Amenazas y Seguridad del Software.

Caso Práctico

Juan acaba de recibir un correo y al abrirlo ha visto que su ordenador no cesa de enviar datos a internet, tanto que casi no puede navegar.

Supuestamente era un mensaje de la red social Facebook, donde le indicaban que alguien había escrito en su muro. Desde el mismo correo entró en una página web que aparentemente era igual que Facebook, e introdujo su usuario y contraseña. Pero, no entró realmente ya que le daba problemas. Dejó de intentarlo pero desde entonces nada parece ir bien, incluso han mandado mensajes a sus amigos de Facebook ofreciéndoles trabajo, supuestamente el mensaje venía desde su muro...

Juan le comenta este problema a su amigo Iván.

- Hombre, ¿no comprobaste la dirección URL? –le dice Iván.

- Pues no, no se me ocurrió, todo parecía tan normal…Voy a mirar en el historial, a ver dónde me conecté.

-¿Lo has encontrado ya? ¿En qué página diste tu usuario y contraseña de Facebook? –pregunta Iván.

- En "www.facebobk.com", fíjate sólo es una "b" en lugar de una "o" –aprecia Juan.

- Sí, está bien pensado, para engañar, claro.

- ¿Crees que te llevará mucho arreglarlo? –pegunta Juan.

- Pues, no lo sé, estoy un poco mosqueado porque al mismo tiempo he recibido un e-mail del equipo de Gmail que dice que han detectado un correo que venía a mi dirección de la empresa de transportes NHLtranservis, desde la dirección de correo support.s.nr4575@dhl.com, que contenía virus en un fichero adjunto y que no lo han dejado pasar. El caso es que yo no espero ningún envío de ninguna empresa.

- ¿No tendrás la misma contraseña en el Facebook que en la cuenta de correo? –pegunta Juan.

- Sí, es la misma, con lo que me cuesta recordar una, no voy a poner dos distintas –se excusa Iván.

- Pues entonces te han capturado también el correo –concluye Juan.

- Ya, algo así debe pasar, por cierto ¿para qué me llamabas? –recuerda Iván.

- Nada, déjalo, ya te lo cuento otro rato, veo que estás liado.

Se despiden.

- Vale. Hasta luego Iván.

- Hasta luego Juan.

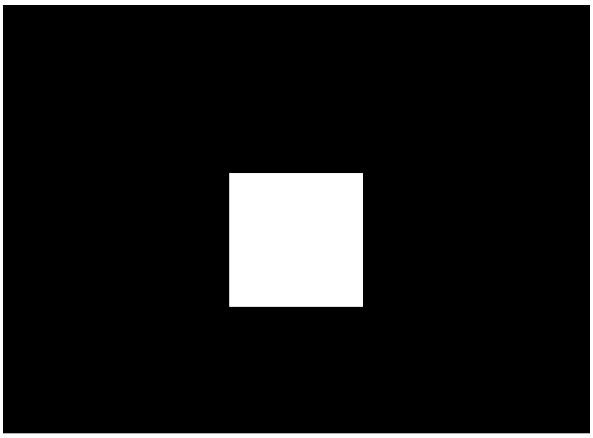
Para saber más

En el siguiente enlace dispones de un artículo publicado en "El Mundo" en el cuál la CNMV advierte de un ataque en el cuál se suplanta su dominio y su imagen.

Suplantación del dominio y la imagen de la CNMV

Debes conocer

La siguiente presentación trata sobre los contenidos fundamentales que se tratarán a lo largo de todo el tema. Es interesante que veas esta presentación para hacerte una idea de lo que vas a aprender en la presente unidad



00:00 00:29

Caso Práctico

Juan e Iván están chateando.

-Oye, Juan, que no me puedo conectar a Genbeta, mira a ver s tú te conectas, quería leer un artículo titulado "El viejo Twitter está a punto de desaparecer" y nada, que no entro en la página, ¿tú puedes entrar? –dice Iván.

-Bueno, he conseguido entrar en la página pero no llego al artículo que dices. No está funcionando bien, creo que es problema suyo –responde Juan.

-Pero si Genbeta es un Weblog colectivo dedicado al software y los servicios vía Internet, con toda la actualidad y los mejores trucos. No creo que tengan problemas en su página, será otra cosa –propone Iván.

-¡Ah!, todo el mundo tiene problemas, sobre todo si publicas artículos para "desenmascarar" a los ladrones de contraseñas y cuentas –se lamenta Juan.

-¿Cómo es eso?

-En noviembre del año pasado publicaron en Genbeta una nota sobre servicios para saber quién te tiene añadido en el Messenger que, en realidad, lo que hacen es recolectar usuarios y contraseñas para usarlos con fines dudosos. Enseguida el artículo empezó a indexar muy bien en Google y recibieron en Genbeta una serie de amenazas para quitarlo o sufrirían un ataque DDoS o denegación de servicio –explica Juan.

-¿Y cumplieron su amenaza? –pregunta intrigado Iván.

-La amenaza se cumplió. Empezaron un domingo a atacar y dejaron la página sin acceso continuo, o sea, que a ratos funcionaba, a ratos no, así durante cuatro días.

-Los días que tardó el proveedor de hosting en resolverlo –supone Iván.

-Qué va, qué va, el viernes ya estuvieron cuatro horas sin servicio en absoluto y entonces el proveedor de hosting les cerró la página por precaución. No fuera a ser que atacaran más páginas web en sus servidores –dice Juan.

-Pero no lo entiendo, sólo estaban atacando un sitio, por qué el ISP tomó esa medida tan radical –se sorprende Iván.

-Porque ese mismo viernes fueron atacadas otras páginas, entre ellas error500.net –recuerda Juan.

Introducción.

Cada vez que visitas una página web se produce un intercambio de información entre tu equipo y la red. Este intercambio es necesario para que puedas acceder a la información y servicios web, pero ¿cuánta información estás enviando? Si no tienes **control** sobre la información que desde tu ordenador se envía a Internet puede causarte **problemas**, pues alguien puede utilizar esa información sin que tú lo sepas.

La información que trasmites cuando navegas por la Web es variada, para empezar tu dirección **IP** (acrónimo Internet Protocol, en inglés protocolo de internet), es decir, nuestra identificación en ese momento, además de la dirección IP de tu máquina, también estás enviando los **lugares** de la página Web donde has hecho clic. Toda esta información junta puede dar una idea del **perfil de persona** que eres a alguien que tú ni siquiera conoces.

Citas para pensar

"Siempre que vayas a atacar y a combatir, debes conocer primero los talentos de los servidores del enemigo, así puedes enfrentarte a ellos según sus capacidades".

DU MU escritor chino de la dinastía Tang. 802-852 d.C. Comentarios a "El arte de la guerra"

Si la persona que hace la recopilación de tu información es un aprendiz de hacker, con tu dirección IP puede intentar una denegación de servicio, es decir, te envía un gran volumen de información que tu ordenador no es capaz de asimilar, por lo que no puedes navegar. La idea es **como el niño pequeño** que repite una y otra vez a su madre:
-¿Puedo ir? ¿Puedo ir? ¿Puedo ir? ¿Puedo ir? ...
En realidad para el niño no supone ningún esfuerzo repetir lo mismo muchas veces pero para la madre es una entrada continua de datos que recibe de su hijo que no le deja hacer otra cosa, más que contestar:
-No, no, no, no...

Pues el ataque DDOS es lo mismo. A tu ordenador le llega infinidad de datos desde la red y el contestar y administrar esta información le **roba tiempo**, tiempo que no puede dedicar a enviar la solicitud de página web que tú estás haciendo.

Ningún dispositivo, incluso los teléfonos móviles, puede sufrir un ataque por lo que es importante minimizar las posibilidades de que esto ocurra. En esta unidad y en la siguiente aprenderás que hay herramientas para proteger tu equipo.

Reflexiona

¿Te has parado a pensar alguna vez cuánta información sale de tu ordenador? Si utilizas tu ordenador para conectarte a una red social, para jugar y ver películas, además de leer el correo, entonces ¿Cuánta información tuya personal hay en el ordenador? ¿Sólo tienes instalados los juegos y aplicaciones que son seguros? ¿Se te ha instalado alguna barra de información en el navegador que no sabes cómo quitar? ¿Podría alguna de ellos estar enviando información de la actividad de tu ordenador?

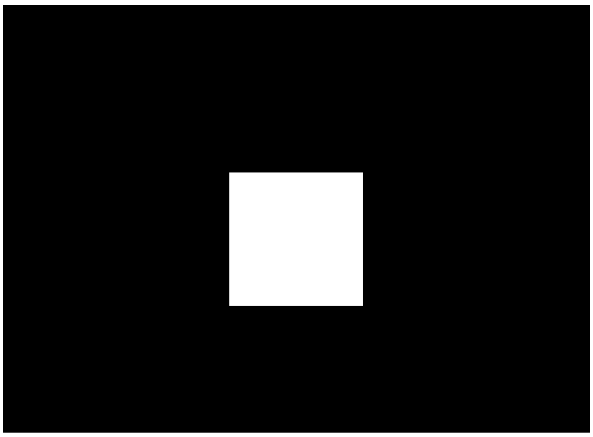
Software que vulnera la Seguridad.

En torno al año 1300 antes de Cristo, los griegos cercaban Troya, ese cerco duró diez años. Después de tanto tiempo los griegos idearon una nueva treta: un gran **caballo** de madera hueco que construyeron de forma que cupieran dentro algunos soldados griegos. La armada griega fingió partir y un espía griego convenció a los troyanos de que el caballo era una **ofrenda** a Atenea. Los troyanos vieron partir a la armada griega y aceptaron el regalo, así que el caballo entró en la ciudad en medio de una gran celebración y, cuando la ciudad entera estaba bajo el sueño de la bebida, **los guerreros griegos salieron del caballo** y abrieron las puertas de la ciudad para permitir la entrada al resto de las tropas. Así fue como Troya fue derrotada y saqueada sin piedad alguna. En el caso de los ordenadores, Troya son nuestros datos, es el núcleo que nosotros queremos proteger y los griegos son las innumerables amenazas que se ciernen sobre el software y la información.
Estas amenazas suelen venir escondidas, como los guerreros Griegos, y son tantas que tienen una difícil clasificación, aunque podemos hablar de dos grandes tipos: **Código malicioso** e **ingeniería social.**

a. **Código malicioso.** Es más conocido como Malware, palabra inglesa abreviatura de “Malicious software”que **significa** software diseñado para interferir en el normal funcionamiento del ordenador.

