antivirus**, **antispyware**, **antirootkit**, etc. y que se suelen llamar **herramientas antimalware**.

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

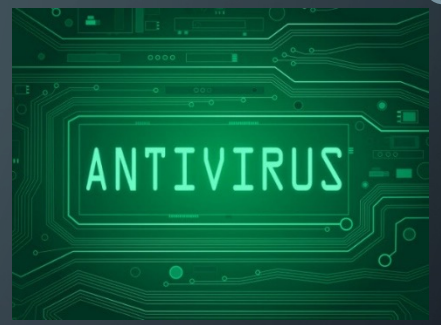
7.1. SUITES DE SEGURIDAD



- Un **antivirus** es, tal vez, la medida de protección más conocida entre los usuarios.
- Se trata de un **programa** desarrollado con una **doble finalidad**: por un lado, permite evitar infecciones por malware y, por otro, sirve para desinfectar los equipos afectados.
- La aparición de nuevas amenazas ha hecho que los antivirus hayan **evolucionado** y sean capaces de reconocer otros tipos de malware, como **spyware**, **rootkits**, etc. y han pasado a llamarse **suites de seguridad**.

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

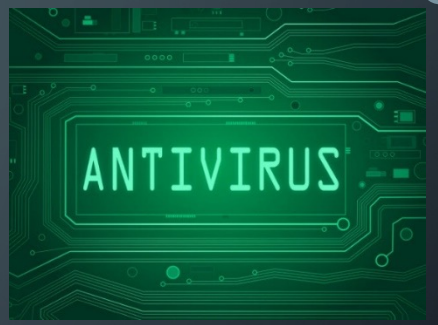
7.1. SUITES DE SEGURIDAD



- Estos programas **combaten** el malware de **dos formas**:
- **Protegiendo** el equipo, en **tiempo real**, contra la instalación de malware, **escaneando** todos los datos procedentes de la red en busca de malware y bloqueando todo lo que suponga una amenaza.
- **Detectando** y **eliminando** malware, que ya ha sido instalado en el equipo. Para ello, escanean el contenido del registro de Windows, los archivos del sistema operativo, la memoria y los programas instalados en el ordenador.
- Las suites de seguridad detectan malware mediante la **comparación con firmas de su base de datos** o mediante **métodos heurísticos** (deduciendo si el equipo está infectado por otros medios).

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

7.1. SUITES DE SEGURIDAD



7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

7.2. CORTAFUEGOS

- Son dispositivos de **software o hardware** que forman parte de un equipo o dispositivo de una red y están diseñados para proteger dicho sistema **bloqueando accesos no autorizados** y **permitiendo** solo los que deban ser permitidos cumpliendo con las **directrices** definidas en la política de seguridad de la organización.
- Todos los mensajes que entren o salgan del equipo o la red pasan a través del cortafuegos, **que examina cada mensaje** y bloquea aquellos que no cumplen los criterios de seguridad especificados.
- Los cortafuegos suelen definir una **política por defecto** que se aplica sobre todos los paquetes que llegan a ellos. Distinguimos dos tipos de políticas: políticas **permisivas** y políticas **restrictivas**.

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

7.2. CORTAFUEGOS

- **Políticas permisivas**: se deniega explícitamente el acceso a la red por parte de algunas aplicaciones, servicios, equipos o redes, permitiéndose el acceso al resto de aplicaciones.
- **Políticas restrictivas**: por defecto está prohibido el acceso a los recursos del sistema, debiendo autorizarse de forma explícita y caso a caso.
- Además de la **política por defecto**, la mayoría de cortafuegos **definen reglas** que son un conjunto de **condiciones** que deben cumplir los mensajes para que el firewall permita o rechace su paso.

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

7.2. CORTAFUEGOS

Se puede clasificar los cortafuegos atendiendo a diferentes criterios, como su ubicación y su modo de funcionamiento.

