

# Capítulo 1: La necesidad de la ciberseguridad

---

Este capítulo explica qué es la ciberseguridad y por qué la demanda de profesionales de ciberseguridad está creciendo. Explica qué es su identidad y sus datos en línea, dónde se encuentra y por qué es de interés para los delincuentes cibernéticos.

Este capítulo también analiza qué son los datos de una organización y por qué deben protegerse. Analiza quiénes son los atacantes cibernéticos y lo que quieren. Los profesionales de la ciberseguridad deben tener las mismas habilidades que los atacantes cibernéticos, pero los profesionales de la ciberseguridad deben trabajar de acuerdo con la ley local, nacional e internacional. Los profesionales de ciberseguridad también deben usar sus habilidades con ética.

Este capítulo también incluye contenido que explica brevemente la guerra cibernética y por qué las naciones y los gobiernos necesitan profesionales de la ciberseguridad para proteger a sus ciudadanos y su infraestructura.

## ¿Qué es la ciberseguridad?

---

La red de información electrónica conectada se ha convertido en una parte integral de nuestra vida cotidiana. Todos los tipos de organizaciones, como instituciones médicas, financieras y educativas, utilizan esta red para funcionar de manera eficaz. Utilizan la red para recopilar, procesar, almacenar y compartir grandes cantidades de información digital. A medida que se recopila y se comparte más información digital, la protección de esta información se vuelve incluso más importante para nuestra seguridad nacional y estabilidad económica.

La ciberseguridad es el esfuerzo constante por proteger estos sistemas de red y todos los datos contra el uso no autorizado o los daños. A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos. A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización. A nivel del estado, la seguridad nacional, y la seguridad y el bienestar de los ciudadanos están en juego.

# Capítulo 1: La necesidad de la ciberseguridad

---

Este capítulo explica qué es la ciberseguridad y por qué la demanda de profesionales de ciberseguridad está creciendo. Explica qué es su identidad y sus datos en línea, dónde se encuentra y por qué es de interés para los delincuentes cibernéticos.

Este capítulo también analiza qué son los datos de una organización y por qué deben protegerse. Analiza quiénes son los atacantes cibernéticos y lo que quieren. Los profesionales de la ciberseguridad deben tener las mismas habilidades que los atacantes cibernéticos, pero los profesionales de la ciberseguridad deben trabajar de acuerdo con la ley local, nacional e internacional. Los profesionales de ciberseguridad también deben usar sus habilidades con ética.

Este capítulo también incluye contenido que explica brevemente la guerra cibernética y por qué las naciones y los gobiernos necesitan profesionales de la ciberseguridad para proteger a sus ciudadanos y su infraestructura.

## ¿Qué es la ciberseguridad?

---

La red de información electrónica conectada se ha convertido en una parte integral de nuestra vida cotidiana. Todos los tipos de organizaciones, como instituciones médicas, financieras y educativas, utilizan esta red para funcionar de manera eficaz. Utilizan la red para recopilar, procesar, almacenar y compartir grandes cantidades de información digital. A medida que se recopila y se comparte más información digital, la protección de esta información se vuelve incluso más importante para nuestra seguridad nacional y estabilidad económica.

La ciberseguridad es el esfuerzo constante por proteger estos sistemas de red y todos los datos contra el uso no autorizado o los daños. A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos. A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización. A nivel del estado, la seguridad nacional, y la seguridad y el bienestar de los ciudadanos están en juego.

## Su identidad en línea y fuera de línea

---

A medida que pasa más tiempo en línea, su identidad, en línea y fuera de línea, puede afectar su vida. Su identidad fuera de línea es la persona con la que sus amigos y familiares interactúan a diario en el hogar, la escuela o el trabajo. Conocen su información personal, como su nombre, edad, o dónde vive. Su identidad en línea es quién es usted en el ciberespacio. Su identidad en línea es cómo se presenta ante otros en línea. Esta identidad en línea solo debería revelar una cantidad limitada de información sobre usted.

Debe tener cuidado al elegir un nombre de usuario o alias para su identidad en línea. El nombre de usuario no debe contener información personal. Debe ser algo correcto y respetuoso. Este nombre de usuario no debe llevar a extraños a pensar que es un objetivo fácil para los delitos cibernéticos o la atención no deseada.

## Sus datos

---

Cualquier información sobre usted puede ser considerada como sus datos. Esta información personal puede identificarlo de manera única como persona. Estos datos incluyen las imágenes y los mensajes que intercambia con su familia y amigos en línea. Otra información, como su nombre, número de seguro social, la fecha y el lugar de nacimiento, o su apellido materno, es de su conocimiento y se utiliza para identificarlo. La información como la información médica, educativa, financiera y laboral, también se puede utilizar para identificarlo en línea.

### **Expediente médico**

Cada vez que asiste al consultorio del médico, más información se agrega a su historial médico. La prescripción de su médico de cabecera se vuelve parte de su historial médico. Su historial médico incluye su estado físico y mental, y otra información personal que puede no estar relacionada médicamente. Por ejemplo, si asistió a terapias durante la niñez cuando se produjeron cambios importantes en la familia, esto figurará en algún lugar de sus historias clínicas. Además de su historia médica y de la información personal, su historial médico también puede incluir información sobre su familia.

Los dispositivos médicos, como las pulseras deportivas, utilizan la plataforma de la nube para permitir la transferencia, el almacenamiento y la visualización inalámbrica de los datos clínicos, como el ritmo cardíaco, la presión arterial y el azúcar en la sangre. Estos dispositivos pueden generar una enorme cantidad de datos clínicos que pueden volverse parte de su historial clínico.

### **Historial educativo**

A medida que avanza en su educación, la información sobre sus notas y puntajes en las evaluaciones, su asistencia, los cursos realizados, los reconocimientos y títulos adquiridos, así como cualquier informe disciplinario puede estar en su historial educativo. Este historial también puede incluir información de contacto, salud y su historial de inmunización, así como un historial de educación especial, incluidos los programas educativos individualizados.

### **Historial financiero y de empleo**

Su historial financiero puede incluir información sobre sus ingresos y gastos. El historial de impuestos pueden incluir talones de cheques de pago, resúmenes de la tarjeta de crédito, su calificación crediticia y otra información bancaria. Su información de empleo puede incluir su empleo anterior y su rendimiento.



## ¿Dónde están sus datos?

Toda esta información es sobre usted. Existen distintas leyes que protegen la privacidad y los datos en su país. Pero, ¿sabe dónde están sus datos?

Cuando está en el consultorio médico, la conversación que tiene con el médico se registra en su expediente médico. Para fines de facturación, esta información se puede compartir con la empresa de seguros para garantizar la facturación y la calidad adecuadas. Ahora, una parte de su historial médico de la visita también se encuentra en la empresa de seguros.

Las tarjetas de fidelidad de la tienda pueden ser una manera conveniente de ahorrar dinero en sus compras. Sin embargo, la tienda compila un perfil de sus compras y utiliza esa información para su propio uso. El perfil muestra que un comprador compra cierta marca y sabor de crema dental regularmente. La tienda utiliza esta información para identificar como objetivo al comprador con ofertas especiales del partner de marketing. Con la tarjeta de fidelidad, la tienda y el partner de marketing tienen un perfil del comportamiento de compra de un cliente.

Cuando comparte sus imágenes en línea con sus amigos, ¿sabe quién puede tener una copia de las imágenes? Las copias de las imágenes están en sus propios dispositivos. Sus amigos pueden tener copias de dichas imágenes descargadas en sus dispositivos. Si las imágenes se comparten públicamente, es posible que desconocidos tengan copias de ellas también. Podrían descargar dichas imágenes o realizar capturas de pantalla de dichas imágenes. Debido a que las imágenes se publicaron en línea, también se guardan en servidores ubicados en distintas partes del mundo. Ahora las imágenes ya no se encuentran solo en sus dispositivos informáticos.

## Sus dispositivos informáticos

---

Sus dispositivos informáticos no solo almacenan sus datos. Ahora estos dispositivos se han convertido en el portal a sus datos y generan información sobre usted.

A menos que haya seleccionado recibir los resúmenes en papel para todas sus cuentas, usted utiliza sus dispositivos informáticos para acceder a los datos. Si desea una copia digital del último resumen de la tarjeta de crédito, utiliza sus dispositivos informáticos para acceder a la página web del emisor de la tarjeta de crédito. Si desea pagar su factura de la tarjeta de crédito en línea, accede a la página web de su banco para transferir los fondos con sus dispositivos informáticos. Además de permitirle acceder a su información, los dispositivos informáticos también pueden generar información sobre usted.

Con toda esta información sobre usted disponible en línea, sus datos personales se han vuelto rentables para los hackers.

## Quieren su dinero

---

Si tiene algo de valor, los delincuentes lo quieren.

Sus credenciales en línea son valiosas. Estas credenciales otorgan a los ladrones acceso a sus cuentas. Puede pensar que los kilómetros de viajero frecuente adquiridos no tienen valor para los delincuentes cibernéticos, pero deberá reconsiderar esta afirmación. Luego de que se hackearan aproximadamente 10 000 cuentas de American Airlines y United, los delincuentes cibernéticos reservaban vuelos gratuitos y mejoras con estas credenciales robadas. Aunque los kilómetros de viajero frecuente fueron devueltos a los clientes por las aerolíneas, esto demuestra el valor de las credenciales de inicio de sesión. Un delincuente también podría aprovechar sus relaciones. Pueden acceder a sus cuentas en línea y su reputación para engañarlo para que transfiera dinero a sus amigos o familiares. El delincuente puede enviar mensajes que indiquen que su familia o amigos necesitan que usted les transfiera dinero para que puedan regresar del extranjero después de perder sus billeteras.

Los delincuentes son muy imaginativos cuando intentan engañarlo para que se les otorgue dinero. No solo roban su dinero; también pueden robar su identidad y arruinarle la vida.

## Quieren su identidad

---

Además de robar su dinero para obtener una ganancia monetaria a corto plazo, los delincuentes desean obtener ganancias a largo plazo robando su identidad.

A medida que aumentan los costos médicos, el robo de la identidad médica también aumenta. Los ladrones de identidad pueden robar su seguro médico y usar sus beneficios de salud para ellos mismos, y estos procedimientos médicos ahora están en sus registros médicos.

Los procedimientos anuales de declaración de impuestos pueden variar de un país a otro; sin embargo, los delincuentes cibernéticos consideran esto como una oportunidad. Por ejemplo, la población de los Estados Unidos necesita presentar sus impuestos antes del 15 de abril de cada año. El Servicio de impuestos internos (IRS) no marca la declaración de impuestos en comparación con la información del empleador hasta julio. Un ladrón de identidad puede generar una declaración de impuestos falsa y recolectar el reembolso. Los usuarios legítimos notarán cuando sus reembolsos sean rechazados por el IRS. Con la identidad robada, también pueden abrir cuentas de tarjeta de crédito y acumular deudas en su nombre. Esto provocará daños en su calificación crediticia y hará que sea más difícil para usted obtener préstamos.

Las credenciales personales también pueden permitir el acceso a datos corporativos y de gobierno.

# Tipos de datos de la organización

---

## Datos tradicionales

Los datos corporativos incluyen información del personal, propiedades intelectuales y datos financieros. La información del personal incluye el material de las postulaciones, la nómina, la carta de oferta, los acuerdos del empleado, y cualquier información utilizada para tomar decisiones de empleo. La propiedad intelectual, como patentes, marcas registradas y planes de nuevos productos, permite a una empresa obtener una ventaja económica sobre sus competidores. Esta propiedad intelectual se puede considerar un secreto comercial; perder esta información puede ser desastroso para el futuro de la empresa. Los datos financieros, como las declaraciones de ingresos, los balances y las declaraciones de flujo de caja de una empresa brindan información sobre el estado de la empresa.

## Internet de las cosas y datos masivos

Con el surgimiento de la Internet de las cosas (IoT), hay muchos más datos para administrar y asegurar. La IoT es una gran red de objetos físicos, como sensores y equipos, que se extiende más allá de la red de computadoras tradicional. Todas estas conexiones, además del hecho de que hemos ampliado la capacidad y los servicios de almacenamiento a través de la nube y la virtualización, llevan al crecimiento exponencial de los datos. Estos datos han creado una nueva área de interés en la tecnología y los negocios denominada "datos masivos". Con la velocidad, el volumen y la variedad de datos generados por la IoT y las operaciones diarias de la empresa, la confidencialidad, integridad y disponibilidad de estos datos son vitales para la supervivencia de la organización.