Debes conocer

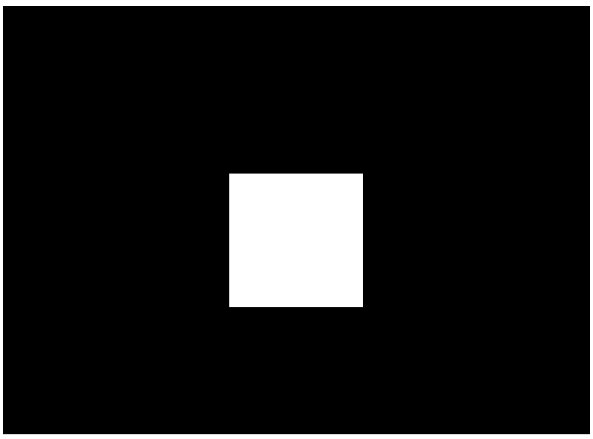
La siguiente presentación trata sobre código malicioso:



b. **Ingeniería Social**. Ingeniería Social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. En la práctica, un ingeniero o ingeniera social usará comúnmente el teléfono o Internet para engañarte, fingiendo ser, por ejemplo, un empleado o empleada de algún banco o alguna otra empresa, un compañero o compañera de trabajo, un cliente o una clienta. Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o envíos falsos que solicitan respuestas e incluso las famosas "**cadenas**", llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. Con este método, los ingenieros e ingenieras sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, por ejemplo, ¿Proporcionarías detalles financieros a un aparente funcionario o funcionaria de un banco?

Debes conocer

La siguiente presentación trata sobre ingeniería social:



00:00 02:13

Autoevaluación

¿Qué es un certificado digital?

- ○ Un certificado firmado y sellado en papel, escaneado.
- ○ Elemento de seguridad por el que un tercero de confianza garantiza que la página es realmente de la entidad que dice ser.
- ○ Elemento de seguridad por el que la propia página web garantiza que la página es realmente la entidad que dice ser.
- ○ Un certificado de un tercero, es decir, de otra empresa, firmado y sellado en papel y escaneado.

No es correcta porque no se trata de un papel escaneado, es una firma digital sobre una página web, no hay ningún papel.

Correcta, es la forma de garantizar que la página es legítima. Hay empresas como VeriSign que emiten certificados de la validez de una página, así el usuario está seguro.

Incorrecta, la misma empresa no se puede certificarse a sí misma.

Falso. No es un papel sino es digital. Es un elemento que se instala en el navegador, demostrando tu confianza en esa empresa pues lo garantiza otra empresa de tú confianza.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

Vulnerabilidad del Software.

A veces te habrás preguntado quién escribe los programas, y como probablemente ya sepas, los escriben personas. Llamamos Software a un conjunto de programas o aplicaciones que realizan las tareas para las que fueron creados en el ordenador. La más importante de todas las aplicaciones es el sistema operativo que nos asiste en la comunicación de las personas con el equipo, puesto que los archivos almacenados se localizan fácilmente. Por otro lado, el sistema operativo realiza tareas y administra los recursos propios y adicionales de los que el ordenador dispone. Ahora bien, estos programas, incluido el sistema operativo, se van perfeccionando a lo largo del tiempo de forma que la actualización de los mismos es una tarea habitual del técnico o técnica de ordenadores.

El software es creado para realizar una tarea en concreto, que puede ser sencilla, por ejemplo, una calculadora o muy complicado y diverso, por ejemplo, un procesador de textos.

¿Cómo puedes saber si el software instalado en tu equipo es vulnerable o no?

Algunas tareas de mantenimiento del software son:

- **Actualizar**: El software en sí mismo puede tener errores de programación, y éstos no suelen ser provocados, sino que los programadores no han tenido en cuenta un factor que hace que el software deje una puerta abierta a la entrada de intrusos. Para prevenir cualquier **BUG** (en inglés insecto) o agujero de seguridad tienes que tener actualizado el software.
- **Configurar**: Por otra parte, también está de tu lado el instalar el programa correctamente. Para ello, te conviene leer las instrucciones y los archivos **leeme.txt** para una correcta instalación y configuración de los mismos.
- **Parchear**: Cuando los programadores y programadoras reciben información de fallos de seguridad en sus programas proceden a parcharlos, es decir, a modificar parte del código del programa para evitar ese fallo. Una vez hecho esto crean los parches de seguridad y los ponen a disponibilidad de la clientela.
- **Desconfiar**: Muchas veces habrás visto programas gratuitos disponibles para ti, sólo con pulsar en descargar. Estos programas son muy atractivos porque tienen las mismas funciones que los programas de pago, pero suelen llevar código añadido, bien sea instalando pequeñas aplicaciones o dentro del mismo código del programa, introduciendo **fragmentos maliciosos** que ponen en peligro la integridad de tus datos.

Para saber más

SANS es una compañía catalogada como la más fiable y la fuente más extensa de cursos de formación sobre seguridad informática en el mundo. Ofrecen conferencias y cursos a través de diferentes métodos, en directo o virtuales. Y también publican documentos sobre vulnerabilidad. En este enlace, puedes encontrar un artículo del INCIBE (Instituto Nacional de Ciberseguridad) en el que puedes encontrar las 30 mayores vulnerabilidades explotadas por los ciberatacantes.

Las 30 mayores vulnerabilidades explotadas por los ciberatacantes

Ten cuidado cuando descargues programas, a veces incluso un antivirus puede resultar ser un virus, un troyano, un gusano o programas espía (spyware). Esto puede traer problemas a tu equipo de:

- **Integridad**, modificando o borrando datos.
- **Disponibilidad**, impedir el acceso de usuarios con permiso de acceso.
- **Confidencialidad**, divulgando tus contraseñas.

Autoevaluación

¿Qué es un bug?

- ○ Caballo de Troya.
- ○ Virus malicioso.
- ○ Agujero de seguridad.
- ○ Un parche.

No es correcta porque no se trata de un fragmento de código malicioso introducido a propósito dentro de otro programa.

Incorrecta, porque no se trata de un programa creado don fines maliciosos.

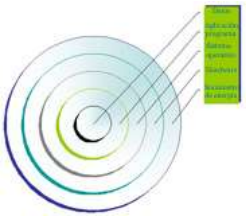
Muy bien. Significa insecto en inglés pero se refiere a un error de programación.

No es la respuesta correcta porque es la solución a los bugs, pero no la definición de éstos.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Tipos de Ataques.



Fíjate cuántas dependencias tienes en tú ordenador. Si te acabas de comprar un ordenador, tendrás que enchufarlo para encenderlo. Al encenderlo, la BIOS tendrá que estar bien configurada para **reconocer** el hardware. Después necesitas un **gestor de arranque** si tienes varios sistemas operativos, y por supuesto, el sistema operativo y los programas. Los sistemas informáticos usan una **diversidad de componentes**, por ejemplo, utilizan electricidad para suministrar alimentación al hardware o instalan multitud de programas una vez instalado el sistema operativo.

Los **ataques** te pueden suceder en **cada eslabón** de esta cadena, siempre y cuando exista una vulnerabilidad que pueda aprovecharse. El esquema que figura a continuación repasa brevemente los distintos niveles que revisten un riesgo para la seguridad: datos, aplicaciones, sistema operativo, hardware y suministro de energía.

Tipos de ataque sobre los sistemas informáticos.

Acceso físico: en este caso, el atacante tiene acceso a las instalaciones e incluso a los equipos:

- Interrupción del suministro eléctrico.
- Apagado manual del equipo.
- Vandalismo.
- Apertura del equipo y robo del disco duro.
- Monitoreo del tráfico de red.

Denegaciones de servicio: el objetivo de estos ataques reside en interrumpir el funcionamiento normal de un servicio. Por lo general, las denegaciones de servicio se deben a la explotación de las:

- Debilidades del protocolo TCP/IP.
- Vulnerabilidades del software del servidor.

Ingeniería social: En la mayoría de los casos, el eslabón más débil es el usuario o usuaria. Muchas veces, por ignorancia o a causa de un engaño, genera una vulnerabilidad en el sistema al brindar información (la contraseña, por ejemplo) al pirata informático o al abrir un archivo adjunto. Cuando ello sucede, ningún dispositivo puede proteger al usuario o usuaria contra la falsificación: sólo el sentido común, la razón y el conocimiento básico acerca de las prácticas utilizadas pueden ayudar a evitar este tipo de errores.

Intrusiones:

- Análisis de puertos.
- Elevación de privilegios: este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada por su diseñador). En ciertos casos, esto genera comportamientos atípicos que permiten acceder al sistema con derechos de aplicación. Los ataques de **desbordamiento de la memoria intermedia (búfer)** usan este principio.
- Ataques malintencionados (virus, gusanos, troyanos).

Intercepción de comunicaciones:

- Secuestro de sesión.
- Falsificación de identidad.
- Redireccionamiento o alteración de mensajes.

Puertas trampa: Son puertas traseras ocultas en un programa de software que brindan acceso a su diseñador o diseñadora en todo momento.

Como ya hemos dicho, los errores de programación de los programas son corregidos con bastante rapidez por su diseñador o diseñadora, apenas se publica la vulnerabilidad. En consecuencia, queda en tus manos estar al día acerca de las actualizaciones de los programas que usas a fin de limitar los riesgos de ataques.

Además, existen ciertos dispositivos (firewalls, sistemas de detección de intrusiones, antivirus, etc.) que brindan la posibilidad de aumentar el nivel de seguridad.

Para saber más

La Asociación de Internautas fundada en 1998 tiene una página web contra el fraude y la seguridad en internet, está actualizada y tiene muchos ejemplos de todos los tipos de ataques. En un artículo reciente, se habla de un ataque DDoS masivo que ha afectado a grandes sitios como Twitter.

Un ataque DDoS masivo afecta a grandes sitios como Twitter, Spotify y GitHub

Atacantes.

¿Qué es un hacker? (inglés, divertirse con el ingenio). Seguramente, si alguien te dice que eres un "**hacker**" lo interpretas como pirata informático. Y seguro que conoces a más de una persona que ha sufrido algún desastre en su ordenador proveniente de estos hackers. Cuando esto ocurre, pensamos en piratas informáticos como: personas con mucha experiencia que han estudiado en detalle nuestros sistemas y entonces han sacado provecho de alguna vulnerabilidad. Pero no siempre es así. Hay muchos tipos de atacantes o piratas:

¿Hay diferentes tipos de piratas? En realidad existen varios tipos de "***atacantes***" divididos en categorías de acuerdo a sus experiencias y motivaciones.

