Asociación Nacional de Universidades e Instituciones de Educación Superior
Dirección de Tecnologías de la Información y Comunicación

# Introducción a la ciberseguridad

# Contenido

¿Qué es la ciberseguridad? ..... 3
Objetivos de la ciberseguridad ..... 3
¿Cuáles son las amenazas más comunes? ..... 4
Causas de una amenaza ..... 5
Fases de la ciberseguridad ..... 6
Herramientas para aumentar la seguridad ..... 8
Protección de redes inalámbricas ..... 9
Elección de un antivirus ..... 10
    Criterios para obtener la mejor protección antivirus ..... 10
Phising ..... 12
    ¿Qué es el phishing? ..... 12
    ¿Quién pueden sufrir un ataque de phishing? ..... 12
    Cómo funciona el phishing y cómo se propaga ..... 13
    Claves para detectar el phishing ..... 14
Referencias ..... 16

## ¿Qué es la ciberseguridad?

Cuando nos planteamos qué es ciberseguridad, hay que decir que se conoce como la seguridad de la tecnología de la información, puesto que engloba un gran número de técnicas y métodos para proteger nuestro sistema, así como otros dispositivos o las redes. Gracias a las herramientas que tenemos disponibles en relación a la ciberseguridad, nuestro sistema estará mejor protegido de los ataques informáticos, hackeos o cualquier robo de datos o identidad. Por todo ello, es importante que para dotar a nuestro sistema con las mejores medidas, tengamos en cuenta cómo va evolucionando este concepto y siempre estemos actualizados para conocer a la perfección las nuevas herramientas que van apareciendo para evitar estas amenazas.

## Objetivos de la ciberseguridad

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- **La infraestructura computacional**: es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.
- **Los usuarios**: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el

sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

- **La información**: esta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

## ¿Cuáles son las amenazas más comunes?

Las amenazas a las que se enfrenta la ciberseguridad son infinitas**.** A pesar de que los ataques informáticos están a la orden del día y se van renovando de forma continuada, podemos decir que existen varias amenazas que son comunes y habituales dentro de este sector las cuales son necesarias tenerlas en cuenta para ponerle todas las barreras posibles a aquellos que intentan vulnerarla.

De momento, nos enfocaremos en las amenazas más habituales en la Red:

- **Ciberguerra**: Se trata de un ataque cuya finalidad por norma general es política. En este contexto, los ciberdelincuentes intentan recopilar el mayor número de información posible y datos relevantes que puedan comprometer, en un futuro, a un partido político o un gobierno. Se han dado casos sonados de partidos políticos cuya estructura se ha tambaleado debido a una de estas acciones.
- **Ciberterrorismo**: Es otra forma de amenaza común, pero en esta ocasión aunque también se intenta recopilar el máximo de información, la finalidad es diferente, puesto que el objetivo es crear un ambiente de terror entre los ciudadanos. Uno de los grandes miedos de la sociedad actual es perder la estabilidad debido a ello.
- **Cibercrimen**: El cibercrimen es una de las amenazas más comunes y la que más se suele producir en todo tipo de países. A través de ella, los hackers acceden a sistemas informáticos protegidos e intentan obtener ganancias financieras. También se realiza a nivel de usuario, tomando el control de

dispositivos concretos y solicitando cantidades económicas a cambio de su liberación entre otras posibilidades.

## Causas de una amenaza

No solamente las amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias no informáticas que deben ser tomadas en cuenta. Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización, por ejemplo mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en clúster para la disponibilidad.

Las amenazas pueden ser causadas por:

**Usuarios**: causa del mayor problema ligado a la seguridad de un sistema informático. En algunos casos sus acciones causan problemas de seguridad, si bien en la mayoría de los casos es porque tienen permisos sobredimensionados, no se les han restringido acciones innecesarias, etc.

**Programas maliciosos**: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado en el ordenador, abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica, un programa espía o spyware, en general conocidos como malware.

**Errores de programación**: la mayoría de los errores de programación que se pueden considerar como una amenaza informática es por su condición de poder ser usados como exploits por los crackers, aunque se dan casos donde el mal desarrollo es, en sí mismo, una amenaza. La actualización de parches de los sistemas operativos y aplicaciones permite evitar este tipo de amenazas.

**Intrusos**: personas que consiguen acceder a los datos o programas a los cuales no están autorizados (crackers, defacers, hackers, script kiddie o script boy, viruxers, etc.).

**Un siniestro (robo, incendio, inundación)**: una mala manipulación o mala intención derivan en la pérdida del material o de los archivos.