# Confidencialidad, integridad y disponibilidad

---

La confidencialidad, integridad y disponibilidad, conocidas como la tríada CID (Figura 1), es una guía para la seguridad informática de una organización. La confidencialidad garantiza la privacidad de los datos mediante la restricción del acceso con el cifrado de la autenticación. La integridad garantiza que la información sea precisa y confiable. La disponibilidad garantiza que la información esté disponible a las personas autorizadas.

## Confidencialidad

Otro término para la confidencialidad sería privacidad. Las políticas de la empresa deben restringir el acceso a la información al personal autorizado y garantizar que solo las personas autorizadas verán estos datos. Los datos se pueden dividir en secciones según el nivel de seguridad o sensibilidad de la información. Por ejemplo, un desarrollador Java no debe tener acceso a la información personal de todos los empleados. Además, los empleados deben recibir capacitación para comprender las mejores prácticas para resguardar datos confidenciales, para protegerse y proteger a la empresa contra ataques. Entre los métodos para garantizar la confidencialidad se incluyen el cifrado de datos, nombre de usuario y contraseña, la autenticación de dos factores y la minimización de la exposición de la información confidencial.

## Integridad

La integridad es precisión, consistencia y confiabilidad de los datos durante su ciclo de vida. Los datos deben permanecer inalterados durante la transferencia y no deben ser modificados por entidades no autorizadas. Los permisos de archivos y el control de acceso de usuarios pueden impedir el acceso no autorizado. El control de versión se puede utilizar para evitar cambios accidentales por parte de usuarios autorizados. Las copias de respaldo deben estar disponibles para restaurar los datos dañados, y la suma de comprobación del hash se puede utilizar para verificar la integridad de los datos durante la transferencia.

La suma de comprobación se utiliza para verificar la integridad de los archivos, o cadenas de caracteres, luego de que se hayan transferido desde un dispositivo a otro a través de su red local o de Internet. Las sumas de comprobación se calculan con funciones de hash. Algunas de las sumas de comprobación comunes son MD5, SHA-1, SHA-256 y SHA-512. Una función de hash utiliza un algoritmo matemático para transformar los datos en un valor de longitud fija que representa los datos, tal como se muestra en la Figura 2. El valor de hash solo está allí para la comparación. Desde el valor de hash, los datos originales no se pueden recuperar

directamente. Por ejemplo, si olvidó su contraseña, su contraseña no se puede recuperar desde el valor de hash. La contraseña se debe restablecer.

Luego de descargar un archivo, puede verificar su integridad comparando los valores de hash del origen con el que usted generó con cualquier calculadora de hash. Al comparar los valores de hash, puede asegurarse de que el archivo no se haya alterado ni dañado durante la transferencia.

### **Disponibilidad**

Mantener los equipos, realizar reparaciones de hardware, mantener los sistemas operativos y el software actualizados, así como crear respaldos, garantiza la disponibilidad de la red y los datos a los usuarios autorizados. Deben existir planes para recuperarse rápidamente ante desastres naturales o provocados por el hombre. Los equipos o software de seguridad, como los firewalls, lo protegen contra el tiempo de inactividad debido a los ataques, como la denegación de servicio (DoS). La denegación de servicio se produce cuando un atacante intenta agotar los recursos de manera tal que los servicios no estén disponibles para los usuarios.

## **Las consecuencias de una violación a la seguridad**

---

Proteger a las organizaciones contra cualquier ciberataque posible no es factible, por algunos motivos. La experiencia necesaria para configurar y mantener la red segura puede ser costosa. Los atacantes siempre seguirán encontrando nuevas maneras de apuntar a las redes. Con el tiempo, un ciberataque avanzado y dirigido tendrá éxito. La prioridad, luego, será con qué rapidez su equipo de seguridad puede responder al ataque para minimizar la pérdida de datos, el tiempo de inactividad y la pérdida de ingresos.

Ahora sabe que todo lo publicado en línea puede vivir en línea para siempre, incluso si logró borrar todas las copias en su poder. Si sus servidores fueron atacados, la información confidencial del personal podría hacerse pública. Un hacker (o un grupo de hacking) puede vandalizar la página web de la empresa al publicar información falsa y arruinar la reputación de la empresa que tardó años en crearse. Los hackers también pueden tirar la página web de la empresa y hacer que esta pierda ingresos. Si la página web queda inactiva durante períodos de tiempo más largos, la empresa puede parecer poco confiable y perder posiblemente la credibilidad. Si el sitio web de la empresa o la red ha tenido una violación de seguridad, esto podría provocar la fuga de los documentos confidenciales, la revelación de los secretos comerciales y el robo de la propiedad intelectual. La pérdida de toda esta información puede impedir el crecimiento y la expansión de la empresa.

El costo monetario de un ataque es mucho mayor que solo reemplazar los dispositivos perdidos o robados, invertir en la seguridad existente y fortalecer la seguridad física del edificio. La empresa será responsable de comunicarse con todos los clientes afectados por la infracción y es posible que deba prepararse para un proceso jurídico. Con toda esta confusión, los empleados pueden elegir irse de la empresa. Es posible que la empresa necesite centrarse menos en el crecimiento y más en la reparación de su reputación.



## Ejemplo 1 de violación de seguridad

El administrador de contraseñas en línea, LastPass, detectó actividad inusual en su red en julio de 2015. Resultó que los hackers habían robado las direcciones de correo electrónico de los usuarios, los recordatorios de la contraseña y los hashes de autenticación. Afortunadamente para los usuarios, los hackers no pudieron obtener el repositorio de la contraseña cifrada de nadie.

Aunque hubo una violación a la seguridad, LastPass pudo de todos modos proteger la información de las cuentas de los usuarios. LastPass requiere la verificación de correo electrónico o la autenticación de varios factores cada vez que hay un nuevo inicio de sesión desde un dispositivo o una dirección IP desconocidos. Los hackers también necesitarían la contraseña principal para acceder a la cuenta.

Los usuarios de LastPass también tienen cierta responsabilidad en la protección de sus cuentas. Los usuarios deben utilizar siempre contraseñas principales complejas y cambiar las contraseñas principales periódicamente. Los usuarios siempre deben tener cuidado con los ataques de phishing. Un ejemplo de un ataque de phishing sería que un atacante envíe correos electrónicos falsos en nombre de LastPass. Los correos electrónicos solicitan que los usuarios hagan clic en un enlace incrustado y cambien la contraseña. El enlace del correo electrónico se envía a una versión fraudulenta de la página web utilizada para robar la contraseña principal. Los usuarios no deben hacer clic en los enlaces incrustados en un correo electrónico. Los usuarios también deben tener cuidado con el recordatorio de la contraseña. El recordatorio de la contraseña no debe revelar sus contraseñas. Lo más importante es que los usuarios deben habilitar la autenticación de dos pasos cuando esté disponible para todo sitio web que lo ofrezca.

Si los usuarios y los proveedores de servicios usan las herramientas y los procedimientos adecuados para proteger la información de los usuarios, los datos de los usuarios podrían protegerse, incluso en el caso de una brecha en la seguridad.

## Ejemplo 2 de violación de seguridad

---

El fabricante de juguetes de alta tecnología para niños, Vtech, sufrió una violación de seguridad en su base de datos en noviembre de 2015. Esta violación de seguridad podría afectar a millones de clientes en todo el mundo, incluidos los niños. La violación de seguridad de los datos expuso información confidencial, incluidos nombres de clientes, direcciones de correo electrónico, contraseñas, imágenes y registros de chat.

Las tablets de juguete se habían convertido en un nuevo objetivo para los hackers. Los clientes habían compartido fotografías y habían utilizado las funciones de chat en las tablets de juguete. La información no se aseguró correctamente, y el sitio web de la empresa no admitía la comunicación segura con SSL. Aunque la violación de seguridad no expuso la información de ninguna tarjeta de crédito ni datos de identificación personal, la empresa fue suspendida en la bolsa de valores debido a la preocupación por la inmensidad del ataque.

Vtech no protegió la información de los clientes correctamente y se vio expuesta durante la violación de seguridad. Aunque la empresa informó a sus clientes que sus contraseñas habían sido encriptadas, aún era posible que los hackers las descifrarán. Las contraseñas en la base de datos se cifraron mediante la función de hash MD5, pero las preguntas y respuestas de seguridad se almacenaron en texto no cifrado. Desafortunadamente, la función de hash MD5 tiene vulnerabilidades conocidas. Los hackers pueden determinar las contraseñas originales comparando millones de valores de hash calculados previamente.

Con la información expuesta en esta violación de seguridad de datos, los delincuentes cibernéticos pudieron utilizarla para crear cuentas de correo electrónico, solicitar créditos y cometer delitos antes de que los niños fueran lo suficientemente grandes como para ir a la escuela. En cuanto a los padres de estos niños, los delincuentes cibernéticos pudieron apropiarse de las cuentas en línea porque muchas personas reutilizan las contraseñas en diversos sitios web y cuentas.

La infracción a la seguridad no solo afectó la privacidad de los clientes, sino que arruinó la reputación de la empresa, según lo indicó la empresa cuando su presencia en la bolsa se suspendió.

Para los padres, es una llamada de atención para ser más cuidadosos sobre la privacidad de sus hijos en línea y solicitar una mejor seguridad para los productos de los niños. En cuanto a los fabricantes de productos conectados a la red, deben ser más agresivos en la protección de los datos de clientes y privacidad ahora y en el futuro, ya que el panorama de los ciberataques evoluciona.

## Ejemplo 3 de violación de seguridad

---

Equifax Inc. es una de las agencias nacionales de informes de crédito para el consumidor de Estados Unidos. Esta empresa recopila información de millones de clientes particulares y empresas en todo el mundo. En función de la información recopilada, se crean puntajes de crédito e informes de crédito acerca de los clientes. Esta información podría afectar a los clientes al solicitar préstamos y buscar empleo.

En septiembre de 2017, Equifax anunció públicamente un evento de violación de datos. Los atacantes aprovecharon una vulnerabilidad en el software de aplicaciones web Apache Struts. La empresa cree que los delincuentes cibernéticos tuvieron acceso a millones de datos personales sensibles de los consumidores estadounidenses entre mayo y julio de 2017. Los datos de carácter personal incluyen nombres completos de los clientes, números de seguro social, fechas de nacimiento, direcciones y otra información personal identificatoria. Hay evidencia de que la violación podría haber afectado a clientes de Reino Unido y Canadá.

Equifax creó un sitio web exclusivo que permite a los consumidores determinar si su información se vio comprometida, e iniciar sesión para que puedan controlar el crédito y protegerse contra el robo de identidad. Mediante el uso de un nuevo nombre de dominio en lugar de utilizar un subdominio de equifax.com, se permitió que personas maliciosas crearan sitios web no autorizados con nombres similares. Estos sitios web



pueden utilizarse como parte de un plan de suplantación de identidad que intenta engañar para que se proporcione información personal. Además, un empleado de Equifax proporcionó un enlace web incorrecto en medios sociales para clientes preocupados. Afortunadamente, este sitio web fue dado de baja dentro de las 24 horas. Fue creado por una persona que lo utilizaba como una oportunidad educativa para revelar las vulnerabilidades que existen en la página de respuesta de Equifax.

Como consumidor preocupado, deseará comprobar rápidamente si su información se vio comprometida para poder minimizar el impacto. En un momento de crisis, puede ser engañado para que use sitios web no autorizados. Debe ser cuidadoso al proporcionar información personal para no volver a convertirse en víctima. Además, las empresas son responsables de mantener nuestra información protegida de accesos no autorizados. Las empresas deben aplicar un parche y actualizar su software de forma periódica para mitigar el aprovechamiento de vulnerabilidades conocidas. Deben enseñar a sus empleados los procedimientos para proteger la información y qué hacer en caso de una violación, y proporcionarles información al respecto.

Por desgracia, las verdaderas víctimas de esta violación son las personas cuyos datos han sido comprometidos. En este caso, Equifax tiene la responsabilidad de proteger los datos recopilados del consumidor durante la verificación de créditos, ya que los clientes no eligieron utilizar los servicios proporcionados por Equifax. El consumidor debe confiar en la empresa para proteger la información recopilada. Además, los atacantes pueden utilizar estos datos para asumir su identidad, y es muy difícil demostrar lo contrario, ya que el atacante y la víctima conocen la misma información. En estas situaciones, lo único que puede hacer es estar alerta cuando proporcione información personal de identificación en Internet. Revise sus informes crediticios periódicamente (una vez al mes o una vez por trimestre). Denuncie de inmediato cualquier información falsa, como solicitudes de crédito que no inició o compras en sus tarjetas de crédito que no realizó.