- Los "**hackers de sombrero blanco**", hackers en el sentido noble de la palabra y cuyo objetivo es ayudar a mejorar los sistemas y las tecnologías informáticas, son casi siempre los responsables de los protocolos informáticos y las herramientas más importantes usadas actualmente, por ejemplo, el correo electrónico.
- Los "**hackers de sombrero negro**", más comúnmente llamados ***piratas***, son personas que irrumpen en los sistemas informáticos con propósitos maliciosos:
  - Los "script kiddies" (guiones o programas para niños) son jóvenes usuarios y usuarias de la red que utilizan programas que han encontrado en Internet, casi siempre de forma incompetente, para dañar sistemas informáticos por diversión.
  - Los "**phreakers**" (de las palabras phone, teléfono en inglés, y freak, monstruo en inglés) son piratas que usan la red telefónica conmutada (**RTC**) para hacer llamadas gratis a través de circuitos electrónicos (llamados *cajas*, como la *caja azul*, la *caja violeta*, etc.) que conectan a la línea telefónica para manipular su funcionamiento.
  - Los "**carders**" (Inglés tarjetistas) principalmente atacan sistemas de tarjetas inteligentes (en especial **tarjetas bancarias**) para entender su funcionamiento y aprovechar sus vulnerabilidades.
  - Los "**crackers**" (inglés *crack*, **romper**) no son galletitas de queso sino personas que crean herramientas de software que permitan el ataque de sistemas informáticos o el craqueo de la **protección anticopia** del software con licencia. Por consiguiente, el "crack" es un programa ejecutable creado para modificar (o *actualizar*) el software original con el fin de quitarle su protección.

- Los "**hacktivistas**" (contracción de *hackers* y *activistas*) son hackers con motivaciones principalmente **ideológicas**. Este término ha sido muy usado por la prensa para transmitir la idea de una comunidad paralela (en general llamada ***underground***, en referencia a las poblaciones que vivían bajo tierra en las películas de ciencia ficción).

De hecho, estos tipos de distinciones no son muy claras ya que algunos *hackers de* ***sombrero blanco*** han sido alguna vez *hackers de sombrero negro* y viceversa. Es común ver a usuarios de listas de distribución y foros discutiendo sobre la diferencia que debería hacerse entre un *pirata* y un *hacker*. El término ***trol*** se usa en general para referirse a temas delicados que buscan provocar reacciones intensas. Por ejemplo: **¿Windows es mejor que Linux?**

Tipos de Hackers

Sombrero negro (piratas).	Sombrero blanco (hackers).
El atractivo de lo prohibido; interés financiero; interés político; interés ético; deseo de reconocimiento; venganza; deseo de dañar (destruir datos, hacer que un sistema no funcione).	Aprender; optimizar los sistemas informáticos; probar las tecnologías hasta el límite para llegar a un ideal más eficiente y fiable.

Autoevaluación

¿Es fácil distinguir a un hacker de un pirata?

- ○ Verdadero.
- ○ Falso.

Incorrecto. Creo que no has leído el texto con atención, ¿verdad?

Claro que no es fácil, a veces les separa una delgada línea.

Solución

1. Incorrecto
2. Opción correcta

Fraude en Internet.

Ya estás familiarizado o familiarizada con quién y cómo puede atacar tu equipo, acceder a la información que en él tienes almacenada o dañar parte del sistema. El software, por tanto, se ve amenazado desde diferentes puntos como el correo electrónico, la mensajería instantánea y los dispositivos extraíbles. No has de olvidar que actualmente en lo que se dibuja como una nube, es decir Internet, se está convirtiendo en un punto de encuentro y de almacenamiento de muchas personas y empresas. Estos nuevos focos de información son un objetivo de los ciberdelincuentes. ¿Cuáles son las vías más habituales de ataque al software?

- **Redes P2P**
  Si un programa está muy solicitado, algunos aprovechan para insertar un programa malicioso en un fichero con el mismo nombre del programa. Además, cracks (Inglés romper) o pequeños programas que convierten en propio un software comercial que no has adquirido, suelen llevar alguna intención más de la que dicen cuando son ejecutados, pues no solo rompen el programa objeto sino que suelen ir acompañados de código malicioso.

- **Páginas web.**
  Navegar por la red supone también un riesgo para el software de nuestro equipo, puesto que existen páginas con dudosa fiabilidad que de forma inadvertida descargan código malicioso en tu ordenador. Lo peor es que también se ha dado casos en los que los hackers han atacado una página web "fiable" y la han convertido en un foco de infección para todos sus visitantes mientras no fue descubierto el ataque.

- **Nombres de dominio.**
  El nombre de dominio de una página web está asociado a una IP, esta asociación es otro punto de ataque. Asociar el nombre de dominio a una IP diferente, casualmente la del ordenador del hacker en la que tiene alojada una página web "copiada" a la original. Así difícilmente podrás percatarte de las pequeñas diferencias entre una y otra, e introduces tu usuario y contraseña, con las que el hacker puede entrar en el sitio verdadero.

- **Redes sociales.**
  Si Facebook tiene almacenados más de 15000 españoles y españolas en su red, un ataque de ingeniería social sobre posibles usuarios de Facebook es una buena idea. Pero no es el único tipo de ataque que puede sufrir puesto que Facebook es, en sí mismo, un programa, por tanto, puede ser también atacado.

- **Web 2.0.**
  La tendencia actual de usuarios y empresas es almacenar la información en algún sistema externo. Por ejemplo, documentos en un disco duro de nuestro ISP. Existen servidores de juegos, de correo electrónico, de redes sociales e incluso del software de una empresa al que se conectan sus ordenadores locales en un **DATACENTER** (inglés centro de datos). Estos Datacenter son, por tanto, un objetivo de los hackers pues allí hay mucha información.

Los delincuentes informáticos **buscan retos** y atacar a las empresas es uno de ellos. Un centro de datos dispone de las mayores medidas de seguridad que existen y romper estas medidas supone poner en peligro la integridad, disponibilidad de los datos y, por supuesto, la privacidad de todos los usuarios y usuarias.

Para saber más

La **Oficina de Seguridad del Internauta** (OSI) de INCIBE proporciona información y soporte para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet. En el siguiente artículo, hablan de cuáles son los fraudes más comunes en Internet:

Fraudes más comunes

Debes conocer

Vídeo-Tutorial de Google for Education en el cuál se hace una introducción sobre seguridad y privacidad en la web:

Introducción sobre Seguridad y Privacidad en la Web para Estudiantes.

http://www.youtube.com/embed/C3Dxx44Us1s

Control de Acceso a la Información.

Caso Práctico

Manuel, el hermano de Juan, visita a su amigo Rodrigo.

-¿Listo para el partido de Tenis? –reta Manuel.

-No del todo. Verás, tenemos en casa una chica extranjera amiga de mi hermana y nos ha pedido utilizar el ordenador para conectarse a Internet –dice Rodrigo.

-Bueno, pues eso no es problema, aquí tienes el ordenador y está conectado a internet. ¡Listo!

-Ya, ya, el caso es que creemos que algo está haciendo mal, pues desde que ella estuvo aquí sentada, no podemos poner un acento a ninguna palabra –dice preocupado Rodrigo.

-Bueno pues habrá cambiado el idioma ¿no?, lo pones en español internacional otra vez y solucionado –propone Manuel.

-Ya lo he intentado, pero eso no está cambiado, debe ser otra cosa.

-¿Crees que está intentando fastidiar el equipo? –pregunta Manuel.

-No, no, que va, creo que simplemente no sabe y como no se atreve a preguntar, pues pincha aquí y allá –responde Rodrigo.

-Bueno pues explícale cómo navegar y arreglado –dice Manuel.

-Ya, está el problema del idioma, la verdad es que no entiende muy bien lo que le dicimos, aunque siempre te contesta amablemente –indica Rodrigo.

-Bueno, pues siéntate aquí con ella -sugiere Manuel- mientras navega y puedes ver qué hace mal.

-Claro, eso podría ser a partir de las ocho, cuando yo llego a casa, pero para entonces ella ya lleva tres horas en casa responde Rodrigo.

-Huf, menudo problema.

Desde el momento en que adquieres un ordenador de sobremesa es recomendable seguir unas buenas prácticas, seguramente ya las conoces, pero vamos a recordarlas:

1. Mantente informado o informada sobre las **novedades** y alertas de seguridad.
2. Mantén **actualizado** tu equipo, tanto el Sistema Operativo como cualquier aplicación que tengas instalada.
3. Haz **copias de seguridad** con cierta frecuencia para evitar la pérdida de datos importante.
4. Utiliza software **legal** pues te ofrece garantía y soporte.
5. Utiliza **contraseñas** fuertes en todos los servicios para dificultar la suplantación de tu usuario (evita nombres, fechas, datos conocidos o deducibles, etc.).
6. Utiliza **herramientas** de seguridad que te ayudan a proteger y/o reparar tu equipo frente a las amenazas.
7. Crea **diferentes usuarios**, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas.
8. Pon una contraseña a la **BIOS**.
9. **Cifra** el contenido del disco duro para evitar el acceso a los datos.
10. **Elimina** datos **innecesarios** que puedan estar almacenados.
11. Si usas GRU como **gestor de arranque**, incluye una contraseña en su configuración para que no sea modificable.

Para saber más

Cómo poner una contraseña a la BIOS o UEFI en Windows 10 para impedir el acceso a nuestro ordenador:

Contraseña en la BIOS o UEFI en Windows 10

En el Sistema Operativo.

Ya hemos hablado de la necesidad de estar actualizados. En el sistema operativo esas **actualizaciones** se suelen llamar "**parches**", pues cada una de las actualizaciones, normalmente, es la respuesta a un problema de seguridad. Si se trata de Windows, Microsoft lanza periódicamente actualizaciones de software de su sistema operativo y, además, actualizaciones del software de otros componentes hardware instalados en él. Para ello, Windows comprueba previamente la licencia de software que posees.