Según el **lugar en que se ubica el cortafuegos**, podemos diferenciar entre:

- **Cortafuegos de equipo o de host**:

Se instala en el equipo que se desea proteger. Analiza todo el tráfico que llega al equipo o sale de él y permite establecer qué aplicaciones pueden enviar y recibir información a través de la red.

- **Cortafuegos de red o perimetral**:

Se ubica en un punto de entrada común a la red, como un router y actúa como barrera entre la red interna y la externa.

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

7.2. CORTAFUEGOS

Según su **funcionamiento**, podemos clasificar los siguientes tipos:

- **Cortafuegos de filtrado de paquetes**: filtran el tráfico mirando únicamente direcciones IP de origen y destino, puertos TCP/UDP o protocolo usado.
- **Cortafuegos de aplicación**: actúan sobre la capa de aplicación del modelo OSI.
- **Cortafuegos de estado**: realiza un seguimiento del estado de las conexiones de red. El cortafuegos está programado para distinguir paquetes legítimos para diferentes tipos de conexiones. Solo los paquetes que coincidan con una conexión activa conocida serán permitidos.

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

7.3. PROTECCIÓN DEL CORREO ELECTRÓNICO

- Una de las **principales formas de propagación** utilizadas por el malware es el correo electrónico.
- Tenemos que ser conscientes de que cualquier correo recibido puede contener **archivos adjuntos** que incluyan software malicioso y que, aunque quien nos envíe el correo electrónico sea un conocido, existe riesgo al utilizar los archivos adjuntos en los correos puesto que esa persona puede habernos enviado un archivo infectado sin saberlo.
- Podemos ser víctimas del **robo** de nuestra cuenta de correo, que es una práctica muy extendida y lucrativa en la actualidad.
- Los atacantes utilizan una gran cantidad de métodos, generalmente basados en **técnicas de ingeniería social**, para obtener acceso a cuentas de correo existentes y suplantar la identidad de las víctimas.

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

7.3. PROTECCIÓN DEL CORREO ELECTRÓNICO

Ahora vamos a ver algunas medidas que podrían protegernos contra el malware en correos electrónicos:

- **PRUDENCIA**: ante todo, la medida básica a observar es actuar con prudencia antes de abrir **archivos adjuntos**, aunque el emisor sea de confianza. Si se quiere verificar la seguridad de un archivo adjunto antes de abrirlo, se recomienda guardar el archivo adjunto en una carpeta y **pasar un antivirus** sobre esa carpeta antes de abrirlo.
- **ANTIVIRUS**: configurar el correo para que el antivirus compruebe los mensajes.

7. MEDIDAS PREVENTIVAS CONTRA EL MALWARE

7.3. PROTECCIÓN DEL CORREO ELECTRÓNICO

- **REENVÍOS**: no reenviar un mensaje sin antes borrar la lista de direcciones de correo electrónico, provenientes de anteriores reenvíos, que se van arrastrando de unos mensajes a otros, y **NO reenviar** mensajes que formen parte de cadenas.
- **ENLACES**: no hacer clic en las direcciones web que aparecen en un correo electrónico a no ser que el correo sea de confianza.
- **INFORMAR**: denunciar el correo abusivo o fraudulento informando al titular del correo desde donde ha partido el mensaje.

8. MEDIDAS PALIATIVAS CONTRA EL MALWARE

- Las **medidas de seguridad paliativas o correctoras** contra el malware constituyen todo el **conjunto de acciones que los usuarios realizan para eliminar malware que ha conseguido infectar al equipo**.
- A este tipo de medidas también se las suele denominar como **medidas de seguridad pasivas**.
- Algunas medidas de seguridad paliativas son las **copias de seguridad**, el software **congelador**, los sistemas **RAID** o las herramientas de **recuperación de datos** borrados.
- Es importante mencionar que **no existe una solución mágica** ante una infección o incidente de seguridad.
- Por ello, en cada caso, deberá estudiarse la gravedad y el alcance de la infección para decidirse por una opción u otra. Para estar informado de las últimas amenazas y la forma más conveniente de desinfección se propone la **suscripción a listas de distribución de seguridad**.