## Tipos de atacantes

---

Los atacantes son personas o grupos que intentan aprovechar las vulnerabilidades para obtener una ganancia personal o financiera. Los atacantes están interesados en todo, desde las tarjetas de crédito hasta los diseños de producto y todo lo que tenga valor.

**Aficionados:** a veces, se denominan Script Kiddies. Generalmente, son atacantes con poca o ninguna habilidad que, a menudo, utilizan las herramientas existentes o las instrucciones que se encuentran en Internet para llevar a cabo ataques. Algunos de ellos solo son curiosos, mientras que otros intentan demostrar sus habilidades y causar daños. Pueden utilizar herramientas básicas, pero los resultados aún pueden ser devastadores.

**Hackers:** este grupo de atacantes ingresa a computadoras o redes para obtener acceso. Según la intención de la intrusión, estos atacantes se clasifican como de Sombrero Blanco, Gris o Negro. Los atacantes de Sombrero Blanco ingresan a las redes o los sistemas informáticos para descubrir las debilidades para poder mejorar la seguridad de estos sistemas. Estas intrusiones se realizan con el permiso previo y los resultados se informan al propietario. Por otro lado, los atacantes de Sombrero Negro aprovechan las vulnerabilidades para obtener una ganancia ilegal personal, financiera o política. Los atacantes de Sombrero Gris están en algún lugar entre los atacantes de sombrero blanco y negro. Los atacantes de Sombrero Gris pueden encontrar una vulnerabilidad en un sistema. Es posible que los hackers de Sombrero Gris informen la vulnerabilidad a los propietarios del sistema si esa acción coincide con su agenda. Algunos hackers de Sombrero Gris publican los hechos sobre la vulnerabilidad en Internet para que otros atacantes puedan sacarles provecho.

La figura ofrece detalles sobre los términos hacker de sombrero blanco, negro y gris.

**Hackers organizados:** estos hackers incluyen organizaciones de delincuentes cibernéticos, hacktivistas, terroristas y hackers patrocinados por el estado. Los delincuentes cibernéticos generalmente son grupos de delincuentes profesionales centrados en el control, el poder y la riqueza. Los delincuentes son muy sofisticados y organizados, e incluso pueden proporcionar el delito cibernético como un servicio a otros delincuentes. Los hacktivistas hacen declaraciones políticas para concientizar sobre los problemas que son importantes para ellos. Los atacantes patrocinados por el estado reúnen inteligencia o causan daño en nombre de su gobierno. Estos atacantes suelen estar altamente capacitados y bien financiados, y sus ataques se centran en objetivos específicos que resultan beneficiosos para su gobierno.

# Amenazas internas y externas

## Amenazas de seguridad internas

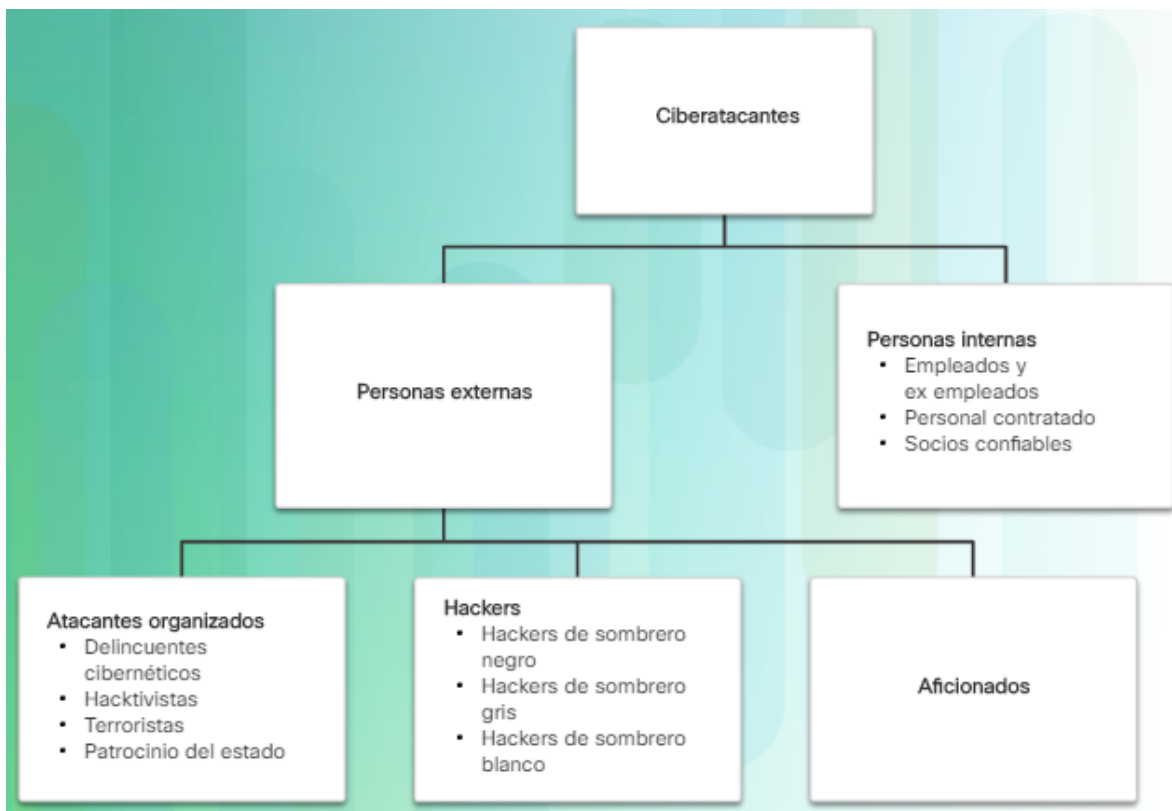
Los ataques pueden originarse dentro de una organización o fuera de ella, como se muestra en la figura. Un usuario interno, como un empleado o un partner contratado, puede de manera accidental o intencional:

- Manipular de manera incorrecta los datos confidenciales
- Amenazar las operaciones de los servidores internos o de los dispositivos de la infraestructura de red
- Facilitar los ataques externos al conectar medios USB infectados al sistema informático corporativo
- Invitar accidentalmente al malware a la red con correos electrónicos o páginas web maliciosos

Las amenazas internas también tienen el potencial de generar mayor daño que las amenazas externas, porque los usuarios internos tienen acceso directo al edificio y a sus dispositivos de infraestructura. Los empleados también tienen conocimiento de la red corporativa, sus recursos y sus datos confidenciales, así como diferentes niveles de usuario o privilegios administrativos.

## Amenazas de seguridad externas

Las amenazas externas de aficionados o atacantes expertos pueden atacar las vulnerabilidades en la red o los dispositivos informáticos, o usar la ingeniería social para obtener acceso.



# ¿Qué es la guerra cibernética?

---

El ciberespacio se ha convertido en otra dimensión importante de guerra, donde las naciones pueden tener conflictos sin los choques de las tropas y las máquinas tradicionales. Esto permite que los países con presencia militar mínima sean tan fuertes como otras naciones en el ciberespacio. La guerra cibernética es un conflicto basado en Internet que implica la penetración de sistemas de computación y redes de otros países. Estos atacantes tienen los recursos y conocimientos para lanzar ataques masivos basados en Internet contra otros países para causar daños o para interrumpir los servicios, como apagar toda la red de energía.

Un ejemplo de un ataque patrocinado por el estado involucró el malware de Stuxnet diseñado para dañar la planta de enriquecimiento nuclear de Irán. El malware de Stuxnet no tomó control de las computadoras específicas para robar información. Se diseñó para dañar el equipo físico controlado por las computadoras. Utilizó la codificación modular programada para realizar una tarea específica en el malware. Utilizó certificados digitales robados para que el ataque pareciera legítimo para el sistema. Haga clic en Reproducir para ver un video sobre Stuxnet.

Haga clic [aquí](#) para leer la transcripción de este video.

Haga clic [aquí](#) para ver otro video para obtener más información sobre Stuxnet.

## El propósito de la guerra cibernética

---

El propósito principal de la guerra cibernética es ganar ventajas sobre los adversarios, ya sea que se trate de naciones o competidores.

Un país puede constantemente invadir la infraestructura de otro país, robar los secretos de defensa, y recopilar información sobre la tecnología para reducir las brechas en sus sectores industriales y militares. Además del espionaje industrial y militar, la guerra cibernética puede dañar la infraestructura de otros países y costar vidas en las naciones específicas. Por ejemplo, un ataque puede afectar la red eléctrica de una ciudad importante. El tráfico se puede ver interrumpido. El intercambio de bienes y servicios se detiene. Los pacientes no pueden obtener el cuidado necesario en situaciones de emergencia. El acceso a Internet también se puede ver interrumpido. Al afectar la red eléctrica, el ataque puede afectar la vida diaria de los ciudadanos comunes.

Además, los datos confidenciales comprometidos pueden brindarles a los atacantes la capacidad de chantajear al personal dentro del gobierno. La información puede permitir que un atacante finja ser un usuario autorizado para acceder a información confidencial o al equipo.

Si el gobierno no puede defenderse de los ataques cibernéticos, los ciudadanos pueden perder la confianza en la capacidad del gobierno de protegerlos. La guerra cibernética puede desestabilizar una nación, interrumpir el comercio y afectar la fe de los ciudadanos en su gobierno sin invadir físicamente el país objetivo.

## Capítulo 1: La necesidad de la ciberseguridad

---

En este capítulo se explicaron las funciones y las características de la ciberseguridad. Se explicó por qué la demanda de profesionales de la ciberseguridad solo continuará aumentando. En el contenido se explica por qué su identidad y sus datos personales en línea son vulnerables a los delincuentes cibernéticos. Se ofrecen sugerencias sobre cómo puede proteger su identidad y sus datos personales en línea.

En este capítulo también se analizaron los datos de la organización: cuáles son, dónde están y por qué deben protegerse. Se explicó quiénes son los atacantes cibernéticos y lo que quieren. Los profesionales de la ciberseguridad deben tener las mismas habilidades que los atacantes cibernéticos. Los profesionales de la ciberseguridad deben trabajar dentro de los parámetros de la ley local, nacional e internacional. Los profesionales de ciberseguridad también deben usar sus habilidades con ética.

Por último, en este capítulo se explicó brevemente la guerra cibernética y por qué las naciones y los gobiernos necesitan profesionales de la ciberseguridad para proteger a sus ciudadanos y su infraestructura.

Si desea explorar más a fondo los conceptos de este capítulo, consulte la página [Actividades y recursos adicionales](#) en Recursos para los estudiantes.

## Capítulo 2: Ataques, conceptos y técnicas

---

Este capítulo abarca las maneras en que los profesionales de la ciberseguridad analizan qué ocurrió después de un ciberataque. Explica las vulnerabilidades de software y hardware de seguridad y las distintas categorías de las vulnerabilidades de seguridad.

Analiza los diferentes tipos de software malicioso (conocido como malware) y los síntomas de malware. Cubre las diferentes maneras en que los atacantes pueden infiltrarse en un sistema, así como los ataques de denegación de servicio.

La mayoría de los ciberataques modernos se consideran ataques combinados. Los ataques combinados usan varias técnicas para infiltrarse en un sistema y atacarlo. Cuando un ataque no puede evitarse, es el trabajo del profesional de ciberseguridad reducir el impacto de dicho ataque.

## Búsqueda de vulnerabilidades en la seguridad

---

Las vulnerabilidades de seguridad son cualquier tipo de defecto en software o hardware. Después de obtener conocimientos sobre una vulnerabilidad, los usuarios malintencionados intentan explotarla. Un *ataque* es el término que se utiliza para describir un programa escrito para aprovecharse de una vulnerabilidad conocida. El acto de aprovecharse de una vulnerabilidad se conoce como ataque. El objetivo del ataque es acceder a un sistema, los datos que aloja o recursos específicos.

### Vulnerabilidades de software

Las vulnerabilidades de software generalmente se introducen por errores en el sistema operativo o el código de aplicación; a pesar de todos los esfuerzos realizados por las empresas para encontrar y corregir las vulnerabilidades, es común que surjan nuevas vulnerabilidades. Microsoft, Apple y otros productores de sistemas operativos lanzan parches y actualizaciones casi todos los días. Las actualizaciones de las aplicaciones también son comunes. Las aplicaciones como navegadores web, aplicaciones móviles y servidores web son actualizadas con frecuencia por las empresas y las organizaciones responsables de estas.