Si tienes dudas de si tu sistema está actualizado o no, puedes utilizar, en el caso de versiones de Microsoft anteriores (como Windows XP y Windows 7) el programa Microsoft Baseline Security Analyzer (**MBSA**). Es una herramienta fácil de usar que te ayuda a determinar tu estado de seguridad de acuerdo con las recomendaciones de seguridad de Microsoft y te ofrece orientación precisa sobre soluciones. Además, mejora el proceso de administración de seguridad si utiliza MBSA, pues detecta errores de configuración de seguridad habituales e identifica las actualizaciones que faltan en tu sistema informático.

En el caso de que emplees versiones de Windows más recientes, como Windows 10, esta aplicación ha dejado de funcionar, por lo que hay que utilizar otras herramientas y técnicas para conocer el estado de actualización del sistema. En el siguiente artículo puedes encontrar, de una forma clara, sencilla y completa, una forma de asegurar que tu sistema está actualizado.

Como saber qué actualizaciones de Windows 10 tienes instaladas.

En Linux, es el **kernel lo que hay que actualizar. Kernel significa núcleo, y se refiere a que es la parte principal del sistema operativo, de hecho en Windows también existe un kernel, es un fichero** llamado **krnl32.dll** y está en **C:\windows\system,** o **C:\windows\system32** (dependiendo de la versión de 32 o 64 bits del sistema operativo). Sí, exactamente, es el primer archivo que todo virus que se precie ataca. En un sistema **GNU/Linux** el kernel está normalmente en **/boot** y se llama **vmlinuz.** Existen varias posibilidades para actualizar tu núcleo según figura en la página kernel.org. En general, las versiones pares son las estables y después hay alguna versión con soporte a largo plazo.

En Mac Os X se descarga la actualización de la página web de Apple y lo hace el propio equipo en el menú: Apple → Actualización software.

Privilegios en las cuentas de usuarios del sistema:

- **En Windows** tienes tres perfiles de usuario: **Administrador**, **Usuario Estandar** e **Invitado** (en Windows 10 por defecto no aparece habilitado). Y puedes configurar el control parental en todos los usuarios, para observar el informe de actividades realizadas desde esa cuenta vigilada.
  Esta gestión se realiza en el panel de control en la utilidad llamada cuentas de usuario. Más adelante puedes crear grupos para establecer derechos sobre carpetas y/o ficheros. También, llamando a la consola **cmd** con el comando **netplwiz.**
- **En Linux** tienes tres usuarios predeterminados, el usuario **estándar**, el **root** y el usuario **especial**. Root tiene todos los privilegios, el usuario estándar sólo tendrá los privilegios necesarios para usar las aplicaciones y el resto de los usuarios tendrán los privilegios que root quiera proporcionarles. Los usuarios se gestionan desde la interfaz gráfica y por comando.
- **En Mac OS X** se gestionan desde preferencias del sistema en CUENTAS. Hay cinco tipos: **root**, **administrador**, **usuario**, gestión **parental** e **invitado**.

Para una buena gestión de las cuentas es recomendable dar sólo a los usuarios los mínimos permisos que necesitan y no utilizar la cuenta de administrador para el desempeño diario, sólo cuando se necesiten los permisos que esta cuenta tiene.

Debes conocer

Gestión de cuentas en Windows 10

Control de Acceso a la Información.

Existe un viejo dicho en la seguridad informática que dicta que "**todo lo que no está permitido debe estar prohibido"** y esto es lo que debe asegurar la Seguridad Lógica. La **Seguridad Lógica** consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo". Los objetivos que te debes plantear serán:

1. **Restringe** el acceso a los programas y archivos.
2. Asegura que los operadores puedan trabajar sin una supervisión minuciosa y **no puedan modificar** los programas ni los archivos que no correspondan.
3. Asegura que se estén utilizados los datos, archivos y programas correctos "**en**" y "**por**" el procedimiento correcto.
4. Que la información que has transmitido sea **recibida** sólo por el **destinatario** al cual tú has enviado los datos y no por otro.
5. Que la información que **recibas** sea la **misma** que has **transmitido**.
6. Que estén a tu disposición sistemas **alternativos secundarios** de transmisión entre diferentes puntos.
7. Que dispongas de pasos alternativos de **emergencia** para la transmisión de información.

En cuanto a los **Controles de Acceso**, los puedes implementar en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro programa. Constituyen una importante ayuda para proteger al sistema operativo y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente que tengas en cuenta otras consideraciones referidas a la seguridad lógica como, por ejemplo, las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standars and Technology (**NIST**) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

1. Identificación y Autentificación.
2. Roles.
3. Transacciones.
4. Limitaciones a los Servicios.
5. Modalidad de Acceso.
6. Ubicación y Horario.
7. Control de Acceso Interno.
8. Control de Acceso Externo.
9. Administración.

Para saber más

Sin duda Internet es un medio que ofrece infinitas posibilidades. Comunicarse, interactuar con otras personas, informarse, etc. son sólo algunas de las ventajas con las que cuenta con respecto a otros medios de comunicación pero al igual que éstos, también puede ofrecer una cara menos amable que se presenta cuando los menores acceden a contenidos que no siempre nos gustaría que vieran.

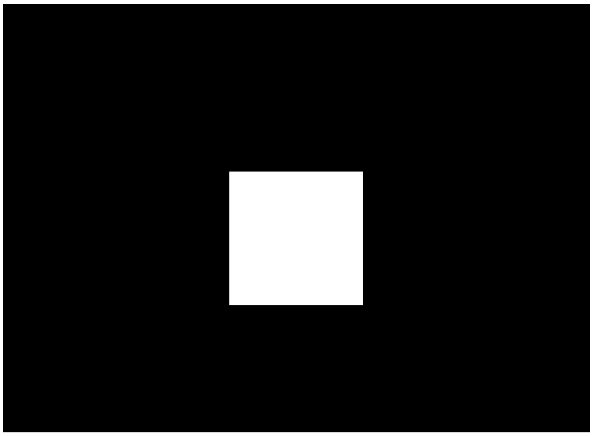
Contenidos inadecuados en Internet

Debes conocer

Principios de seguridad según el National Institute for Standars and Technology **(NIST)**. En el siguiente enlace tienes toda la información:

Principios de Seguridad.

Además aquí tienes una presentación que ilustra lo anterior:



00:00 02:24

Monitorización del Sistema.

Como ya sabes las infiltraciones más dañinas al sistema seguridad de una empresa, son generalmente con ayuda de alguien de **dentro**. Se estipula que el 70% de los incidentes de seguridad que causan pérdidas no involucran a extraños ni extrañas sino a usuarios y usuarias propias. Tener firewalls y detectores de virus puede protegerlo de ataques externos pero no internos. La única forma de proteger tu sistema es **monitoreando** los registros de los servidores y generando alertas en tiempo real.

Los ficheros **LOG** (inglés ficheros de registro de actividad), te permiten detectar incidentes y comportamientos no habituales. Esta información puede resultarte muy útil para localizar fallos en las configuraciones de los programas o cambios que se hayan hecho sobre dicha configuración. También detectarás si se ha **desconectado** al dispositivo del sistema y controlarás el uso de recursos por parte del usuario o usuaria. Además, tendrás información sobre el **rendimiento** del sistema que te puede resultar útil para detectar cuándo un equipo empezó a fallar.

¿Qué es el registro de eventos de Windows?

Los Sistemas Operativos incorporan ficheros LOG donde registran información sobre qué usuarios y en qué momento abren y cierran sesión, qué procesos están en ejecución dentro del sistema, las aplicaciones que son ejecutadas por los usuarios, así como los posibles problemas de seguridad. Estos LOG en Windows son llamados **registros de sucesos.** Estos registros contienen la información más importante para el diagnóstico de los fallos en aplicaciones y en el sistema. Los registros del sistema te informan sobre el correcto funcionamiento, el estado de un sistema y si las aplicaciones funcionan correctamente.

Los Sistemas de Windows almacenan todos los registros en archivos binarios **.Evt** y hay tres tipos básicos de registros de sucesos: **Aplicación** (AppEvent.Evt), **Sistema** (SysEvent.Evt), y de **Seguridad** (SecEvent.Evt). Los sistemas Windows 2000 y posteriores pueden contener registros de sucesos adicionales, por ejemplo, el servidor DNS (DNSEvent.Evt).

- Los **registros referentes al Sistema** registran eventos como arranque, apagado y eventos como fallos del hardware y del controlador.
- El **registro de Aplicación**, es una fuente importante de información sobre el estado de las aplicaciones. Si está bien integrado con el sistema operativo Windows, las aplicaciones pueden informar de sus errores al registro de sucesos registrando una entrada de evento en el registro de Aplicación.
- El **Registro de eventos de seguridad**, registra eventos como inicio y termino de sesión, cambios a los derechos de acceso e inicio y apagado del sistema.

Con el comando “eventvwr.msc” abrimos dicha lista, mientras que todos esos archivos se almacenan en “AppEvent.Evt”, “SecEvent.Evt, “SysEvent.Evt”, ubicados todos ellos dentro del directorio **%SystemRoot%/system32/config.** A partir de Windows 7, la carpeta es **%SystemRoot%/system32/winevt/Logs**, y los archivos se han renombrado (empleando una extensión *.evtx, que ha mejorado la información suministrada y algunos aspectos de formato). Los archivos pasan a llamarse "Application.evtx", "Security.evtx" y "System.evtx".

En Linux para abrir el visor de Linux, podemos acceder desde Sistema> Administración> Visor de archivos de sucesos. O acceder directamente a la ruta: /var/log y el archivo de sistema es syslog que, si hace rotaciones, tendrá también sus backups (Inglés, significa copia de respaldo) como syslog.0, syslog.1, etc.

Las herramientas de monitoreo pueden ser un peligro de seguridad cuando son usadas para el espionaje. Se conocen casos de empresas que utilizan estas herramientas para controlar a sus empleados y empleadas o de ordenadores compartidos en las que instalan este tipo de utilidades para espiar a sus usuarios y usuarias.

> Si conoces la existencia de estos programas es importante: No tratar información confidencial en ordenadores de uso público que pueden ser controlados por otras personas y pueden llegar a obtener: la actividad de los programas que usamos, las páginas web que visitamos, las contraseñas que usamos en dichas páginas…

La mejor forma de detectar estos programas es analizar los procesos que corren en nuestro sistema, usando una aplicación, por ejemplo, TimeTrack (Inglés: Rastro del tiempo) que guarda un log con las actividades de los usuarios y usuarias en el sistema.