**Personal técnico interno**: técnicos de sistemas, administradores de bases de datos, técnicos de desarrollo, etc. Los motivos que se encuentran entre los habituales son: disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, etc.

## Fases de la ciberseguridad

Protegerse ante los peligros de la era actual implica llevar a cabo procesos de ciberseguridad que se sustenten sobre su efectividad y para hacerlo, **hay que conocer las fases en las que aplicarlos**. Podemos dividir el proceso en tres fases concretas: prevención, localización y reacción.

- **Prevención:** El primer paso siempre es la prevención, lo que reducirá en gran medida el margen de riesgo. Por ello, hay que actuar de forma temprana e informarnos de todo lo que puede ocurrirle a nuestro sistema. Determinar las posibles amenazas y cuáles serán las medidas de prevención y reacción en caso de vernos afectados por una de ellas, nos permitirá estar más preparados. Es primordial que los empleados del negocio tengan unos conocimientos básicos sobre ciberseguridad. Deben conocer las distintas herramientas que se utilizan y cómo garantizar su máximo nivel de seguridad para que no cometan errores que puedan abrir el camino a la entrada de los hackers.

Puedes analizar exhaustivamente los sistemas que utilizas para identificar posibles amenazas siguiendo las siguientes recomendaciones

- **Asegurarte de que el tipo de conexión que utilizas es segura:** tanto si utilizas el PC como el móvil para navegar, lo mejor que puedes hacer para proteger tu conexión es configurar una conexión VPN.
- **Comprobar las páginas web que visitas y los servicios online que usas:** fíjate si son espacios seguros, para ello utiliza contraseñas imposibles de descifrar.

- **No dar nunca tus datos personales a la ligera:** y si lo haces asegúrate constantemente de que nadie los está usando sin tu consentimiento.
- **Instalar antivirus en tu equipo informático:** parece obvio, pero esto te ayuda a evitar que el *malware* (virus informático) entre en tu sistema como de manera tan sencilla.
- **Hacer copias de seguridad a menudo:** otra obviedad que te va a salvar la vida si todo tu sistema se daña, así podrás recuperar tu información en lugar de perderla irremediablemente.

Poniendo en práctica todas estas acciones podrás prevenir la mayoría de los ataques perniciosos**.**

- **Localización:** Hay veces en las que prevenir no es suficiente, y por mucha barrera que pongas, al final termina por colarse algún agente informático pernicioso. En el caso de haber sufrido algún tipo de problema, habrá que localizar dónde radica el problema. Para ello la mejor herramienta es disponer de un antivirus potente que nos ayude a detectar el ataque en tiempo real y concentrarnos en él de inmediato. Localizar el ataque o la infección no es tan fácil como pueda parecer, dado que los hackers son conscientes del uso de los antivirus y lo que hacen es trabajar de manera que sus ataques puedan pasar desapercibidos. En algunos casos, desde el momento en el que se produce el golpe hasta que la empresa lo detecta, pueden pasar más de 100 días. Para intentar reducir en la medida de lo posible este problema, hay que concentrarse en dos aspectos: gestionar las vulnerabilidades de nuestro sistema y por otro llevar a cabo una monitorización de forma continuada.
- **Reacción:** Una vez que hemos localizado la amenaza, tendremos que dar una respuesta técnica sobre la misma y para ello lo ideal es aplicar una reacción para neutralizarla de una vez por todas**.**

Para ello puedes realizar estas acciones:

1. Desconecta tu sistema informático de Internet.
2. Instala un antivirus que pueda satisfacer las necesidades o actualiza el que ya tenías.
3. Cambia todas tus contraseñas. Es la mejor forma de asegurarte que nadie acceda a ningún servicio online haciéndose pasar por ti.
4. Utiliza las copias de seguridad guardadas para sustituir tus archivos dañados.
5. Vuelve a conectar el equipo a la Red y asegúrate de que el antivirus está actualizado.

Con todo esto deberías ser capaz de neutralizar la amenaza. Aun así, si te han robado información sensible no dudes en denunciarlo como un delito informático**.**