En 2015, una vulnerabilidad importante, llamada SYNful Knock, se descubrió en Cisco IOS. Esta vulnerabilidad permitió a los atacantes obtener el control de los routers de nivel empresarial, como los antiguos routers 1841, 2811 y 3825 de Cisco. Los atacantes pudieron así monitorear todas las comunicaciones de red y tuvieron la capacidad de infectar otros dispositivos de la red. Esta vulnerabilidad se introdujo en el sistema cuando una versión alterada de IOS se instaló en los routers. Para evitar esto, verifique siempre la integridad de la imagen de IOS descargada y limite el acceso físico al equipo solo al personal autorizado.

El objetivo de las actualizaciones de software es mantenerse actualizado y evitar el aprovechamiento de vulnerabilidades. Si bien algunas empresas tienen equipos de prueba de penetración dedicados a la búsqueda y la corrección de vulnerabilidades de software antes de que puedan ser aprovechadas, hay investigadores de seguridad independientes que también se especializan en la búsqueda de vulnerabilidades de software.

El Proyecto Zero de Google es un excelente ejemplo de esta práctica. Después de descubrir varias vulnerabilidades en los diversos programas de software utilizados por los usuarios finales, Google formó un equipo dedicado a encontrar vulnerabilidades de software. La investigación de seguridad de Google puede encontrarse [aquí](#).

### Vulnerabilidades de hardware

Las vulnerabilidades de hardware se presentan a menudo mediante defectos de diseño del hardware. La memoria RAM, por ejemplo, consiste básicamente en capacitores instalados muy cerca unos de otros. Se descubrió que, debido a la cercanía, los cambios constantes aplicados a uno de estos capacitores podían influir en los capacitores vecinos. Por esta falla de diseño, se generó una vulnerabilidad llamada Rowhammer. Mediante la reescritura repetida de memoria en las mismas direcciones, el ataque Rowhammer permite que se recuperen los datos de las celdas de memoria de direcciones cercanas, incluso si las celdas están protegidas.

Las vulnerabilidades de hardware son específicas de los modelos de dispositivos y generalmente no se ven atacadas por intentos comprometedores aleatorios. Si bien las vulnerabilidades de hardware son más comunes en ataques altamente dirigidos, la protección contra malware tradicional y la seguridad física son suficientes para proteger al usuario común.

## Clasificación de las vulnerabilidades en la seguridad

---

La mayoría de las vulnerabilidades en la seguridad del software se incluye en una de las siguientes categorías:

**Desbordamiento del búfer:** esta vulnerabilidad ocurre cuando los datos se escriben más allá de los límites de un búfer. Los búferes son áreas de memoria asignadas a una aplicación. Al cambiar los datos más allá de los límites de un búfer, la aplicación accede a la memoria asignada a otros procesos. Esto puede llevar a un bloqueo del sistema, comprometer los datos u ocasionar el escalamiento de los privilegios.

**Entrada no válida:** los programas suelen trabajar con la entrada de datos. Estos datos que entran al programa pueden tener contenido malicioso diseñado para que el programa se comporte de manera no deseada. Considere un programa que recibe una imagen para procesar. Un usuario malintencionado podría crear un archivo de imagen con dimensiones de imagen no válidas. Las dimensiones creadas maliciosamente podrían forzar al programa a asignar búferes de tamaños incorrectos e imprevistos.

**Condiciones de carrera:** esta vulnerabilidad sucede cuando el resultado de un evento depende de resultados ordenados o temporizados. Una condición de carrera se convierte en una fuente de vulnerabilidad cuando los eventos ordenados o temporizados requeridos no se producen en el orden correcto o el tiempo adecuado.

**Debilidades en las prácticas de seguridad:** los sistemas y los datos confidenciales pueden protegerse con técnicas tales como autenticación, autorización y encriptación. Los desarrolladores no deben intentar crear sus propios algoritmos de seguridad porque es probable que introduzcan vulnerabilidades. Se recomienda encarecidamente que los desarrolladores utilicen las bibliotecas de seguridad ya creadas, aprobadas y verificadas.

**Problemas de control de acceso:** el control de acceso es el proceso de controlar quién hace qué y va desde la administración del acceso físico a los equipos hasta determinar quién tiene acceso a un recurso, por ejemplo, un archivo, y qué pueden hacer con este, como leerlo o modificarlo. Muchas vulnerabilidades de seguridad se generan por el uso incorrecto de los controles de acceso.

Casi todos los controles de acceso y las prácticas de seguridad pueden superarse si el atacante tiene acceso físico a los equipos objetivo. Por ejemplo, no importa que haya configurado los permisos de un archivo, el sistema operativo no puede evitar que alguien eluda el sistema operativo y lea los datos directamente del disco. Para proteger los equipos y los datos contenidos, el acceso físico debe restringirse y deben usarse técnicas de encriptación para proteger los datos contra robo o daño.

## Actividad: Identificar la terminología de la vulnerabilidad

Término	Descripción
✓ Entrada no validada	Datos que entran al programa con contenido malicioso, diseñado para que este se comporte de manera no deseada.
✓ Debilidad en las prácticas de seguridad	Cuando los desarrolladores intentan crear sus propias aplicaciones de seguridad.
✓ Condiciones de carrera	Cuando el resultado de un evento depende de los resultados ordenados o temporizados.
✓ Desbordamiento del buffer	Cuando una aplicación maliciosa accede a la memoria asignada a otros procesos.
✓ Problemas de control de acceso	Regulación incorrecta de quién hace qué y qué puede hacer con los recursos.

## Tipos de malware

Malware, acrónimo para el inglés “Malicious Software” (Software malicioso), es cualquier código que pueda utilizarse para robar datos, evitar los controles de acceso, ocasionar daños o comprometer un sistema. A continuación, se encuentran algunos tipos comunes de malware:

**Spyware:** este malware está diseñado para rastrear y espiar al usuario. El spyware a menudo incluye rastreadores de actividades, recopilación de pulsaciones de teclas y captura de datos. En el intento por superar las medidas de seguridad, el spyware a menudo modifica las configuraciones de seguridad. El spyware con frecuencia se agrupa con el software legítimo o con caballos troyanos.

**Adware:** el software de publicidad está diseñado para brindar anuncios automáticamente. El adware a veces se instala con algunas versiones de software. Algunos adware están diseñados para brindar solamente anuncios, pero también es común que el adware incluya spyware.

**Bot:** de la palabra robot, un bot es un malware diseñado para realizar acciones automáticamente, generalmente en línea. Si bien la mayoría de los bots son inofensivos, un uso cada vez más frecuente de bots maliciosos es el de los botnets. Varias computadoras pueden infectarse con bots programados para esperar silenciosamente los comandos provistos por el atacante.

**Ransomware:** este malware está diseñado para mantener captivo un sistema de computación o los datos que contiene hasta que se realice un pago. El ransomware trabaja generalmente encriptando los datos de la computadora con una clave desconocida para el usuario. Algunas otras versiones de ransomware pueden aprovechar vulnerabilidades específicas del sistema para bloquearlo. El ransomware se esparce por un archivo descargado o alguna vulnerabilidad de software.

**Scareware:** este tipo de malware está diseñado para persuadir al usuario de realizar acciones específicas en función del temor. El scareware falsifica ventanas emergentes que se asemejan a las ventanas de diálogo del sistema operativo. Estas ventanas muestran mensajes falsificados que indican que el sistema está en riesgo o necesita la ejecución de un programa específico para volver al funcionamiento normal. En realidad, no se evaluó ni detectó ningún problema y, si el usuario acepta y autoriza la ejecución del programa mencionado, el sistema se infecta con malware.

**Rootkit:** este malware está diseñado para modificar el sistema operativo a fin de crear una puerta trasera. Los atacantes luego utilizan la puerta trasera para acceder a la computadora de forma remota. La mayoría de los rootkits aprovecha las vulnerabilidades de software para realizar el escalamiento de privilegios y modificar los archivos del sistema. También es común que los rootkits modifiquen las herramientas forenses de supervisión del sistema, por lo que es muy difícil detectarlos. A menudo, una computadora infectada por un rootkit debe limpiarse y reinstalarse.

**Virus:** un virus es un código ejecutable malintencionado que se adjunta a otros archivos ejecutables, generalmente programas legítimos. La mayoría de los virus requiere la activación del usuario final y puede activarse en una fecha o un momento específico. Los virus pueden ser inofensivos y simplemente mostrar una imagen o pueden ser destructivos, como los que modifican o borran datos. Los virus también pueden programarse para mutar a fin de evitar la detección. La mayoría de los virus ahora se esparcen por unidades USB, discos ópticos, recursos de red compartidos o correo electrónico.

**Troyano:** un troyano es malware que ejecuta operaciones maliciosas bajo la apariencia de una operación deseada. Este código malicioso ataca los privilegios de usuario que lo ejecutan. A menudo, los troyanos se encuentran en archivos de imagen, archivos de audio o juegos. Un troyano se diferencia de un virus en que se adjunta a archivos no ejecutables.

**Gusanos:** los gusanos son códigos maliciosos que se replican mediante la explotación independiente de las vulnerabilidades en las redes. Los gusanos, por lo general, ralentizan las redes. Mientras que un virus requiere la ejecución de un programa del host, los gusanos pueden ejecutarse por sí mismos. A excepción de la infección inicial, ya no requieren la participación del usuario. Una vez infectado el host, el gusano puede propagarse rápidamente por la red. Los gusanos comparten patrones similares. Todos tienen una vulnerabilidad de activación, una manera de propagarse y contienen una carga útil.

Los gusanos son responsables de algunos de los ataques más devastadores en Internet. Como se muestra en la Figura 1, en 2001 el gusano Código Rojo infectó 658 servidores. En el plazo de 19 horas, el gusano infectó más de 300 000 servidores, como se muestra en la Figura 2.

**Hombre en el medio (MitM):** el MitM permite que el atacante tome el control de un dispositivo sin el conocimiento del usuario. Con ese nivel de acceso, el atacante puede interceptar y capturar información sobre el usuario antes de retransmitirla a su destino. Los ataques MitM se usan ampliamente para robar información financiera. Existen muchas técnicas y malware para proporcionar capacidades de MitM a los atacantes.

**Hombre en el móvil (MitMo):** una variación del hombre en el medio, el MitMo es un tipo de ataque utilizado para tomar el control de un dispositivo móvil. Cuando está infectado, puede ordenarse al dispositivo móvil que exfiltre información confidencial del usuario y la envíe a los atacantes. Zeus, un ejemplo de ataque con capacidades de MitMo, permite que los atacantes capturen silenciosamente SMS de verificación de 2 pasos enviados a los usuarios.

## Síntomas de malware

---

Independientemente del tipo de malware con el que se ha infectado un sistema, estos son síntomas frecuentes de malware:

- Aumento del uso de la CPU.
- Disminución de la velocidad de la computadora.
- La computadora se congela o falla con frecuencia.
- Hay una disminución en la velocidad de navegación web.
- Existen problemas inexplicables con las conexiones de red.

- Se modifican los archivos.
- Se eliminan archivos.
- Hay una presencia de archivos, programas e iconos de escritorio desconocidos.
- Se ejecutan procesos desconocidos.
- Los programas se cierran o reconfiguran solos.
- Se envían correos electrónicos sin el conocimiento o el consentimiento del usuario.

Actividad: Identificar los tipos de malware	
Término	Descripción
✓ Bot	Malware diseñado para entrar en acción de manera automática, generalmente en línea.
✓ Ransomware	Malware diseñado para mantener cautivo un sistema computacional o los datos que contiene hasta que se realice un pago.
✓ Rootkit	Malware diseñado para modificar el sistema operativo a fin de crear una puerta trasera.
✓ Spyware	Generalmente agrupado con software legítimo, este malware está diseñado para realizar un seguimiento de la actividad del usuario.
✓ Virus	Código malintencionado que se adjunta a otros archivos ejecutables, generalmente de programas legítimos.
✓ Troyano	Malware que ejecuta operaciones maliciosas bajo la apariencia de una operación deseada.
✓ Adware	Agrupado en algunos casos con otro software, este malware está diseñado para mostrar automáticamente anuncios publicitarios.
✓ MitMo	Malware que se utiliza para tomar el control de un dispositivo móvil.
✓ Scareware	Malware diseñado para persuadir al usuario para que realice alguna acción específica en función del temor.
✓ Gusano	Código malicioso que se replica atacando de manera independiente las vulnerabilidades en las redes.