Recursos de Seguridad en el Sistema Operativo.

a. **Cuotas de Disco.**
- A cada **usuario** se le puede asignar una capacidad distinta en función de sus necesidades.
- También a cada **partición** del equipo se la puede restringir de distinta manera según sus capacidades o necesidades del usuario.

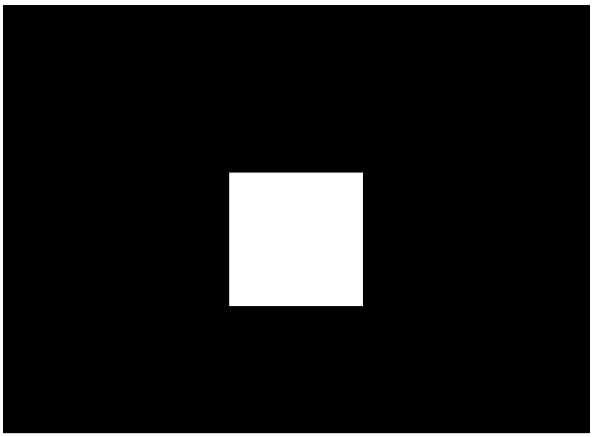
En casi todos los sistemas operativos tienes mecanismos para impedir que ciertos usuarios hagan uso indebido de la capacidad de disco, y así evitar la ralentización del equipo por saturación del sistema de ficheros y el perjuicio al resto de usuarios.
Las cuotas de disco se pueden configurar según distintos criterios.

Debes conocer

El gestor de arranque de muchos equipos es el GRUB: Una buena práctica de seguridad es ponerle una contraseña. En el siguiente artículo de la web Hacking Ético indica cómo proceder.

Cómo poner contraseña al GRUB.

Además, en esta presentación, tienes los pasos descritos para Ubuntu 8.10:



Cómo poner contraseña al GRUB.

b. **Cifrado.**
- **Una partición del sistema** que contiene los archivos necesarios para iniciar el equipo permanece sin cifrar para poder iniciar el equipo.
- **Una partición del sistema operativo** (que contiene Windows) que se cifra.

Para proteger la confidencialidad de los datos almacenados en los volúmenes de un disco podemos cifrar las particiones, con cualquier software destinado a este tema se puede encriptar un Volumen.

Los sistemas operativos Windows comienzan a introducir la herramienta de **bitlocker** para el cifrado de datos. Hasta ahora, la capacidad de cifrar unidades mediante BitLocker está disponible únicamente en las ediciones Windows 7 Ultimate y Enterprise.

Por ejemplo: configurar el disco duro para el Cifrado de unidad BitLocker. Para cifrar la unidad en la que está instalado Windows, el equipo debe tener dos particiones:

En las versiones anteriores de Windows, es posible que se haya tenido que crear manualmente estas particiones. En Windows 7, estas particiones se crean automáticamente. Si el equipo no incluye ninguna partición del sistema, el asistente de BitLocker creará una automáticamente, que ocupará 200 MB de espacio disponible en disco. **No se asignará** una letra de **unidad** a la partición del sistema y **no se mostrará en la carpeta Equipo.**

Para saber más

Siempre es más sencillo con los asistentes gráficos, pero para ciertos asuntos relativos a la seguridad para los que es conveniente que uses los comandos, para que las aprendas a hacer "de verdad". Una de esas cosas para las que merece la pena que te remangues es aprender a cifrar o encriptar particiones o discos duros completos. Las instrucciones que vas a encontrar en el siguiente enlace están pensadas para cifrar una partición en dispositivo externo pero también valdrían para una partición interna.

Cifrar una partición o disco duro externo en GNU/Linux.

Autoevaluación

¿Cuáles son los tres registros de log más importantes de Windows?:

- ○ Aplicación, Instalación y Sistema.
- ○ Instalación, Seguridad y Sistema.
- ○ Aplicación, Seguridad y Sistema.
- ○ Eventos reenviados, Seguridad y Sistema.

No es la respuesta correcta. Sólo dos de los tres eventos principales de Windows están citados en esta pregunta.

No es correcta porque no son los tres eventos principales de Windows.

Correcta. Estos son los principales, instalación y eventos reenviados también existen pero se preguntan por los principales. Muy bien, buen trabajo.

Incorrecto. Son los tres eventos de Windows, pero eventos reenviados no forma parte de los eventos principales.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

Seguridad en Redes.

Caso Práctico

Juan se encuentra trabajando y recibe la llamada telefónica de Felipe que es el encargado de la red en la imprenta “El buen libro”. No le puede atender en ese momento pero tiempo después le informan del aviso.

-Juan, te ha llamado Felipe, el de la imprenta “El buen libro”, parece que no funciona la red inalámbrica –le dice su compañera Marta.

-¿Qué crees que puede pasar? –pregunta Juan.

-Dicen que el alumnado del instituto cercano conocen la contraseña de la red y se conectan, esto colapsa el sistema, pues no hay ancho de banda para tanta gente –responde Marta.

-Pero si ya cambiamos la contraseña hace dos meses –recuerda Juan-, ¿cómo es posible que hayan averiguado de nuevo la contraseña?

-Bueno, se ve que cambiar la contraseña no es suficiente, habrá que tomar otra medida más efectiva –dice Marta.

-Yo creo que el problema también tiene que venir de dentro -razona Juan-, algún ordenador de la empresa puede estar enviando o recibiendo datos a internet y esté acaparando el ancho de banda de la red.

-Bueno, igual no tienen un problema, sino dos, lo de la contraseña y lo del empleado o empleada –resume Marta.

Cada vez que te conectas a Internet se produce un intercambio de información entre tu equipo y la red.

Ningún dispositivo, por sencillo que sea, está libre de sufrir un ataque por lo que es muy importante minimizar las posibilidades de que esto ocurra.

El caso más habitual de obtener información es mediante un **spyware.** Se trata de un pequeño programa que se instala en nuestro equipo con el objetivo de espiar nuestros movimientos por la red y robar nuestros datos, de modo que a través de él puede obtenerse información como nuestro correo electrónico y contraseña, la dirección IP de nuestro equipo, las compras que realizamos por internet e incluso el numero de la tarjeta.

Este tipo de software se instala sin que tengas conocimiento de ello y trabaja en segundo plano, de modo que no te das cuenta de su presencia, aunque puede haber una serie de indicios.

Para saber más

En la actualidad, la inmensa mayoría de la población española cuenta con un dispositivo móvil. Bien se trate de un teléfono básico, bien de un dispositivo más sofisticado (tipo tableta o smartphone) la realidad es que se ha convertido en un elemento cotidiano para nosotros.

La guía del INTECO que puedes ver en el enlace te ofrece recomendaciones para garantizarte una utilización segura de tu móvil: qué hacer para proteger tanto el terminal como la información que contiene y cómo actuar en caso de robo o pérdida:

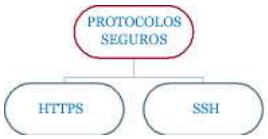
Guía para proteger y usar de forma segura su móvil. (1,5 MB)

Y desde el INCIBE, se nos proporciona un decálogo de buenas prácticas en seguridad móvil.

Decálogo de buenas prácticas en seguridad móvil.

Protocolos Seguros.

Cuando te conectas a determinados servidores, puedes ver que la dirección web que aparece en tu navegador comienza con **HTTPS** (Acrónimo Inglés. Hypertext Transfer Protocol Secure. Significa Protocolo Seguro de Transferencia de Hipertexto), en lugar de con el habitual **HTTP**. Esto se debe a que nos acabamos de conectar a un servidor seguro, que encriptará los mensajes que envíes por la red para que solo tu equipo pueda interpretarlos .



Protocolo HTTPS

El objetivo de HTTPS es proporcionar una conexión segura sobre un canal inseguro. Se basa en el **intercambio de claves** y el uso de **certificados válidos**, verificados por una autoridad de certificación que garantiza que el titular del mismo es quien dice ser de modo que un atacante no pueda hacerse pasar por él o ella.

Podemos verlo en sitios donde tengamos que escribir información privada, datos bancarios, etc., también es utilizado por los servidores de correo, cuando se trata de consultar el correo en la web, pero la activación del mismo tiene que ser voluntaria.

Protocolo SSH

El protocolo Secure Shell (SSH. Acrónimo en inglés: Secure Shell significa: Intérprete de comandos seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a equipos remotos a través de una red y copiar datos que residen en ellos de forma segura, utilizándose como **alternativa** al uso de **Telnet.**

Su forma de trabajar es similar a la de Telnet, ya que permite manejar por completo la computadora remota mediante un intérprete de comandos, pero SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera **no legible** y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

Para saber más

La web ArchLinux, en su Wiki, una guía sobre OpenSSH, la versión libre de distribución de SSH.

OpenSSH

Autoevaluación

Telnet y SSH son servicios similares, pero telnet incorpora técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión. ¿Verdadero o Falso?

- ○ Verdadero.
- ○ Falso.

No es exactamente así, prueba a leer de nuevo el texto con más atención.

Efectivamente, SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible, no Telnet.

Solución

1. Incorrecto
2. Opción correcta

Seguridad en Redes Cableadas.

Fueron las primeras redes que existieron, las que se conectaban mediante cables. Esto hace que se consideren más seguras que las redes inalámbricas. Pero como Internet existe y la evolución de las comunicaciones permite que te conectes a redes cableadas incluso si estás a miles de kilómetros, pues entonces debes pensar en proteger tu red de intrusiones externas. Una solución son las redes privadas virtuales (**VPN**. Acrónimo inglés: virtual private network: Red privada virtual.).

Red privada virtual

Una VPN o red privada virtual no es más que una red dentro de otra, habitualmente se crea una red privada virtual a través de Internet, de forma que si estás lejos de la empresa puedas hacer una conexión a ésta y situarte dentro de la empresa como un equipo más, por tanto, con **acceso a los servicios locales.**

Si eres tú el que está lejos de la empresa, pues te conviertes en el cliente VPN, y necesitas establecer una conexión VPN desde tu equipo a la empresa, donde el servidor VPN te contesta y realiza la conexión. Para ti, como cliente VPN se trata de una conexión que estableces entre su equipo y el servidor. Esta conexión es **transparente** para internet, simplemente los **datos son enviados al servidor de la misma manera que si llegaran a través de la LAN de la empresa a la que te conectas.**

Te preguntarás cómo funciona una VPN, pues establece un **túnel** entre los dos extremos de la conexión y usa sistemas de **encriptación** y **autenticación** para asegurar la confidencialidad e integridad de los datos que se transmiten.
Existen muchas aplicaciones que nos permiten crear VPN, que ofrecen diferentes niveles de seguridad y posibilidades distintas para la configuración.