## Herramientas para aumentar la seguridad

- **La protección contra el código malicioso malware:** Comúnmente se conoce como antivirus, este tipo de seguridad es imprescindible para cualquier organización , sin importar su actividad o tamaño, además es importante ir más allá de sistemas informáticos, puesto de trabajos o servidores, y reunir todos los aspectos que se relacionan con la movilidad. La gran cantidad de distintos tipos de malware y su evolución, se transforman en una de las amenazas más difíciles de lidiar.
- **La protección antifraude o pishing:** Estas es una de las más importantes, el sentido común. El engaño, se ha convertido en una de las prácticas más usadas en internet, tanto para para infectar miles de dispositivos, como para conseguir datos de los usuarios. Aquí no existen herramientas para combatir estas amenazas, se tiene que contar con el sentido común y desconfiar de lugares sospechosos.
- **Ser previsivos** Estas herramientas constan en conseguir por varios medios la supervivencia de la organización o empresa, después de un inconveniente de seguridad, dentro de esta solución se encuentran, copias de seguridad en

la nube o en otros dispositivos, que mantienen a salvo la información de la empresa, la cual es indispensable para poder desempeñar sus funciones. También existen otras soluciones como las herramientas de recuperación de sistemas, la cual permiten restaurar un sistema desde un punto desde antes del ataque para perder el menor número posible de datos.

- **Protección de comunicaciones:** Estas soluciones se encargan de proteger a la organización de un grupo de amenazas, como los ataques de denegación de servicios, accesos no autorizados o la intercepción de las comunicaciones. También debemos de tener en cuenta que las amenazas no solo pueden partir desde Internet, sino también del interior de las empresas, es por ello que la protección de las comunicaciones es imprescindibles cuando existen varias oficinas o sedes en varias partes del mundo, cuando se realizan diariamente a través de internet.

## Protección de redes inalámbricas

Usar una red inalámbrica en tu hogar te ofrece la comodidad de utilizar la computadora prácticamente en cualquier lugar de la casa y conectarte a otras computadoras de tu red o acceder a Internet. Sin embargo, si tu red no es segura, estarás expuesto a riesgos importantes. Por ejemplo, un hacker puede hacer lo siguiente:

- Interceptar cualquier dato que envíes o recibas
- Obtener acceso a tus archivos compartidos

Estas son algunas medidas sencillas que puedes tomar para proteger tu red y enrutador inalámbricos:

- **Evita usar la contraseña predeterminada**

  Es fácil que un hacker encuentre la contraseña predeterminada del fabricante de tu enrutador inalámbrico y luego la use para acceder a tu red inalámbrica. Por eso, te recomendamos cambiar la contraseña de administrador de tu enrutador inalámbrico. A la hora de crear la contraseña nueva, trata de elegir una serie compleja de números y letras, y evita usar una contraseña que sea fácil de adivinar.

- **No permitas que tu dispositivo inalámbrico anuncie su presencia**

  Desactiva la transmisión SSID (identificador de red de servicio) para evitar que tu dispositivo inalámbrico anuncie tu presencia al mundo.
- **Cambia el nombre de SSID de tu dispositivo**

  Reiteramos que, para un hacker, es fácil descubrir el nombre de SSID predeterminado del fabricante de tu dispositivo y luego usarlo para ubicar tu red inalámbrica. Cambia el nombre de SSID predeterminado de tu dispositivo y procura evitar un nombre que sea fácil de adivinar.
- **Cifra tus datos**

  Asegúrate de habilitar el cifrado en la configuración de conexión. Si el dispositivo admite cifrado WPA, úsalo; en caso contrario, usa cifrado WEP.
- **Protégete contra malware y ataques por Internet**

  Asegúrate de instalar un producto antimalware potente en todas las computadoras y otros dispositivos. Para mantener actualizada la protección contra malware, selecciona la opción de actualización automática dentro del producto.

## Elección de un antivirus

Existen numerosos factores que debes considerar a la hora de seleccionar la mejor solución antivirus para tus necesidades. Con la seguridad de tus datos, tu identidad digital y tus transacciones financieras en juego, merece la pena invertir algo de tiempo en evaluar cada producto antivirus.

Además, si haces un amplio uso de Internet, el correo electrónico, otros servicios web y de mensajería, es importante considerar una solución que incluya tecnologías y software de seguridad de Internet que protejan más tus actividades en línea.

### Criterios para obtener la mejor protección antivirus

Lamentablemente, no todos los productos antivirus proporcionan una solución utilizable y confiable que brinde un nivel de protección adecuado contra malware.

Si las comparamos basándonos en los siguientes criterios, incluso las 10 principales soluciones antivirus del mercado pueden registrar puntuaciones distintas:

- **Confiabilidad**

  Hasta la solución antivirus más completa puede resultar absolutamente inútil si entra en conflicto con otro programa de software que se está ejecutando en tu computadora. Si estos conflictos causan un mal funcionamiento o una suspensión temporal de los procesos de protección antivirus, puedes quedar expuesto a riesgos.