## Ingeniería social

La ingeniería social es un ataque de acceso que intenta manipular a las personas para que realicen acciones o divulguen información confidencial. Los ingenieros sociales con frecuencia dependen de la disposición de las personas para ayudar, pero también se aprovechan de sus vulnerabilidades. Por ejemplo, un atacante puede llamar a un empleado autorizado con un problema urgente que requiere acceso inmediato a la red. El atacante puede atraer la vanidad o la codicia del empleado o invocar la autoridad mediante técnicas de nombres.

Estos son algunos tipos de ataques de ingeniería social:

- **Pretexto:** esto es cuando un atacante llama a una persona y miente en el intento de obtener acceso a datos privilegiados. Un ejemplo implica a un atacante que pretende necesitar datos personales o financieros para confirmar la identidad del objetivo.



- **Seguimiento:** esto es cuando un atacante persigue rápidamente a una persona autorizada a un lugar seguro.
- **Algo por algo (quid pro quo):** esto es cuando un atacante solicita información personal de una parte a cambio de algo, por ejemplo, un obsequio.

## Decodificación de contraseñas Wi-Fi

---

La decodificación de contraseñas Wi-Fi es el proceso de detección de la contraseña utilizada para proteger la red inalámbrica. Estas son algunas técnicas utilizadas en la decodificación de contraseñas:

**Ingeniería social:** el atacante manipula a una persona que conoce la contraseña para que se la proporcione.

**Ataques por fuerza bruta:** el atacante prueba diversas contraseñas posibles en el intento de adivinar la contraseña. Si la contraseña es un número de 4 dígitos, por ejemplo, el atacante deberá probar cada una de las 10 000 combinaciones. Los ataques por fuerza bruta normalmente involucran un archivo de lista de palabras. Este es un archivo de texto que contiene una lista de palabras tomadas del diccionario. Un programa luego prueba cada palabra y las combinaciones comunes. Debido a que los ataques por fuerza bruta llevan tiempo, las contraseñas complejas llevan mucho más tiempo para descifrar. Algunas herramientas para forzar las contraseñas incluyen Ophcrack, L0phtCrack, THC Hydra, RainbowCrack y Medusa.

**Monitoreo de la red:** mediante la escucha y la captura de paquetes enviados por la red, un atacante puede descubrir la contraseña, si la contraseña se envía sin cifrar (en texto plano). Si la contraseña está cifrada, el atacante aún puede revelarla mediante una herramienta de decodificación de contraseñas.

## Suplantación de identidad

---

La suplantación de identidad es cuando una persona maliciosa envía un correo electrónico fraudulento disfrazado como fuente legítima y confiable. El objetivo de este mensaje es engañar al destinatario para que instale malware en su dispositivo o comparta información personal o financiera. Un ejemplo de suplantación de identidad es un correo electrónico falsificado similar al enviado por una tienda de conveniencia que solicita al usuario que haga clic en un enlace para reclamar un premio. El enlace puede ir a un sitio falso que solicita información personal o puede instalar un virus.

La suplantación de identidad focalizada es un ataque de suplantación de identidad altamente dirigido. Si bien la suplantación de identidad y la suplantación de identidad focalizada usan correos electrónicos para llegar a las víctimas, los correos electrónicos de la suplantación de identidad (phishing) focalizada se personalizan para cada persona específica. El atacante investiga los intereses del objetivo antes de enviarle el correo electrónico. Por ejemplo, el atacante descubre que al objetivo le interesan los automóviles y que está interesado en la compra de un modelo específico. El atacante se une al mismo foro de debate sobre automóviles donde el objetivo es miembro, publica una oferta de venta del automóvil y envía un correo electrónico al objetivo. El correo electrónico contiene un enlace a imágenes del automóvil. Cuando el objetivo hace clic en el enlace, el malware se instala en la computadora del objetivo.

## Aprovechamiento de vulnerabilidades

---

El aprovechamiento de vulnerabilidades es otro método común de infiltración. Los atacantes analizan las computadoras para obtener información. A continuación encontrará un método común de aprovechamiento de vulnerabilidades:

**Paso 1.** Recopilación de información sobre el sistema de destino. Esto se puede hacer de muchas formas diferentes, como con un escáner de puerto o a través de la ingeniería social. El objetivo es aprender tanto como sea posible acerca de la computadora de destino.

**Paso 2.** Parte de la información pertinente aprendida en el Paso 1 puede ser el sistema operativo, su versión y una lista de los servicios que ejecuta.

**Paso 3.** Una vez que conoce el sistema operativo y la versión del objetivo, el atacante busca cualquier vulnerabilidad conocida específica para dicha versión del SO u otros servicios del sistema operativo.

**Paso 4.** Cuando encuentra una vulnerabilidad, el atacante busca usar un ataque desarrollado anteriormente. Si no se ha desarrollado ningún ataque, el atacante puede considerar desarrollar uno.

La Figura 1 representa a un atacante que usa **Whois**, una base de datos de Internet pública que contiene información sobre nombres de dominio y personas registradas. La Figura 2 representa a un atacante que usa la herramienta **Nmap**, un escáner popular de puerto. Con un escáner de puerto, un atacante puede sondear los puertos de la computadora de un objetivo para conocer qué servicios se ejecutan en la computadora.

### **Amenazas persistentes avanzadas**

Una forma de lograr la infiltración es a través de amenazas persistentes avanzadas (APT). Estas consisten en una operación cautelosa y avanzada de varias fases a largo plazo contra un objetivo específico. Debido a la complejidad y el nivel de habilidad requeridos, las APT generalmente están bien financiadas. Las APT apuntan a las organizaciones o las naciones por motivos políticos o comerciales.

Generalmente relacionadas con el espionaje con base en la red, el propósito de las APT es implementar malware personalizado en uno o varios sistemas de destino y pasar desapercibidas. Con múltiples fases de operación y varios tipos personalizados de malware que afecten a distintos dispositivos y realizan funciones específicas, un atacante individual generalmente carece del conjunto de habilidades, recursos o la perseverancia necesarios para llevar a cabo una APT.

## **DoS**

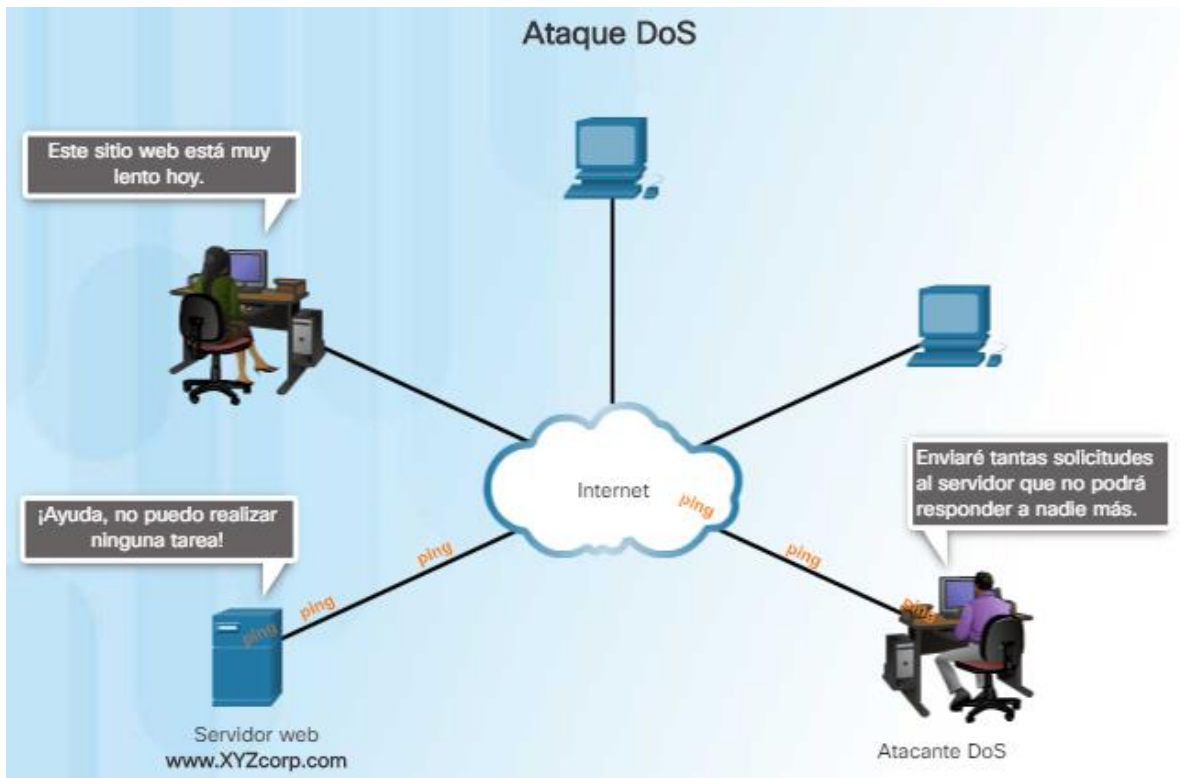
---

Los ataques de denegación de servicio (DoS) son un tipo de ataque a la red. Un ataque DoS da como resultado cierto tipo de interrupción del servicio de red a los usuarios, los dispositivos o las aplicaciones. Existen dos tipos principales de ataques DoS:

**Cantidad abrumadora de tráfico:** esto ocurre cuando se envía una gran cantidad de datos a una red, a un host o a una aplicación a una velocidad que no pueden administrar. Esto ocasiona una disminución de la velocidad de transmisión o respuesta o una falla en un dispositivo o servicio.

**Paquetes maliciosos formateados:** esto sucede cuando se envía un paquete malicioso formateado a un host o una aplicación y el receptor no puede manejarlo. Por ejemplo, un atacante envía paquetes que contienen errores que las aplicaciones no pueden identificar o reenvía paquetes incorrectamente formateados. Esto hace que el dispositivo receptor se ejecute muy lentamente o se detenga.

Los ataques de DoS se consideran un riesgo importante porque pueden interrumpir fácilmente la comunicación y causar una pérdida significativa de tiempo y dinero. Estos ataques son relativamente simples de llevar a cabo, incluso por un atacante inexperto.



## DDoS

Un ataque DoS distribuido (DDoS) es similar a un ataque DoS pero proviene de múltiples fuentes coordinadas. Por ejemplo, un ataque DDoS podría darse de la siguiente manera:

Un atacante crea una red de hosts infectados, denominada botnet. Los hosts infectados se denominan zombies. Los zombies son controlados por sistemas manipuladores.

Las computadoras zombie constantemente analizan e infectan más hosts, lo que genera más zombies. Cuando está listo, el hacker proporciona instrucciones a los sistemas manipuladores para que los botnet de zombies lleven a cabo un ataque DDoS.

Haga clic en Reproducir en la figura para ver las animaciones de un ataque DDoS.



## Envenenamiento SEO

Los motores de búsqueda, como Google, funcionan clasificando páginas y presentando resultados relevantes conforme a las consultas de búsqueda de los usuarios. Según la importancia del contenido del sitio web, puede aparecer más arriba o más abajo en la lista de resultados de la búsqueda. La optimización de motores de búsqueda (SEO, por sus siglas en inglés) es un conjunto de técnicas utilizadas para mejorar la clasificación de un sitio web por un motor de búsqueda. Aunque muchas empresas legítimas se especializan en la optimización de sitios web para mejorar su posición, un usuario malintencionado puede utilizar la SEO para hacer que un sitio web malicioso aparezca más arriba en los resultados de la búsqueda. Esta técnica se denomina envenenamiento SEO.

El objetivo más común del envenenamiento SEO es aumentar el tráfico a sitios maliciosos que puedan alojar malware o ejercer la ingeniería social. Para forzar un sitio malicioso para que califique más alto en los resultados de la búsqueda, los atacantes se aprovechan de los términos de búsqueda populares.