Para saber más

Ejemplo de acceso remoto y software de escritorio que puedes utilizara para acceso, asistencia técnica y gestión de dispositivos en cualquier momento y en cualquier lugar.

Detección de intrusos.

Sistema detector de intrusos.), son un paso adelante en las funciones que implementan los cortafuegos. Existen varias herramientas de detección de intrusos pero su uso es bastante complejo, un ejemplo representativo es Snort (Inglés: Olfatear).

Este IDS escucha el tráfico de la red en tiempo real y lo relaciona con una serie de **normas ya predefinidas**, que pueden descargarse desde internet. Cuando encuentra alguna **coincidencia** alerta sobre ella, hace un log de dicho tráfico o lo ignora, según se haya indicado en la norma.

Arranque de servicios.

Como has visto en otros módulos, un **servicio** de un sistema operativo es una pequeña aplicación que corre en **segundo plano** y da soporte a este, para permitir tener funcionalidades como, por ejemplo, el uso del protocolo SSH.

El número de servicios que se pueden instalar y utilizar en un equipo es innumerable pero tienes que tener en cuenta que, cuantas más acciones queramos que haga automáticamente nuestro sistema operativo peor será el rendimiento del equipo. Y no solo eso, sino que es posible que también estemos poniendo en peligro su seguridad.

Autoevaluación

Un servidor VPN es lo que un usuario o usuaria que está lejos de la empresa necesita en su ordenador para conectarse mediante VPN a su empresa.

- ○ Verdadero.
- ○ Falso.

Incorrecto. Creo que te falta poner más atención. Tómate un descanso e inténtalo más tarde.

Correcto. Es un cliente VPN lo que el usuario necesita para conectarse al servidor local de la empresa si está fuera de la misma.

Solución

1. Incorrecto
2. Opción correcta

Seguridad en Redes Inalámbricas.

Seguro que te has fijado que en los últimos años, las necesidades de comunicación en las empresas y en el ámbito doméstico han cambiado mucho. La velocidad de las conexiones a Internet ha aumentado y, además en muchas casas, incluso en la tuya, puede que encuentres una red WI-FI o inalámbrica.

> "Wi-Fi" y el "Style logo" del Ying Yang fueron inventados por la agencia Interbrand. Nosotros (WiFi Alliance) contratamos Interbrand para que nos hiciera un logotipo y un nombre que fuera corto, tuviera mercado y fuera fácil de recordar. Necesitábamos algo que fuera algo más llamativo que "IEEE 802.11b de Secuencia Directa". Interbrand creó nombres como "Prozac", "Compaq", "OneWorld", "Imation", por mencionar algunas. Incluso inventaron un nombre para la compañía: VIVATO." **Phil Belanger**, miembro fundador de Wi-Fi Alliance.

La Tecnologías Wi-Fi es el estándar IEEE 802.11, define los dos primeros niveles de la capa OSI para las redes de área local inalámbricas (**WLAN**). Si hablas de la seguridad Wi-Fi puedes aplicar varias medidas de seguridad, que se pueden agrupar según el nivel en el que aplican:

- ***Nivel físico***: en este nivel se trata de controlar el **alcance** de la señal de cada punto de acceso. El uso de **antenas** puede proporcionar mayor cobertura a un mismo punto de acceso.
- ***Nivel de enlace***: es el nivel donde se establece la contraseña. El objetivo es **controlar** el acceso a través de una **contraseña** común para todos los clientes.
- ***Nivel de aplicación:*** en la capa de aplicación se **revisará** el **protocolo** RADIUS (Remote Authentication Dial-in User Service), el cual está basado en la arquitectura cliente-servidor.

Seguridad WEP.

WEP *(Wired Equivalent Privacy)* es el sistema de cifrado estándar que se utilizó inicialmente para el cifrado del protocolo **802.11**. Intenta dar a las redes inalámbricas la seguridad que tienes en las redes cableadas. La principal diferencia entre las redes cableadas e inalámbricas es que en las redes inalámbricas puedes intentar entrar en la red si estás dentro del alcance, aunque sea fuera de la empresa, mientras que una red cableada hay que tener acceso físico a dicha red, es decir, hay que estar dentro de la empresa. Cuando se utiliza WEP, el punto de acceso y las estaciones de trabajo tienen que **compartir** una clave WEP. Esta clave puede ser según el estándar, de longitud 104 bits (13 caracteres) o 40 bits (5 caracteres). WEP de 128-bits no es una contraseña muy segura, pudiéndose averiguar si tienes acceso a un número de tramas suficiente. Se suele utilizar en antiguos clientes que no son compatibles con WPA/WPA2. WEP en lo posible debe evitarse dado el **bajo nivel de protección** que garantiza.

Seguridad WPA.

WPA (**W**i-Fi **P**rotected **A**ccess) y **WPA2** que se centran en **asegurar** el proceso de **autenticación y cifrado** de comunicaciones y fueron creados en respuesta a las serias debilidades de otros protocolos como **WEP** (**W**ired **E**quivalent **P**rivacy). Implementa la mayoría de lo que conforma el estándar IEEE 802.11i y fue diseñado para funcionar con todas los dispositivos para redes inalámbricas, excepto los puntos de acceso de primera generación. **WPA2** implementa todo el estándar IEEE 802.11i, pero no funciona con muchos dispositivos viejos.

Seguridad WPA personal.

Con este sistema el administrador asigna una **contraseña entre 8 y 63 caracteres** en el punto de acceso. Existen dos tipos de encriptación en WPA: **TKIP**, que son renovables y se comparten con los clientes y **AES**, que es más robusto y complejo que TKIP, requiere hardware más potente.

Seguridad WPA empresarial.

Proporciona autentificación en el nivel de enlace, no es específico para Wi-Fi, ya que puede usarse **también en redes cableadas.** Se utiliza, por ejemplo, en conjunto con un RADIUS. Este tipo de método de protección **es la más segura y flexible**, y por lo tanto, se utiliza en configuraciones grandes.

Seguridad Activa.

Caso Práctico

Iván tiene que encontrar una solución para una autoescuela ya que han instalado una sala de ordenadores para realizar ejercicios de test y, mientras los realizan, no hay nadie con ellos vigilando. Está comentando la situación con Juan.

-¡Ah!, y quieren que nadie haga nada más que el test –dice Juan.-Y que no entren virus, ni instalen programas –añade Iván.-Pero ¿cómo pueden entrar los virus? –pregunta Juan.-Los alumnos se llevan los resultados de los test en un lápiz de memoria o pendrive, que seguramente habrán utilizando antes en otro ordenador –supone Iván.-¿Están los ordenadores conectados a Internet? –pregunta Juan.-Sí, sí, tienen que estar conectados a Internet pues los test están en la web -responde Iván.-Pero, tenemos muchas soluciones software para ello. ¿Cuántos ordenadores tienen? –quiere saber Juan.-Son cuarenta y cinco ordenadores en total –responde Iván- y añade que a lo largo del año, pueden llegar a mil personas, pero claro, van cambiando de mes en mes hasta que aprueban el teórico.-¿Hay alguien vigilando la sala? aparte de las cámaras de seguridad –pregunta Juan.-No, pero ten en cuenta que están conectados a internet, algún atacante podría entrar en ellos, modificarlos e incluso dejar de funcionar porque estarán conectados todo el día.-Ya, eso también hay que tenerlo en cuenta, que están conectados todo el día -responde Iván.-Según el CSI, (inglés Computer Security Institute) de San Francisco, entre un 60 y un 80 por ciento de los incidentes son causados dentro de la red. –continua Juan - Luego tenemos que tener en cuenta tanto las amenazas internas como las externas.

Las amenazas internas pueden ser más serias que las externas por varias razones, los usuarios y usuarias conocen la red y saben cómo es su funcionamiento, además tienen algún nivel de acceso a la red por necesidades de trabajo, y cuentan con la ventaja de que los **IDS y Firewalls son mecanismos inefectivos en amenazas internas.**

Esta situación no se presenta en tu casa, pero en las empresas se presenta debido a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planificación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

El resultado es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de euros.

Las amenazas externas son aquellas amenazas que se originan de fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

Las amenazas informáticas que vendrán en el futuro ya no son con la inclusión de troyanos en los sistemas o software espías, sino con el hecho de que los **ataques** se han **profesionalizado** y manipulan el significado del contenido virtual.

Recuerda que para prevenir estas nuevas amenazas sólo tienes que recordar:

- **Mantener** las soluciones activas y actualizadas.
- **Evita** realizar operaciones comerciales en ordenadores de uso público.
- **Verifica** los archivos adjuntos de mensajes sospechosos y evitar su descarga en caso de duda.

Para saber más

En este artículo de la revista PC Actual puedes encontrar formas de reducir los problemas de vulnerabilidad de tu PC.

Decir adios a las vulnerabilidades

Antivirus.

Un **antivirus** no es más que una aplicación cuya finalidad es la **detección, bloqueo y eliminación de virus** y otros códigos maliciosos. En tu ordenador tendrás instalado uno y seguro que lo mantienes actualizado diariamente, pues los virus van cambiando día a día. Según "av-comparatives.org", una página web que realiza test independientes sobre antivirus, en mayo de 2011 dice que los antivirus detectaban como mucho el 60% del nuevo malware que aparece en el mercado. Esto teniendo en cuenta que tienes el antivirus siempre actualizado.

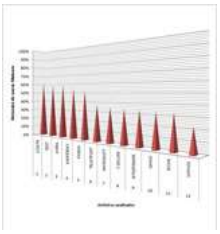
Hay que considerar que los antivirus pueden dar falsas alarmas y que encuentren software malicioso donde realmente no existe. A veces, esto se convierte en un problema y ha pasado a formar parte de las estadísticas de los antivirus como una variable más, es decir, que no de falsas alarmas mejora la eficiencia de un antivirus.

Debes conocer

OSI, "Oficina de Seguridad del Internauta", es un servicio del INCIBE y entre sus objetivos se fija el elevar la cultura de seguridad, prevenir, concienciar y formar proporcionando información clara y concisa acerca de la tecnología y el estado de la seguridad en Internet. Al mismo tiempo impulsa la detección y denuncia de nuevas amenazas en la red, de fraudes, estafas online o de cualquier otro tipo de ataque de Seguridad Informática. Uno de los servicios que proporciona es la sección de herramientas donde puedes encontrar un conjunto de aplicaciones muy útiles para solucionar problemas de seguridad que se te puedan plantear:

Herramientas Gratuitas de OSI

Virus circulando por la red.