- **Capacidad de uso**

  Si el uso diario de un antivirus requiere habilidades especiales, puede ser poco práctica para numerosos usuarios. Cualquier producto antivirus que sea difícil de usar, que plantee preguntas complejas al usuario o que le exija tomar decisiones difíciles puede llegar a aumentar las posibilidades de que se produzcan "errores de operador". En algunos casos, si el software antivirus es demasiado difícil de ejecutar, el usuario puede sencillamente inhabilitarlo.

- **Protección integral**

  Un antivirus debe brindar protección continua para todos los dominios informáticos, todos los tipos de archivos y todos los elementos de red que podrían estar expuestos al ataque de un virus informático u otro tipo de malware. El programa debe ser capaz de detectar código malicioso y proteger todos los canales o puntos de entrada a la computadora, como correo electrónico, Internet, FTP y más.

- **Calidad de la protección**

  Los antivirus deben ser capaces de operar en un entorno agresivo que cambia constantemente, con nuevos virus informáticos, gusanos y troyanos que pueden ser mucho más complejos que el malware conocido anterior y pueden incluir nuevas maneras de sortear las acciones de los programas antivirus. En parte, la calidad de la protección depende de los siguientes elementos:

- Eficacia de los procesos de detección de malware
- Frecuencia y regularidad de las actualizaciones
- Capacidad de eliminar infecciones de la computadora
- Eficacia en la entrega de protección a la computadora, sin afectar de manera importante su rendimiento

# Phising

El phishing es, desde hace años, una de las mayores amenazas de ciberseguridad para empresas e internautas ¿sabes en qué consiste, cómo se propaga y cuáles son las consecuencias para la privacidad de tus datos personales? Aprende a detectar el phishing con estas claves de seguridad informática.

## ¿Qué es el phishing?

Cuando hablamos de este término nos estamos refiriendo a una de los principales peligros que, desde hace años, afecta a miles de internautas y empresas y que provoca que, a través de un engaño, nuestros datos personales o bancarios acaben en manos de los ciberdelincuentes.

De esta manera, la definición de phishing está asociada directamente al concepto de robo de identidad. A través de técnicas de ingeniería social, los ciberdelincuentes engañan al internauta y, de esta manera, obtienen sus datos personales (contraseñas, acceso a perfiles de redes sociales, claves bancarias...) o los de las empresas contra los que se dirigen.

## ¿Quién pueden sufrir un ataque de phishing?

Nadie está a salvo de ser víctima de una estafa en Internet. En los últimos años se han multiplicado los ciberataques a través de dispositivos móviles, no en vano el smartphone ya es la principal vía de conexión a Internet.

Aprender a detectar el phishing a tiempo es básico. En caso de no hacerlo, las consecuencias para el internauta o la empresa pueden ser mucho más graves.

Según los datos de un informe de Google sobre el phishing, las víctimas de estos ataques tienen 400 veces más posibilidades que las de otros incidentes de perder sus datos por completo.

## Cómo funciona el phishing y cómo se propaga

Uno de los grandes problemas a la hora de detectar el phishing es, precisamente, la habilidad de los ciberdelincuentes para ocultar el fraude a través de 'ganchos', promociones y comunicaciones de apariencia real que, sin embargo, te llevan a 'webs pantalla' en las que tus datos quedan expuestos o bien a través de la descarga de archivos maliciosos que ejecutan un malware en tu dispositivo y permiten acceder a tus claves.

Los ataques que persiguen hacerse con tus datos personales tienen múltiples vías de entrada y propagación. Estas son algunas de las técnicas más empleadas que te pueden ser de utilidad para detectar el phishing y no sufrir sus consecuencias:

- Envío de correos en nombre de una empresa, banco o usuario en el que te informan de un error o problema con tus claves y te piden que las confirmes en una web que, pese a parecerse mucho, no es la original.
- Envío de correos en los que se incorpora un archivo adjunto (normalmente en formato .zip) que al ejecutarlo instala un troyano en tu ordenador y permite a los ciberdelincuentes acceder a tus datos.
- Mensajes de través de servicios como WhatsApp en los que te ofrecen cupones descuento, encuestas o premios por rellenar una encuesta con tus datos personales. De la misma manera, la web a la que te remiten es falsa.
- En los últimos años las redes sociales han cobrado un alto protagonismo en los ataques de suplantación de identidad. Ya sea a través de entradas con grandes promociones u ofertas o incluso a través del envío de mensajes personales (phishing en Facebook a través de Messenger o mensajes privados en Twitter) en los que te adjuntan un enlace fraudulento.
- Otra de las vías de entrada en los últimos años es a través de aplicaciones maliciosas que consiguen colarse en tiendas oficiales como Google Play y que,

suplantando a las oficiales u ofreciendo servicios o recursos se instalan directamente en los smartphones de las víctimas.