## Actividad: Identificar el tipo de DoS

Descripción	DoS	DDoS	Envenenamiento SEO
Relativamente simple de llevar a cabo, incluso por un atacante inexperto.	✓		
Se origina a partir de múltiples fuentes coordinadas.		✓	
Los zombies son controlados por sistemas de manipulación.		✓	
Cuando se envía un paquete con formato malicioso a un host o una aplicación y el receptor no puede manejarlo.	✓		
Hace que un sitio web malicioso aparezca con mayor relevancia en los resultados de la búsqueda.			✓
Aumenta el tráfico a sitios maliciosos que pueden alojar malware o realizar la ingeniería social.			✓
Un atacante crea una red de hosts infectados denominada botnet.		✓	
Cuando se envía una gran cantidad de datos a una red, a un host o a una aplicación a una velocidad que no pueden procesar.	✓		

## ¿Qué es un ataque combinado?

Los ataques combinados son ataques que usan diversas técnicas para comprometer un objetivo. Mediante el uso de varias técnicas de ataque simultáneas, los atacantes tienen malware que combina gusanos, troyanos, spyware, registradores de pulsaciones, spam y esquemas de suplantación de identidad. Esta tendencia de ataques combinados revela malware más complejo y pone los datos de los usuarios en gran riesgo.

Los tipos más comunes de ataque combinado utilizan mensajes de correo electrónico no deseado, mensajes instantáneos o sitios web legítimos para distribuir enlaces donde se descarga malware o spyware secretamente en la computadora. Otro ataque combinado común utiliza DDoS combinado con correos electrónicos de suplantación de identidad (phishing). Primero, el ataque DDoS se utiliza para suspender un sitio web popular de un banco y enviar correos electrónicos a sus clientes disculpándose por la inconveniencia. El correo electrónico además redirecciona a los usuarios a un sitio de emergencia falso donde la información real de inicio de sesión puede ser robada.

Muchos de los gusanos más perjudiciales de las computadoras, como Nimbda, CodeRed, BugBear, Klez y Slammer, se categorizan mejor como ataques combinados, como se muestra a continuación:

- Algunas variantes de Nimbda utilizan archivos adjuntos de correo electrónico, descargas de archivos de un servidor web comprometido y uso compartido de archivos de Microsoft (intercambios anónimos) como métodos de propagación.
- Otras variantes de Nimbda pueden modificar las cuentas de invitado del sistema para proporcionar al atacante o código malicioso los privilegios administrativos.

Los gusanos recientes Conficker y Zeus/LICAT también son ataques combinados. Conficker utiliza todos los métodos de distribución tradicionales.

## ¿Qué es la reducción del impacto?

Si bien la mayoría de las empresas exitosas de hoy en día son conscientes de los problemas de seguridad comunes y ponen gran esfuerzo en su prevención, no hay ningún conjunto de prácticas de seguridad 100 % eficiente. Dado que es probable que ocurra una violación a la seguridad si el premio es grande, las empresas y organizaciones también deben estar preparadas para contener el daño.

Es importante comprender que el impacto de la violación de seguridad no solo está relacionado con el aspecto técnico, los datos robados, las bases de datos dañadas o los daños a la propiedad intelectual; los daños también se extienden a la reputación de la empresa. Responder ante una infracción de datos es un proceso muy dinámico.

A continuación, hay algunas medidas importantes que una empresa debe adoptar cuando identifica una violación de seguridad, según muchos expertos en seguridad:

- Comunicar el problema. Informar internamente a los empleados del problema y llamarlos a la acción. Informar externamente a los clientes a través de comunicación directa y anuncios oficiales. La comunicación genera transparencia, que es crucial para este tipo de situación.
- Ser sincero y responsable en caso de que la empresa tenga la culpa.
- Proporcionar detalles. Explicar por qué ocurrió la situación y qué se vio afectado. También se espera que la empresa se haga cargo de los costos de los servicios de protección contra el robo de identidad para los clientes afectados.
- Comprender qué causó y facilitó la violación de seguridad. De ser necesario, contrate expertos en informática forense para investigar y conocer los detalles.
- Aplicar lo aprendido de la investigación de informática forense para garantizar que no se produzcan violaciones de seguridad similares en el futuro.
- Asegurarse de que todos los sistemas estén limpios, que no se hayan instalado puertas traseras y que no haya nada más comprometido. Los atacantes con frecuencia probarán dejar una puerta trasera para facilitar las infracciones futuras. Asegúrese de que esto no suceda.
- Capacitar a los empleados, los partners y los clientes acerca de cómo prevenir las violaciones futuras.

## Capítulo 2: Ataques, conceptos y técnicas

---

Este capítulo cubre las maneras en que los profesionales de la ciberseguridad analizan qué ocurrió después de un ciberataque. Explica las vulnerabilidades de seguridad en software y hardware y las distintas categorías de las vulnerabilidades de seguridad.

Explica los diferentes tipos de software malicioso (conocido como malware) y los síntomas de malware. Parte del malware analizado incluyó virus, gusanos, troyanos, spyware, adware y otros.

Se cubrieron las diferentes maneras en que los atacantes pueden infiltrarse en un sistema, entre ellas, la ingeniería social, la decodificación de contraseñas Wi-Fi, la suplantación de identidad y el aprovechamiento de vulnerabilidades. También se explicaron distintos tipos de ataques de denegación de servicio.

Los ataques combinados usan varias técnicas para infiltrarse en un sistema y atacarlo. Muchos de los gusanos más perjudiciales para las computadoras, como Nimda, CodeRed, BugBear, Klez y Slammer, se categorizan mejor como ataques combinados. Cuando un ataque no puede evitarse, es el trabajo del profesional de ciberseguridad reducir el impacto de dicho ataque.

Si desea explorar más a fondo los conceptos de este capítulo, consulte la página [Actividades y recursos adicionales](#) en Recursos para los estudiantes.

## Capítulo 3: Protección de sus datos y de su seguridad

---

Este capítulo se centra en sus dispositivos personales y sus datos personales. Incluye sugerencias para proteger sus dispositivos, crear contraseñas seguras y usar redes inalámbricas de manera segura. También analiza el mantenimiento de sus datos protegidos.

Sus datos en línea valen mucho para los delincuentes cibernéticos. Este capítulo abarca brevemente las técnicas de autenticación para ayudarlo a mantener sus datos protegidos. Además, cubre las opciones para mejorar la seguridad de sus datos en línea con sugerencias sobre qué hacer y qué no hacer en línea.

### Proteja sus dispositivos informáticos

---

Sus dispositivos informáticos almacenan sus datos y son el portal hacia su vida en línea. La siguiente es una breve lista de pasos a seguir para proteger sus dispositivos informáticos contra intrusiones:

- **Mantenga el firewall encendido:** ya sea un firewall de software o un firewall de hardware en un router, el firewall debe estar activado y actualizado para evitar que los hackers accedan a sus datos personales o empresariales. Haga clic [Windows 7 y 8.1](#) o [Windows 10](#) para activar el firewall en la versión correspondiente de Windows. Haga clic [aquí](#) para activar el firewall en los dispositivos Mac OS X.
- **Utilice un antivirus y antispyware:** el software malicioso, como virus, troyanos, gusanos, ransomware y spyware, se instala en los dispositivos informáticos sin su permiso para obtener acceso a su computadora y sus datos. Los virus pueden destruir sus datos, ralentizar su computadora o apoderarse de ella. Una manera en que los virus pueden apoderarse de su computadora es permitiendo que los emisores de correo no deseado envíen correos electrónicos desde su cuenta. El spyware puede supervisar sus actividades en línea, recopilar su información personal o enviar anuncios emergentes no deseados a su navegador web mientras está en línea. Una buena regla es descargar software solamente de sitios web confiables para evitar obtener spyware en primer lugar. El software antivirus está diseñado para analizar su computadora y correo electrónico entrante para detectar virus y eliminarlos. A veces el software antivirus también incluye antispyware. Mantenga su software actualizado para proteger su computadora de software malicioso reciente.
- **Administre su sistema operativo y navegador:** los hackers siempre están intentando aprovechar las vulnerabilidades en sus sistemas operativos y navegadores web. Para proteger su computadora y sus datos, establezca los parámetros de seguridad en su computadora o navegador en medio o alto. Actualice el sistema operativo de la computadora, incluidos los navegadores web, y descargue e instale periódicamente parches y actualizaciones de seguridad del software de los proveedores.
- **Proteja todos sus dispositivos:** sus dispositivos informáticos, ya sean PC, PC portátiles, tablets o smartphones, deben estar protegidos con contraseña para evitar el acceso no autorizado. La información almacenada debe estar cifrada, especialmente en el caso de datos sensibles o confidenciales. En los dispositivos móviles, almacene solo información necesaria en caso de robo o pérdida cuando está fuera de su hogar. Si alguno de sus dispositivos se ve comprometido, los delincuentes pueden tener acceso a todos sus datos a través del proveedor de servicios de almacenamiento en la nube, como iCloud o Google Drive.

Los dispositivos de IoT (Internet de las cosas) representan un riesgo incluso mayor que los otros dispositivos electrónicos. Mientras que las computadoras de escritorio, portátiles y los dispositivos móviles reciben actualizaciones de software frecuentes, la mayoría de los dispositivos de IoT aún tiene su firmware original. Si se encuentran vulnerabilidades en el firmware, el dispositivo de IoT es probable que se mantenga vulnerable. Para empeorar el problema, los dispositivos de IoT están diseñados para conectarse con los servidores del proveedor (call home) y solicitar acceso a Internet. Para acceder a Internet, la mayoría de los fabricantes de dispositivos de IoT confían en la red local del cliente. El resultado es que los dispositivos de IoT son muy propensos a verse comprometidos y, cuando lo están, permiten el acceso a la red local del cliente y sus datos. La mejor manera de protegerse de esta situación es contar con dispositivos de IoT con una red aislada compartida únicamente con otros dispositivos de IoT.

Haga clic [aquí](#) para visitar Shodan, un escáner de dispositivos de IoT basado en la web.

## Use las redes inalámbricas en forma segura

---

Las redes inalámbricas permiten que los dispositivos habilitados con Wi-Fi, como computadoras portátiles y tablets, se conecten a la red por medio de un identificador de red conocido como identificador de conjunto de servicios (SSID). Para evitar que los intrusos ingresen en su red inalámbrica doméstica, el SSID predeterminado y la contraseña predeterminada para la interfaz de administración en el navegador web deben cambiarse. Los hackers son conscientes de este tipo de información de acceso predeterminada.

Opcionalmente, el router inalámbrico también puede configurarse para que no difunda el SSID, lo que añade una barrera adicional para la detección de la red. Sin embargo, esto no debe considerarse una seguridad adecuada para una red inalámbrica. Además, debe encriptar la comunicación inalámbrica habilitando la seguridad inalámbrica y la función de encriptado WPA2 en el router inalámbrico. Incluso con el encriptado WPA2 habilitado, la red inalámbrica aún puede ser vulnerable.

En octubre de 2017, se descubrió una falla de seguridad en el protocolo WPA2. Esta falla permite a un intruso descifrar la encriptación entre el router inalámbrico y el cliente inalámbrico, lo que permite que este tenga acceso al tráfico de red y lo manipule. Esta vulnerabilidad puede ser atacada utilizando el Ataque de reinstalación de clave (KRACK, Key Reinstallation Attack). Afecta a todas las redes wifi protegidas, modernas. Para mitigar un ataque, un usuario debe actualizar todos los productos afectados: routers inalámbricos y cualquier dispositivo inalámbrico, como computadoras portátiles y dispositivos móviles, tan pronto como las actualizaciones de seguridad estén disponibles. Para las computadoras portátiles u otros dispositivos con NIC por cable, una conexión por cable podría mitigar esta vulnerabilidad. Además, también puede utilizarse un servicio de VPN de confianza para prevenir el acceso no autorizado a los datos mientras se utiliza la red inalámbrica.

Haga clic [aquí](#) para saber más acerca de KRACK.

Cuando está lejos de casa, los puntos públicos de acceso inalámbrico permiten tener acceso a su información en línea y navegar por Internet. Sin embargo, es mejor no acceder ni enviar información personal confidencial a través de una red pública inalámbrica. Verifique si su computadora está configurada para compartir archivos y medios digitales y si requiere la autenticación de usuario con encriptación. Para evitar que una persona intercepte su información (lo que se conoce como “eavesdropping”) mientras utiliza una red pública inalámbrica, utilice túneles VPN y servicios encriptados. El servicio VPN proporciona acceso seguro a Internet con una conexión cifrada entre la computadora y el servidor VPN del proveedor de servicios VPN. Con un túnel VPN encriptado, aunque se intercepte una transmisión de datos, no podrá descifrarse.

Haga clic [aquí](#) para obtener más información acerca de la protección al utilizar redes inalámbricas.