Diferentes tipos de virus circulan por la red en busca de ordenadores desprotegidos y usuarios o usuarias incautas. Las principales motivaciones para infectar tu equipo son varias:

- Conseguir los datos bancarios o de servicios de pago en línea para suplantar tu identidad y hacer desaparecer tu dinero.
- Utilizar tu sistema como puente para realizar otro tipo de actividades maliciosas, enviar correo basura o atacar otros sistemas.
- Las vías de entrada de los virus para infectar los sistemas son muy variadas y están en constante evolución. Las más comunes son:
  - **Al visitar páginas maliciosas**, que aprovechan agujeros de seguridad en el navegador y en los programas utilizados para ver las páginas, reproductores de vídeo, visores de texto (pdf), etc.
  - **Al abrir ficheros maliciosos**, que llegan al sistema a través del correo electrónico, mensajería instantánea, redes P2P o descargados directamente de alguna página poco confiable.
  - **Al conectar al ordenador memorias USB** que previamente han sido utilizadas en un PC infectado.

Para saber más

En el siguiente enlace te muestran diversas formas de fraude a través de nuevas herramientas de seguridad.

Falsos antivirus y anti espías. (0.50 MB)

Autoevaluación

¿Cuál de los siguientes empresas antivirus ofrecen escaneo de virus en línea (on-line):

- [ ] Secunia.
- [ ] Panda.
- [ ] Eset.
- [ ] Sophos.

Mostrar retroalimentación

Solución

1. Incorrecto
2. Correcto
3. Correcto
4. Incorrecto

Antimalware.

Cuando hablas de **antimalware** te refieres a herramientas destinadas a la protección de sistemas informáticos: servidores, ordenadores de sobremesa, portátiles, dispositivos móviles, etc., frente a todo tipo de software malicioso que pueda afectarles (virus, troyanos, gusanos, spyware, etc.).

Como has visto el software malicioso o malware es una amenaza que utiliza múltiples técnicas y vías de entrada: páginas web, correo electrónico, mensajería instantánea, redes P2P, dispositivos de almacenamiento externos, redes P2P, etc. y puertos abiertos en nuestro ordenador. Estas vías son utilizadas por el malware para infectar a los sistemas informáticos y propagarse por ellos, afectando al uso para el que están destinados de distintas formas, tales como impidiendo acciones, vigilando usos, ralentizando sistemas, ejecutando acciones no permitidas, etc. Las herramientas anti-malware son de uso generalizado y las más antiguas que existen.

Su uso se ha generalizado puesto que proporcionan una protección fundamental y necesaria tanto para usuarias y usuarios domésticos como para empresas u organizaciones. Puedes recomendar su uso en todo tipo de sistemas informáticos, ya sean servidores, dispositivos de sobremesa o portátiles, incluyendo tabletas y smartphones. Y también en aquellos escenarios en los que se realiza un uso intensivo de Internet y del correo electrónico, y el intercambio frecuente ficheros o de memorias USB (pen-drive). Podemos distinguir tres grandes tipos de antimalware:

1. **Herramientas anti-virus.** Son las herramientas de seguridad **más antiguas** dentro de la categoría de antimalware. Originalmente estaban destinadas a la protección contra los virus y hoy en día su aplicación ha ido evolucionando hacia la protección de las distintas variantes de virus y ante otros tipos de malware (troyanos, gusanos,…). Las técnicas de protección también han ido evolucionando haciéndose cada vez más complejas para la detección de malware de nueva aparición.

Debes conocer

Puedes aprender, paso a paso, varias tareas habituales para la eliminación de un virus en el ordenador, como la edición de registro y la terminación de procesos.

Lucha contra los virus

2. **Herramientas anti-spyware.** Son herramientas anti-malware centradas en la lucha contra los programas creados con fines de marketing o publicitarios que suelen terminar en los ordenadores de los usuarios y usuarias por el simple hecho de navegar o usar el correo electrónico. Es un tipo de malware que aunque no siempre es perjudicial, sí es **molesto** ya que **espía tu actividad y ralentiza tu ordenador**.
3. **Herramientas UTM y appliance.** Los UTM se denominan así de sus siglas en inglés (Unified Thread Management) que se corresponde con Gestión Unificada de Amenazas y consisten en servidores o dispositivos, en ocasiones appliances específicos, que **integran distintas soluciones de seguridad** con un único interfaz de gestión. Ambos, appliances y UTM, suelen estar destinados a la protección de redes de pequeño, mediano o gran tamaño. Es muy habitual encontrar soluciones completas anti-fraude unidas a otras categorías, como anti-malware en formato UTM.

Mantén actualizado las aplicaciones y el sistema operativo, sobre todo actualiza con frecuencia el navegador y el cliente de correo electrónico, si es que lo usas habitualmente.

Para saber más

En la red cada vez hay más servicios que se están volviendo imprescindibles para el día a día: bancos, administraciones, comercio, información. Es necesario que conozcas la forma de acceder de manera segura:

Manual de INTECO para la configuración segura del navegador. (0.98 MB)

Amenaza	Relación	Solución
Amenaza externa.	☐	3. Congelar.
Eliminación de información.	☐	4. Antivirus.

Enviar

Los virus, los programas espías son, junto con las amenazas externas y la eliminación de información las amenazas más habituales en tu equipo.

Correo.

Si eres usuario o usuaria de Google Chrome y recibes un correo basura en el que te anuncian que está disponible una nueva extensión de este navegador que te ayudará a acceder a tus documentos desde los emails, para descargar esa nueva extensión lo único que tienes que hacer es seguir el link incluido en el cuerpo del mensaje. Si lo haces, serás redirigidos a una página que imita a la oficial de descargas de extensiones de Google Chrome. La sorpresa es que si te descargas la supuesta aplicación lo que estarás haciendo, en realidad, es introducir una copia del troyano Trojan.Agent.20577 en tu equipo.

Este troyano modifica el archivo HOSTS de Windows en un intento de bloquear el acceso a la página web de Google y de Yahoo. Cada vez que los usuarios quieren acceder a esas páginas son **redirigidos** a otra similar a la original pero creada para distribuir malware. De esta manera, los ciberdelincuentes **infectan** el ordenador del usuario o usuaria con nuevos códigos maliciosos.

Hay que tener en cuenta que por el hecho de recibir un correo fraudulento ninguno de tus datos personales ni la seguridad de tu equipo se encuentran en peligro, por otro lado, las entidades financieras, establecimientos de comercio electrónico y la administración pública **NUNCA** se dirigen a su clientela solicitando sus datos de acceso o de pago por medio de un correo electrónico, por lo que conviene desconfiar de este tipo de mensajes.

La solución es simplemente, **NO RESPONDER** a este tipo de mensajes si no tienes las máximas garantías de que provienen de la fuente correcta. Si crees que una compañía, con la que mantienes una cuenta o a la que le haces pedidos de compra, o cualquier administración pública pueden necesitar este tipo de información, comunícate directamente ellas. Utiliza para este contacto una **vía alternativa** al origen de la solicitud y sobre la que tengas certeza de su **fiabilidad**, como puede ser llamar por teléfono o acudir a la oficina correspondiente.

Estos mensajes utilizan todo tipo de ingeniosos argumentos relacionados con la seguridad de la entidad o el adelanto de algún trámite administrativo para justificar la necesidad de facilitar tus datos personales.

Algunas excusas frecuentes son:

Excusas frecuentes.

Tipo	Ejemplo de excusa utilizada
Nuevas recomendaciones de seguridad para prevención del fraude.	Recientes detecciones de fraude y urgente incremento del nivel de seguridad.
Problemas de carácter técnico.	Cambios en la política de seguridad de la entidad.
Promoción de nuevos productos.	Premios, regalos o ingresos económicos inesperados.

Además, un correo fraudulento tratará de forzar al usuario o usuaria a tomar una decisión de forma casi inmediata advirtiendo de consecuencias negativas como puede ser la denegación de acceso al servicio correspondiente.
Aunque los timadores perfeccionan sus técnicas continuamente, los mensajes fraudulentos generalmente se generan a través de herramientas automáticas de traducción por lo que suelen presentar faltas ortográficas y errores gramaticales.

Debes conocer

CONAN Mobile lleva a cabo un análisis exhaustivo de los elementos de riesgo de tu smartphone o tableta, agrupando y cotejando toda esa información para su análisis posterior. CONAN Mobile es gratuita:

Acceso a CONAN Mobile

Cómo crear una Contraseña Segura.

Actualmente, el método más extendido para **obtener acceso** a información personal que se almacena en los ordenadores y/o servicios en línea es mediante **contraseñas.** Se trata **de solicitar información secreta** que solo deberías de conocer tú como propietario o propietaria de la cuenta, para controlar el acceso hacia algún recurso.

Dado que la mayoría de las veces una contraseña es la **única barrera entre los datos confidenciales y potenciales atacantes** es necesario que inviertas un poco de tiempo y esfuerzo en generar una contraseña **segura.** Has de tener en cuenta de que si alguien malintencionado consiguiera apoderarse de esa información podría desde acceder a información personal **violando tu privacidad** hasta tener **acceso a servicios financieros**, suplantarte en transacciones en línea e incluso solicitar una hipoteca.

Como generar una contraseña segura:

- La longitud de las contraseñas **no debe ser inferior a ocho caracteres. Debes tener en cuenta que cuanto mayor longitud tenga más difícil será de reproducir y mayor seguridad ofrecerá.**
- Tus contraseñas deben estar formadas por una **mezcla de caracteres alfabéticos** (donde se combinen las mayúsculas y las minúsculas), **dígitos** e incluso **caracteres especiales** (@, +, &).
- **Debes cambiar** las contraseñas **regularmente.** (Dependiendo de la criticidad de los datos puede ser cada 2 meses).

Como ya dijimos, si un usuario malintencionado consiguiera apoderarse de tu contraseña, podría acceder a información personal violando tu privacidad hasta tener acceso a tus servicios financieros, pero si la cambias regularmente, sólo tendría acceso durante un tiempo determinado.