- En los últimos años han vuelto a popularizarse los ataques a través de SMS, algo que se conoce como Smishing y del que puedes obtener más información en este enlace.

## Claves para detectar el phishing

¿Sabes cómo detectar el phishing en un correo electrónico, un mensaje privado o en una promoción u oferta en redes sociales? Sigue estos consejos y ¡Atento! Una de las características del phishing es su constante cambio de formatos y formas en las que puede presentarse. Sigue estas claves:

### 1-Muy atento a la dirección web

Da igual que recibas un correo electrónico o un SMS o que accedas al enlace de una promoción en redes sociales. La primera clave para detectar el phishing es fijarse muy bien en la URL a la que nos remite el enlace que nos envían. Repetimos que hay que fijarse muy bien porque en algunas ocasiones las diferencias son inapreciables y se centran incluso en caracteres que se copian o se alteran (una l minúscula por una i mayúscula; un punto situado en un lugar poco visible...).

### 2-Muy atento a la ortografía

La segunda clave que debes tener en cuenta para detectar el phishing, sobre todo cuando hablamos de correos electrónicos, es la forma en la que está redactado el mensaje. Los ataques no tienen nacionalidad ni lengua y, en muchas ocasiones se traducen automáticamente o contienen faltas de ortografía, errores gramaticales o un tratamiento o forma de dirigirse a ti que ninguna comunicación oficial de tu banco, organismos o empresas contendría.

### 3-Muy atento al remitente y a lo que piden

¿Te ha llegado un correo electrónico de tu banco, de la Agencia Tributaria, de Amazon u otra empresa? Lo primero que debes mirar es el remitente y comprobar que esa dirección es la que está vinculada a esos servicios. De la misma manera, si

el correo te ha llegado a la carpeta de spam ya es un signo inequívoco de que el remitente es sospechoso. ¿Qué te piden en el correo? Ten muy presente que los bancos y las empresas u organismos no reclaman jamás que introduzcas tus datos personales o que los reingreses en una web para reactivar tu cuenta. Repetimos: No lo reclaman jamás.

### 4-Desconfía de los cupones promocionales y las encuestas

Esta modalidad de phishing ha sido una de las que más éxito ha tenido en los últimos años y ha afectado a todas las grandes marcas, todo a través de cupones promocionales en los que te prometen una compra o un vale descuento a cambio de que accedas a un enlace y rellenes tus datos personales. A partir de este momento eres víctima de phishing.

### 5-Evita descargar adjuntos

Salvo que hayas comprobado todos los pasos anteriores y estés completamente seguro de la identidad del remitente, así como del objeto del mensaje, no descargues documentos adjuntos sin antes pasarlos por un buen antivirus. Recuerda que basta con que el adjunto se descargue para que el malware comience a hacer de las suyas en tu equipo por lo que ante la duda no descargues.

### 6-Aplica el sentido común y desconfía siempre

Este consejo es válido para detectar el phishing o cualquier otra amenaza en Internet. ¿Quién va a regalar gafas Ray-Ban o a venderlas un 75% por debajo de su precio? ¿Por qué te llega esa oferta de una empresa de la que no eres cliente y que además te indica que has ganado un premio en un concurso en el que no has participado? ¿Eres tan afortunado siempre o solo en redes sociales y gracias a los enlaces compartidos de tu red de amigos?

### 7-Consulta siempre fuentes oficiales

Existen páginas y perfiles en redes sociales en los que puedes mantenerte al día de los avisos de seguridad, así como aprender claves para detectar el phishing y cualquier otra amenaza contra tu ciberseguridad.

# Referencias


OBS Bisiness School. (s. f.). ¿Qué es ciberseguridad y de qué fases consta? | OBS Business School. Recuperado 22 de mayo de 2020, de https://obsbusiness.school/int/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta

Gl, J. (2019, octubre 7). ¿Qué es la ciberseguridad? Aprende a reforzar tu seguridad informática con estas claves y consejos. Recuperado 22 de mayo de 2020, de https://ciberpatrulla.com/que-es-la-ciberseguridad/

colaboradores de Wikipedia. (2020, mayo 1). Seguridad informática - Wikipedia, la enciclopedia libre. Recuperado 22 de mayo de 2020, de https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Andalicía es digital. (2018, agosto 31). 7 Claves para detectar el phishing ¡No piques! Recuperado 22 de mayo de 2020, de https://www.blog.andaluciaesdigital.es/claves-para-detectar-el-phishing/