Muchos dispositivos móviles, como smartphones y tablets, incluyen el protocolo inalámbrico Bluetooth. Esta funcionalidad permite que los dispositivos con Bluetooth habilitados se conecten entre sí y compartan información. Desafortunadamente, Bluetooth puede ser atacado por hackers a fin de espiar algunos dispositivos, establecer controles del acceso remoto, distribuir malware y consumir baterías. Para evitar estos problemas, mantenga Bluetooth desactivado cuando no lo utiliza.

## Utilice contraseñas únicas para cada cuenta en línea

---

Posiblemente tenga más que una cuenta en línea y cada cuenta debe tener una contraseña única. Son muchas contraseñas para recordar. Sin embargo, la consecuencia de no usar contraseñas seguras y únicas los deja a usted y sus datos vulnerables ante los delincuentes cibernéticos. Usar la misma contraseña para todas las cuentas en línea es como usar la misma llave para todas las puertas cerradas; si un atacante consiguiera su contraseña, tendría acceso a todo lo que usted posee. Si los delincuentes obtienen su contraseña mediante la suplantación de identidad, por ejemplo, intentarán ingresar en sus otras cuentas en línea. Si solo utiliza una contraseña para todas las cuentas, pueden ingresar en todas estas, robar o borrar todos sus datos, o hacerse pasar por usted.



Utilizamos tantas cuentas en línea que necesitan contraseña que es demasiado para recordar. Una solución para evitar reutilizar las contraseñas o utilizar contraseñas débiles es utilizar un administrador de contraseñas. El administrador de contraseñas almacena y encripta todas sus contraseñas complejas y diferentes. El administrador puede ayudarlo a iniciar sesión en sus cuentas en línea automáticamente. Solo debe recordar la contraseña maestra para acceder al administrador de contraseñas y administrar todas sus cuentas y contraseñas.

#### Consejos para elegir una buena contraseña:

- No use palabras del diccionario o nombres en ningún idioma.
- No use errores ortográficos comunes de palabras del diccionario.
- No use nombres de equipos o cuentas.
- De ser posible, use caracteres especiales como ! @ # \$ % ^ & \* ( ).
- Utilice una contraseña con diez o más caracteres.

A graphic with a blue background and a white circle. At the top, the text "Ejemplos de contraseñas" is written in white. Below it is a table with three columns: "Aceptable", "Buena", and "Mejor". Each column contains five password examples.

Aceptable	Buena	Mejor
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin\$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

## Use una frase en lugar de una palabra como contraseña.

Para evitar el acceso físico no autorizado a los dispositivos informáticos, use frases en lugar de palabras como contraseñas. Es más fácil crear una contraseña larga en forma de frase que en forma de palabra porque generalmente está en el formato de oración en lugar de palabra. Una longitud mayor hace que las frases sean menos vulnerables a los ataques de fuerza bruta o de diccionario. Además, una frase puede ser más fácil de recordar, especialmente si debe cambiar de contraseña con frecuencia. Aquí se incluyen algunas sugerencias para elegir buenas contraseñas o frases:

#### Sugerencias para elegir una buena frase:

- Elija una oración que signifique algo para usted.
- Agregue caracteres especiales, como ! @ # \$ % ^ & \* ( ).

- Mientras más larga, mejor.
- Evite oraciones comunes o famosas, por ejemplo, letras de una canción popular.

Recientemente, el Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos publicó requisitos de contraseña mejorados. Las normas del NIST están destinadas a aplicaciones del gobierno, pero también pueden servir como normas para otras. Las nuevas pautas tienen como objetivo proporcionar una mejor experiencia del usuario y poner la responsabilidad de comprobación del usuario en los proveedores.

#### Resumen de las nuevas pautas:

- Esta debe tener una longitud mínima de 8 caracteres, pero no más de 64 caracteres.
- No utilice contraseñas comunes ni que se puedan adivinar con facilidad; por ejemplo, contraseña, abc123.
- No hay reglas de composición, como el tener que incluir números y letras mayúsculas y minúsculas.
- Mejore la precisión de escritura permitiendo que el usuario vea la contraseña mientras la escribe.
- Se permiten todos los caracteres de impresión y espacios.
- Sin pistas de contraseña.
- Sin fecha de caducidad periódica o arbitraria de la contraseña.
- Sin autenticación basada en conocimientos, tales como información de preguntas secretas compartidas, datos de marketing, historial de transacciones.

Haga clic [aquí](#) para obtener más información sobre el requisito de contraseña mejorado del NIST.

Aunque el acceso a sus computadoras y dispositivos de red sea seguro, también es importante proteger y preservar sus datos.



## Encripte sus datos

Sus datos siempre deben estar encriptados. Es posible que piense que no tiene secretos ni nada que ocultar, ¿por qué usar la encriptación? Quizás cree que nadie desea sus datos. Muy probablemente, esto no es cierto.

¿Está listo para mostrar todas sus fotos y documentos a extraños? ¿Está listo para compartir información financiera almacenada en su computadora con sus amigos? ¿Desea divulgar sus correos electrónicos y las contraseñas de sus cuentas al público en general?

Esto puede ser incluso más problemático si una aplicación maliciosa infecta su computadora o dispositivo móvil y le roba información potencialmente valiosa, como números de cuenta, contraseñas y otros documentos oficiales. Dicho tipo de información puede generar robos de identidad, fraude o rescates. Los delincuentes pueden decidir simplemente encriptar sus datos y hacer que sean inutilizables hasta que la extorsión se liquide.

¿Qué es la encriptación? La encriptación es el proceso de conversión de la información a un formato que una parte no autorizada no puede leer. Solo una persona de confianza autorizada con la contraseña o clave secreta puede descifrar los datos y acceder a ellos en su formato original. La encriptación en sí misma no evita que una persona intercepte los datos. La encriptación solo puede evitar que una persona no autorizada vea o acceda al contenido.

Se utilizan programas de software para encriptar archivos, carpetas e incluso unidades enteras.

El sistema de encriptación de archivos (EFS, Encrypting File System) es una característica de Windows que permite encriptar datos. El EFS está directamente vinculado a una cuenta de usuario determinada. Solo el usuario que cifró los datos puede acceder a estos una vez encriptados con el EFS. Para encriptar datos con EFS en todas las versiones de Windows, siga estos pasos:

**Paso 1:** Seleccione uno o más archivos o carpetas.

**Paso 2:** Haga clic derecho en los datos seleccionados y en **>Propiedades**.

**Paso 3:** Haga clic en **Opciones avanzadas...**

**Paso 4:** Seleccione la casilla de verificación **Encriptar contenido para proteger datos**.

**Paso 5:** Las carpetas y los archivos encriptados con el EFS se muestran en verde, como se muestra en la ilustración.

## Realice un respaldo de sus datos

---

Su disco duro puede fallar. Su computadora portátil puede perderse. Pueden robar su teléfono. Quizá borró la versión original de un documento importante. Tener un respaldo puede evitar la pérdida de datos irremplazables, como fotos familiares. Para hacer un respaldo correcto de los datos, necesitará una ubicación de almacenamiento adicional para los datos y deberá copiar los datos en dicha ubicación periódica y automáticamente.

La ubicación adicional para los archivos de copia de seguridad puede estar en su red doméstica, una ubicación secundaria o la nube. Si almacena los respaldos de los datos de manera local, tendrá el control total de los datos. Puede decidir copiar todos sus datos en un dispositivo de almacenamiento conectado a la red (NAS), un disco duro externo simple o puede seleccionar solo algunas carpetas importantes para hacer un respaldo en unidades de memoria USB, CD/DVD o incluso cintas. En dicho escenario, es usted el propietario y es totalmente responsable del costo y el mantenimiento de los equipos del dispositivo de almacenamiento. Si contrata un servicio de almacenamiento en la nube, el costo depende de la cantidad de espacio de almacenamiento que necesita. Con un servicio de almacenamiento en la nube, como Amazon Web Services (AWS), tendrá acceso a sus datos de respaldo siempre que tenga acceso a su cuenta. Cuando contrata servicios de almacenamiento en línea, es posible que deba ser más selectivo respecto de los datos que respalda debido al costo del almacenamiento y las constantes transferencias de datos en línea. Uno de los beneficios de guardar un respaldo en una ubicación alternativa es que es seguro en caso de incendio, robo u otro desastre, excepto que falle el dispositivo de almacenamiento.

## Eliminación de sus datos en forma permanente

---

Cuando mueve un archivo a la papelera de reciclaje y lo elimina de manera permanente, no se puede acceder al archivo solo desde el sistema operativo. Cualquier persona con las herramientas forenses adecuadas puede recuperar el archivo debido al rastro magnético que deja en el disco duro.

Para borrar datos de modo que no sean recuperables, los datos deben sobrescribirse con unos y ceros varias veces. Para evitar la recuperación de los archivos eliminados, es posible que deba utilizar herramientas diseñadas específicamente para hacerlo. El programa SDelete de Microsoft (para Vista y versiones posteriores) reclama tener la capacidad de eliminar los archivos confidenciales por completo. Shred para Linux y Secure Empty Trash para Mac OSX son algunas herramientas que aseguran proporcionar un servicio similar.

La única forma de estar seguros de que los datos o los archivos no son recuperables es destruir físicamente el disco duro o el dispositivo de almacenamiento. Muchos delincuentes cometen la insensatez de pensar que sus archivos son impenetrables o irrecuperables.

Además de almacenar datos en las unidades de disco duro locales, sus datos también pueden guardarse en línea en la nube. Dichas copias también deberán eliminarse. Tómese un momento para preguntarse: ¿dónde están guardados mis datos? ¿En una copia de seguridad en algún lado? ¿Están encriptados? Cuando deba eliminar sus datos o librarse de un disco duro o de una computadora, pregúntese: ¿he protegido los datos para evitar que caigan en las manos incorrectas?

## Autenticación de dos factores

---

Los servicios en línea más populares, como Google, Facebook, Twitter, LinkedIn, Apple y Microsoft, utilizan la autenticación de dos factores para agregar una capa adicional de seguridad para los inicios de sesión de la cuenta. Además del nombre de usuario y la contraseña, o un patrón o número de identificación personal (PIN), la autenticación de dos factores requiere un segundo token, por ejemplo:

- **Un objeto físico:** una tarjeta de crédito, una tarjeta de cajero automático, un teléfono o un control.

Escaneo biométrico: huellas digitales, impresión de la palma o reconocimiento de voz o de rostro.

## OAuth 2.0

---

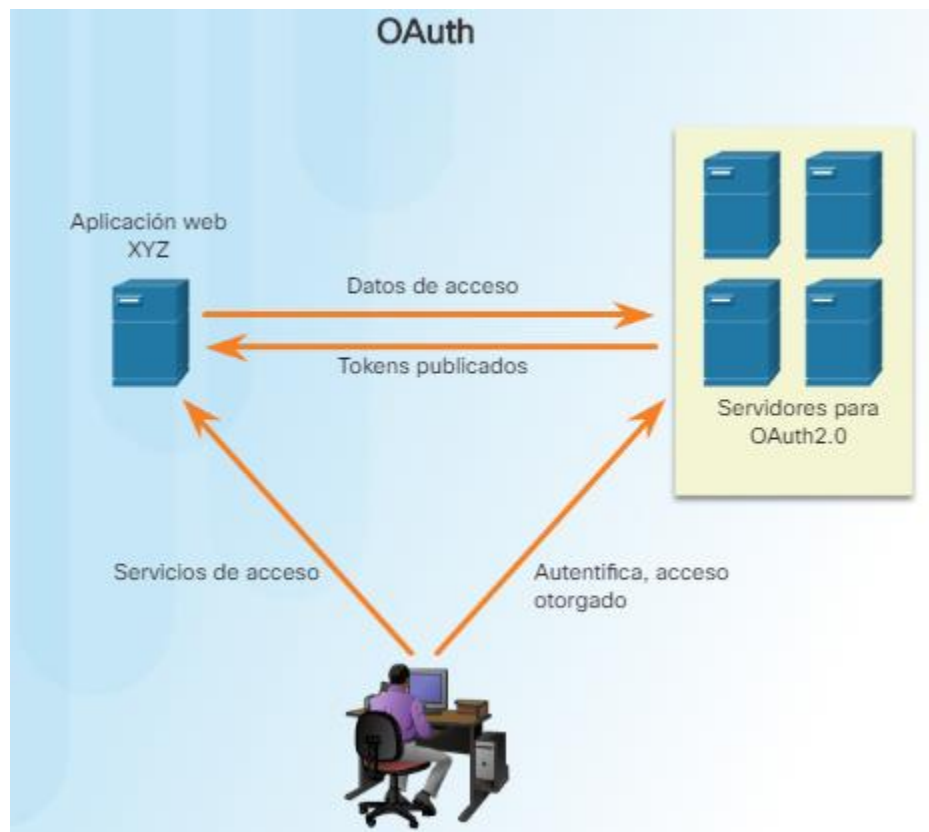
Open Authorization (OAuth) es un protocolo de estándar abierto que permite que las credenciales de los usuarios finales tengan acceso a aplicaciones de terceros sin exponer las contraseñas de los usuarios. OAuth actúa como intermediario para decidir si los usuarios finales pueden acceder a aplicaciones de terceros. Por ejemplo, supongamos que desea acceder a la aplicación web XYZ y no tiene una cuenta de usuario para acceder a esta aplicación web. Sin embargo, XYZ tiene la opción de permitirle iniciar sesión con las credenciales de la red social ABC. Por lo que puede acceder al sitio web XYZ con el inicio de sesión de la red social ABC.