Un **buen método para crear una contraseña sólida** es que pienses en una **frase fácil** de memorizar y **acortarla** aplicando alguna regla sencilla. Un ejemplo sería seleccionando la primera letra de cada palabra y convirtiendo algunas de las letras en números que sean similares. Por ejemplo, el mensaje "La seguridad es como una cadena, es tan fuerte como el eslabón más débil" podría convertirse en "Lsec1cetfceemd".

Es posible crear contraseñas más seguras **dificultando la regla** a aplicar sobre la frase. Por ejemplo, intercalando mayúsculas y minúsculas y sustituyendo la primera de las letras **"e"** por el símbolo **"¬"**, quedando **Ls¬c1cEtFcEeMd.**

Estrategias que deben evitarse con respecto a las contraseñas:

- La contraseña **no debe contener** el **identificador o nombre de usuario de la cuenta**, o cualquier otra **información personal** que sea fácil de averiguar (cumpleaños, nombres de hijos, cónyuges, etc.).
- Tampoco una serie de letras dispuestas **adyacentemente** en el teclado (123456, qwerty).
- **No se recomienda emplear la misma contraseña** para todas las cuentas creadas para acceder a servicios en línea.
- Si alguna de ellas queda expuesta, todas las demás cuentas protegidas por esa misma contraseña también deberás considerarlas en peligro.

Asimismo, debes evitar contraseñas que contengan **palabras existentes en algún idioma** (por ejemplo Aguilanegra), uno de los ataques más conocidos para romper contraseñas es probar cada una de las palabras que figuran en el diccionario y/o palabras de uso común, es lo que se llama un **ataque de diccionario.**

No debes **almacenar** las contraseñas en un **lugar público y al alcance de los demás.** No **compartas** las contraseñas en Internet, **por correo electrónico ni por teléfono.** En especial debes **desconfiar** de cualquier mensaje de correo electrónico en el que te soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla. **Casi con total seguridad se trata de un fraude.**

Autoevaluación

¿Cuáles de las siguientes contraseñas son seguras?

- [ ] Sllrsxqlsls0"=Ç/*.
- [ ] M"-#.
- [ ] 3s=q: _OoNo.
- [ ] Secreta.

Mostrar retroalimentación

Solución

1. Correcto
2. Incorrecto
3. Correcto
4. Incorrecto

Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	
	Autoría: Urs Steiner. Licencia: CC BY 2.0. Procedencia: http://farm3.static.flickr.com/2345/5713704415_8a6973f7a2.jpg		Autoría: Instituto Industria, Turismo Licencia: Copyrigl Procedencia: option=com_news
	Autoría: Óscar Javier Estupiñán Estupiñán. Licencia: CC BY-NC-SA 3.0. Procedencia: http://recursostic.educacion.es/bancoimagenes/ArchivosImagenes/DVD04/CD06/1667__37_a_1.jpg		Autoría: I Believe Licencia: CC BY-N Procedencia: http
	Autoría: Pandafrance. Licencia: CC BY-NC-ND 2.0. Procedencia: http://farm4.static.flickr.com/3597/3500294328_2e3faf9f23.jpg		Autoría: Tomasz F Licencia: CC BY 2 Procedencia: http
	Autoría: Aaronth. Licencia: CC BY-NC-ND 2.0. Procedencia: http://farm4.static.flickr.com/3042/2631172234_c929645e2f.jpg		Autoría: ChrisDag Licencia: CC BY 2 Procedencia: http
	Autoría: Saad Irfan. Licencia: CC BY-NC-SA 2.0. Procedencia: http://farm6.static.flickr.com/5295/5536875685_ebb83af81c.jpg		Autoría: Miniyo73 Licencia: CC BY-S Procedencia: http
	Autoría: zentolos. Licencia: CC BY-NC-SA 2.0. Procedencia: http://farm3.static.flickr.com/2253/2331052514_a09c46746e.jpg		Autoría: Ségozym Licencia: CC BY-N Procedencia: http
	Autoría: Pandafrance. Licencia: CC BY-NC-ND 2.0. Procedencia: http://farm4.static.flickr.com/3517/3784978198_cc1c509734.jpg		Autoría: Pandafra Licencia: CC BY-N Procedencia: http
	Autoría: Robin Hutton. Licencia: CC BY-NC-ND 2.0. Procedencia: http://farm5.static.flickr.com/4115/4754119170_ed9bdaf5b7.jpg		Autoría: Robin Hu Licencia: CC BY 2 Procedencia: http
	Autoría: BitDefender España. Licencia: CC BY-NC-SA 2.0. Procedencia: http://www.flickr.com/photos/bitdefenderes/4534458358/in/photostream		Autoría: INTECO. Licencia: COPYR Procedencia: http://cert.inteco.e
	Autoría: Dev.Arka. Licencia: CC BY-ND 2.0. Procedencia: http://farm2.static.flickr.com/1356/808187848_f1609b79e3.jpg		Autoría: Ron Benr Licencia: CC BY 2 Procedencia: http
	Autoría: Ruzzilla. Licencia: CC BY-NC-SA 2.0. Procedencia: http://farm1.static.flickr.com/119/290667375_91212a5bca.jpg		Autoría: Johannes Licencia: CC BY-N Procedencia: http://farm6.static.

Congelación.

Cuando acabas de configurar un equipo y esa es la configuración correcta, deseas que nada ni nadie lo cambien, que el equipo se quede así, funcionando correctamente días y días, que nadie sea capaz de infectar ni desestabilizar ese equipo. Este deseo se hace mayor si **administras** sistemas con **muchos equipos** y muchos usuarios y usuarias utilizándolos a lo largo del día. Bueno pues eso es lo que hace el software de congelación, establece como configuración original el software completo que el equipo tiene en el momento de la **congelación**. **Cada vez que un equipo congelado se reinicia recupera exactamente esta configuración**, independientemente de cualquier operación que se haya hecho con el software durante la última sesión.

¿Por qué congelarías un ordenador? La congelación resulta muy útil para el mantenimiento del software de equipos, sobre todo cuando éstos son de **uso colectivo** o cuando existe un riesgo potencial de eliminación no deseada de información, de ataques de virus, de instalación de software no deseado, etc.

La congelación en los equipos es algo que previene cualquier modificación del disco duro, lo que no permite siquiera el guardar un fichero por lo que si es necesario almacenar información habrá que establecer dos particiones y sólo congelar una de ellas. Por ejemplo, en un cibercafé garantizaría que todos los equipos estuvieran iguales siempre que se encienden los ordenadores

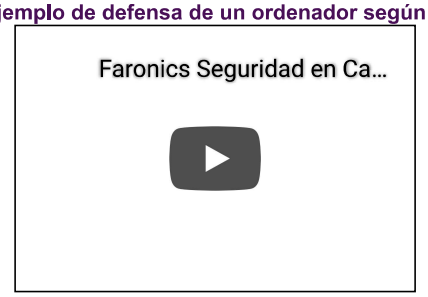
¿Cuándo crees que es necesario descongelar? Siempre que quieras hacer algún cambio en la configuración de software. Los motivos pueden ser diversos: instalación de nuevo software o actualización de versiones, reconfiguración de redes locales y de acceso a Internet, creación de una imagen personalizada, instalación de nuevo hardware, etc.

¿Cómo congelar y descongelar el equipo? Hace falta un programa para ello, por ejemplo, **Deepfreeze**, el programa se instala y tras realizar un apagado del equipo queda preparado para congelarlo. Normalmente, el programa se defiende con una contraseña para que no se modifique el estado congelado por personas diferentes al administrador.

Debes conocer

En este vídeo verás cómo se defiende un ordenador con una combinación de tres programas, un antivirus, un autoejecutable y el congelador. El vídeo las llama capas, pero no tienen nada que ver con las capas OSI:

Vídeo de ejemplo de defensa de un ordenador según Faraonics.



Para saber más

La suplantación de empresas o individuos es una práctica habitual usada por los creadores de malware para engañar a los usuarios y usuarias y conseguir que ejecuten sus creaciones o accedan a enlaces preparados para descargar malware. Fuente: Blog laboratorio Ontinet.com 25/07/2010.

Imageshack usado para propagar malware.

Autoevaluación

Relaciona las amenazas con la defensa que se utiliza para cada una de ellas, escribiendo el número asociado a la ciudad en el hueco correspondiente.

Ejercicio de relacionar

Amenaza	Relación	Solución
Los Virus.	☐	1. Antispyware.
Los programas espías.	☐	2. Firewall.

Firewall o Cortafuegos en Equipos.

Un **cortafuegos** (***firewall*** en inglés) es una parte de tu sistema que bloquea el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un software configurado para permitir, limitar, cifrar y descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

La ventaja de un cortafuegos es que **bloquea** el acceso a personas no autorizadas a redes privadas. Pero tiene algunas limitaciones. El cortafuegos filtra el tráfico. Se puede producir una ataque informático que use tráfico aceptado por el cortafuegos, por ejemplo, a través de puertos TCP abiertos expresamente: puerto 80 o que sencillamente no use la red, seguirá constituyendo una amenaza.

La siguiente lista muestra nueve casos de **riesgos** contra los que el cortafuegos no puede proteger:

- Tráfico que no pasa por él.
- Uso negligente.
- Copias de datos de forma local.
- Ingeniería social.
- Robos de dispositivos físicos.
- Virus ya instalados.
- Virus que llegan de dispositivos locales, como memorias USB.
- Fallos de seguridad en los servicios.
- Tráfico a través de puertos abiertos.

Políticas del cortafuegos.

Hay dos políticas básicas en la configuración de un cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad que quieras aplicar en la organización:

- **Política restrictiva**: **Deniegas** todo el tráfico excepto el que está **explícitamente** permitido. El cortafuegos obstruye todo el tráfico y tienes que **habilitar expresamente** el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar la empresa y organismos gubernamentales.
- **Política permisiva**: **Permites todo** el tráfico **excepto** el que esté explícitamente **denegado**. Cada servicio potencialmente peligroso lo aíslas básicamente caso por caso, mientras que el resto del tráfico no lo filtras. Esta aproximación puedes utilizarla en universidades, centros de investigación y servicios públicos de acceso a internet.

La política restrictiva es la más segura ya que es más difícil permitir por error, tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

Debes conocer

Completo vídeo-tutorial de INTECO que explica las características básicas de un cortafuegos y explica paso a paso cómo configurarlo, en concreto para el sistema operativo Windows 7:

Cómo configurar el cortafuegos en Windows 7.

Para saber más

Listado de cortafuegos gratuitos para instalar en tu ordenador:

Cortafuegos gratuitos.