8. MEDIDAS PALIATIVAS CONTRA EL MALWARE

8.1. COPIAS DE SEGURIDAD

- Son una medida de seguridad paliativa muy **importante** y que consiste en guardar una parte o toda la información del sistema para poder recuperarla en el caso de que se haya producido una pérdida de la información.
- Es muy importante que la información salvaguardada se encuentre **almacenada en un dispositivo diferente del original**. Se distinguen copias de seguridad del **sistema** que permiten restaurar un equipo y de **datos** que permiten restaurar algunos ficheros.

8. MEDIDAS PALIATIVAS CONTRA EL MALWARE

8.2. SOFTWARE CONGELADOR

- El **software "congelador"** es un software especial, del tipo **"reinicie y restaure".** Recibe su nombre de la traducción literal del inglés "freezer".
- Cuando se instala, **permite "congelar" el estado del equipo** en un momento determinado, con la configuración y contenidos exactos que el equipo tenía en ese momento.
- Cada vez que se inicie el equipo, estará en el mismo estado en el que quedó "congelado".
- Permite al usuario realizar acciones como instalar programas, realizar cambios en la configuración, enviar y recibir correos, recordar contraseñas, etc. y, al reiniciar el equipo, todos estos datos se pierden y este vuelve al estado en que quedó "congelado".

8. MEDIDAS PALIATIVAS CONTRA EL MALWARE

8.2. SOFTWARE CONGELADOR

- La congelación es una medida de protección que **se utiliza habitualmente en ordenadores a los que acceden muchas personas**.
- No obstante, hay que tener en cuenta que **la información generada por los usuarios en cada sesión será automáticamente eliminada al reiniciar el equipo**, por lo que para almacenarla hay dos opciones: usar **dispositivos externos** de almacenamiento (pendrive, nube, etc.) o **particionar** el disco y "congelar" únicamente una de las particiones.

9. CENTROS DE PROTECCIÓN Y RESPUESTA FRENTE A AMENAZAS

- El mundo del malware **evoluciona** constantemente y cada día surgen **nuevas amenazas** que conviene conocer y de las que conviene estar protegidos.
- Para satisfacer esta necesidad de **informar a los usuarios** y proporcionarles **mecanismos** para protegerse frente a amenazas relacionadas con el malware surgen los centros de **información y respuesta ante amenazas e incidencias de seguridad**, como por ejemplo **CERT o CSIRT**, entre otros.
- Estos centros son **organismos** compuestos por **expertos** en desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

9. CENTROS DE PROTECCIÓN Y RESPUESTA FRENTE A AMENAZAS

- Estos organismos **estudian** el estado de seguridad global de redes y ordenadores, **proporcionan** servicios de respuesta ante incidentes a víctimas de ataques en la red, **publican** alertas relativas a amenazas y vulnerabilidades y ofrecen información que ayude a mejorar la seguridad de estos sistemas.
- Por tanto, **ofrecen dos tipos de servicios**: **preventivos y reactivos**.

9. CENTROS DE PROTECCIÓN Y RESPUESTA FRENTE A AMENAZAS

- **PREVENTIVOS**:
  - **Avisos** de seguridad.
  - **Búsqueda** de **vulnerabilidades.**
  - **Auditorías** o evaluaciones de seguridad.
  - **Configuración** y **mantenimiento** de herramientas de seguridad, aplicaciones e infraestructuras.
  - **Desarrollo** de herramientas de seguridad.
  - Propagación de **información** relacionada con la seguridad.

9. CENTROS DE PROTECCIÓN Y RESPUESTA FRENTE A AMENAZAS

- **REACTIVOS**:
  - **Gestión de incidentes de seguridad** (análisis, respuesta, soporte y coordinación de incidentes de seguridad).
  - **Gestión de vulnerabilidades** (análisis, respuesta y coordinación de vulnerabilidades detectadas).

10. BUENAS PRÁCTICAS PARA PROTEGERSE DEL MALWARE

- Ya hemos visto que no existe un sistema totalmente seguro, pero que se pueden **minimizar los riesgos** llevando a cabo unas prácticas seguras que siempre se basan en el sentido común y que, en muchos casos afectan al **eslabón de seguridad más débil y más frecuentemente olvidado: las personas que utilizan el sistema.**
- Habitualmente **las infecciones** no **se producen** por tener más o menos herramientas de seguridad, sino **por el uso que se hace del sistema** o las **decisiones** que se toman al navegar por Internet o abrir un mensaje de correo electrónico.

10. BUENAS PRÁCTICAS PARA PROTEGERSE DEL MALWARE

- Entre las medidas de protección que se pueden llevar a cabo, están las siguientes:

Recomendaciones frente al malware	
Actualizar el sistema operativo y aplicaciones	Es fundamental actualizar periódicamente el sistema operativo y todas las aplicaciones, especialmente las críticas (navegador web y sus plugins).
Protección antimalware	Se debe instalar una suite antimalware, así como un cortafuegos, y mantenerlos actualizados, configurándolos para que se actualicen automáticamente. También podría ser conveniente la utilización de un sistema de detección y prevención de intrusos IDS/IPS.
Cuentas de usuario	Conviene usar cuentas de usuario con privilegios limitados para el uso diario del equipo y utilizar la cuenta de administrador solo cuando sea necesario cambiar la configuración o instalar un nuevo programa.

10. BUENAS PRÁCTICAS PARA PROTEGERSE DEL MALWARE

Recomendaciones frente al malware	
Políticas de contraseñas	Se deben diseñar políticas que incluyan la definición de contraseñas complejas, tanto para usuarios del equipo como para aplicaciones en red.
Datos personales y claves	Es muy importante no facilitar datos personales ni claves, ni códigos PIN solicitados por correo electrónico u otro medio (SMS, teléfono, etc). Esta información solo deberíamos introducirla en páginas web en las que estemos seguros de su procedencia y que establezcan un canal de comunicación seguro como https.
Precaución al navegar	No se debe navegar por páginas web sospechosas, no confiables o que ofrezcan regalos o promociones dudosas. También se recomienda desactivar la interpretación de Visual Basic Script y únicamente permitir JavaScript, ActiveX y cookies en páginas web de confianza.

10. BUENAS PRÁCTICAS PARA PROTEGERSE DEL MALWARE

Recomendaciones frente al malware	
Correo electrónico	Se deben observar las recomendaciones expuestas en el apartado de correo electrónico de esta unidad.
Instalación de aplicaciones	Se debe tener precaución al instalar o ejecutar programas procedentes de Internet, así como evitar la descarga de software de redes P2P, pues se desconocen su contenido y procedencia reales. Debemos pasar el antivirus a los medios extraíbles, como memorias USB antes de utilizarlos, ya que son una fuente de propagación de malware muy común.
Reciclaje constante	Los administradores de sistemas deben mantenerse actualizados: suscribiéndose a boletines de seguridad, consultando periódicamente webs de información (la del CERT por ejemplo), etc.
Copias de seguridad	Se deben hacer regularmente copias de respaldo a medios extraíbles de los documentos importantes para poderlos recuperar en caso de infección.
Otras medidas	Otras posibles medidas son la realización periódica de auditorías de seguridad y la concienciación de los usuarios en cuestiones de seguridad informática.

11. BIBLIOGRAFÍA

- Seguridad Informática. G.Escrivá, R.Romero y otros. Ed.Macmillan Profesional.
- Seguridad Informática. I.Triviño. Ed.Síntesis.