Para que esto funcione, la aplicación 'XYZ' se registra con 'ABC' y es una aplicación aprobada. Cuando accede a XYZ, utiliza sus credenciales de usuario para ABC. Luego XYZ solicita un token de acceso a ABC en su nombre. Ahora tiene acceso a XYZ. XYZ no tiene ninguna información sobre usted y sus credenciales de usuario; esta interacción es completamente transparente para el usuario. El uso de tokens secretos impide que una aplicación maliciosa obtenga su información y sus datos.

- 

Incluso con la autenticación de dos factores, los hackers aún pueden obtener acceso a sus cuentas en línea mediante ataques tales como suplantación de identidad, malware e ingeniería social.

Haga clic [aquí](#) para detectar si los sitios web que visita usan la autenticación de dos factores.



## No comparta demasiado en las redes sociales

---

Si desea mantener su privacidad en las redes sociales, comparta la menor información posible. No debe compartir información como su fecha de nacimiento, dirección de correo electrónico o número de teléfono en su perfil. La persona que necesita conocer su información personal probablemente ya la sepa. No complete su perfil de redes sociales en su totalidad, solo proporcione la información mínima requerida. Además, verifique las configuraciones de sus redes sociales para permitir que solo las personas que conoce vean sus actividades o participen en sus conversaciones.

Mientras más información personal comparta en línea, más fácil será para alguien crear un perfil sobre usted y aprovecharse de usted fuera de línea.

¿Alguna vez ha olvidado el nombre de usuario y la contraseña de una cuenta en línea? Las preguntas de seguridad tales como "¿Cuál es el nombre de su madre?" o "¿En qué ciudad nació?" supuestamente deben ayudar a mantener su cuenta protegida de intrusiones. Sin embargo, cualquier persona que desee acceder a sus cuentas puede buscar las respuestas en Internet. Puede responder estas preguntas con información falsa, siempre que recuerde las respuestas falsas. Si tiene un problema para recordarlas, puede usar el administrador de contraseñas para que las administre.

## Privacidad del correo electrónico y el navegador web

---

Cada día, millones de mensajes de correo electrónico se utilizan para comunicarse con amigos y realizar negocios. El correo electrónico es una manera conveniente de comunicarse rápidamente. Cuando envía un correo electrónico, es similar a enviar un mensaje mediante una tarjeta postal. El mensaje de la tarjeta postal se transmite a plena vista de cualquier persona que pueda observarlo; el mensaje de correo electrónico se transmite en texto sin formato y es legible para cualquier persona que tenga acceso. Estas comunicaciones

además pasan por diferentes servidores en la ruta hacia su destino. Incluso si borra los mensajes de correo electrónico, los mensajes pueden archivarse en los servidores de correo durante algún tiempo.

Cualquier persona con acceso físico a su computadora o a su router puede ver qué sitios web ha visitado con el historial del navegador web, el caché y posiblemente los archivos de registro. Este problema puede minimizarse habilitando el modo de navegación privada en el navegador web. La mayoría de los exploradores web populares tienen un nombre propio para el modo de navegación privada:

- **Microsoft Internet Explorer:** InPrivate
- **Google Chrome:** Incognito
- **Mozilla Firefox:** ventana privada/pestaña privada
- **Safari:** navegación privada

Al utilizar el modo privado, se deshabilitan las cookies y los archivos temporales de Internet y el historial de exploración se eliminan después de cerrar la ventana o el programa.

Mantener su historial de exploración de Internet privado puede impedir que otros recopilen información sobre sus actividades en línea y lo tienen para comprar algo con publicidad dirigida. Incluso con la navegación privada habilitada y las cookies desactivadas, las empresas desarrollan diferentes maneras de identificar usuarios para recopilar información y seguir el comportamiento de los usuarios. Por ejemplo, los dispositivos intermediarios, como los routers, pueden tener información sobre el historial de navegación web del usuario.

En última instancia, es su responsabilidad proteger sus datos, su identidad y sus dispositivos informáticos. Cuando envía un correo electrónico, ¿debe incluir su historial médico? La próxima vez que busque en Internet, ¿será segura su transmisión? Simplemente algunas precauciones pueden ahorrarle problemas en el futuro.

## Laboratorio: descubra su propio comportamiento riesgoso en línea

---

En esta práctica de laboratorio, identificará comportamientos riesgosos en línea y explorará algunas sugerencias sobre cómo aumentar la seguridad en línea.

[Laboratorio: descubrir su propio comportamiento riesgoso en línea](#)

## Capítulo 4: Protección de la organización

---

Este capítulo abarca algunos de los procesos y tecnologías utilizados por los profesionales de la ciberseguridad para proteger la red, equipos y los datos de una organización. Primero, explica brevemente los tipos de firewalls, dispositivos de seguridad y software que se utilizan actualmente, incluidas las mejores prácticas

Luego, este capítulo explica los botnets, the kill chain, la seguridad basada en comportamientos y el uso de NetFlow para monitorear una red.

Abarca brevemente las herramientas que los profesionales de la ciberseguridad utilizan para detectar y prevenir los ataques a la red. Abarca brevemente las herramientas que los profesionales de la ciberseguridad utilizan para detectar y prevenir los ataques a red.

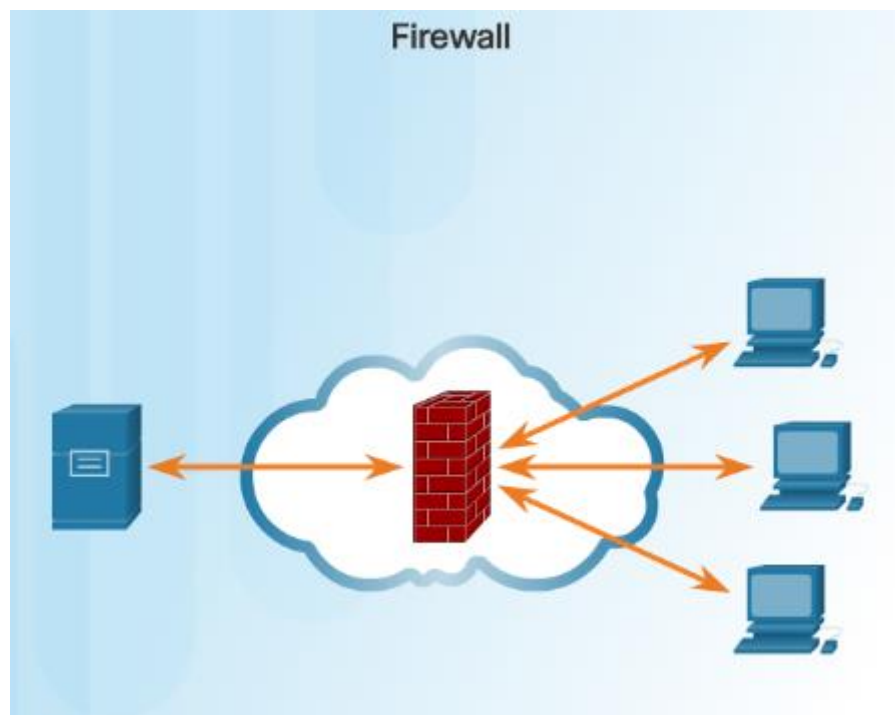
### Tipos de firewall

---

Un firewall (cortafuegos) es un muro o partición diseñada para evitar que el fuego se propague de una parte a otra de un edificio. En las redes de computadoras, un firewall está diseñado para controlar o filtrar la entrada o salida de comunicaciones de un dispositivo o una red, como se muestra en la figura. Un firewall puede instalarse en una única computadora con el propósito de proteger dicha computadora (firewall ejecutado en un host) o puede ser un dispositivo de red independiente que protege toda una red de computadoras y todos los dispositivos host en dicha red (firewall basado en la red).

Durante años, dado que los ataques a la computadora y la red se han vuelto más sofisticados, se han desarrollado nuevos tipos de firewalls que atienden diferentes fines en la protección de la red. Esta es una lista de los tipos de firewall comunes:

- **Firewall de capa de red:** filtrado basado en las direcciones IP de origen y destino.
- **Firewall de capa de transporte:** filtrado basado en puertos de origen y datos de destino y filtrado basado en los estados de conexión.
- **Firewall de capa de aplicación:** filtrado basado en la aplicación, el programa o el servicio.
- **Firewall de aplicación consciente del contexto:** filtrado basada en el usuario, el dispositivo, la función, el tipo de aplicación y el perfil de amenazas.
- **Servidor proxy:** filtrado de solicitudes de contenido web, como URL, dominio, medios, etcétera.
- **Servidor de proxy inverso:** ubicados frente a los servidores web, los servidores de proxy inversos protegen, ocultan, descargan y distribuyen el acceso a los servidores web.
- **Firewall de traducción de direcciones de red (NAT):** ocultan o enmascaran las direcciones privadas de los hosts de red.
- **Firewall basado en host:** filtrado de puertos y llamadas de servicio del sistema en el sistema operativo de una computadora.



### Actividad: Identificar el tipo de firewall

Tipo	Descripción
✓ NAT	Oculta o enmascara las direcciones privadas de los hosts de la red.
✓ Servidor proxy	Filtrado de las solicitudes de contenido web.
✓ Basado en el host	Filtrado de puertos y llamadas de servicio al sistema en un sistema operativo de computadora.
✓ Sensible al contexto	Filtrado basado en el usuario, el dispositivo, la función y el perfil de la amenaza.
✓ Capa de transporte	Filtrado basado en los puertos de datos de origen y destino, y estados de la conexión.
✓ Servidor proxy inverso	Se coloca por encima de los servidores web para proteger, ocultar, descargar y distribuir el acceso a los servidores web.
✓ Capa de aplicación	Filtrado basado en el programa o el servicio.
✓ Capa de red	Filtrado basado en las direcciones IP de origen y destino.

## Escaneo de puertos

El escaneo de puertos es un proceso de comprobación de una computadora, un servidor u otro host de red para conocer los puertos abiertos. En redes, a cada aplicación que se ejecuta en un dispositivo se le asigna un identificador llamado número de puerto. Este número de puerto se utiliza en ambos extremos de la transmisión para asegurar que los datos estén llegando a la aplicación correcta. El escaneo de puertos se puede utilizar con fines maliciosos como una herramienta de reconocimiento, para identificar el sistema operativo y los servicios que se ejecutan en una computadora o un host, o se puede utilizar inofensivamente por parte de un administrador de red para verificar las políticas de seguridad en la red.

Con el propósito de evaluar el firewall de la red de computadoras y la seguridad de los puertos, puede utilizar una herramienta de escaneo de puertos, como Nmap, para encontrar todos los puertos abiertos en su red. El escaneo de puertos se puede considerar como precursor para un ataque a la red y, por lo tanto, no debe realizarse en servidores públicos en Internet o en la red de una empresa sin permiso.

Para ejecutar el escaneo de puertos Nmap de una computadora en la red doméstica local, descargue y ejecute un programa como Zenmap, proporcione la dirección IP de destino de la computadora que desea analizar, elija un perfil de escaneo predeterminado y presione Escanear. El escaneo de Nmap reportará cualquier servicio que se esté ejecutando (como servicios web, servicios de correo, etc.) y los números de puerto. El escaneo de puertos generalmente provoca alguna de estas tres respuestas:

- **Abierto o aceptado:** el host respondió e indicó que hay un servicio activo en el puerto.
- **Cerrado, denegado o no escucha:** el host respondió e indicó que se denegarán las conexiones en el puerto.
- **Filtrado, caído o bloqueado:** no hubo respuesta del host.



Para ejecutar escaneo del puerto desde fuera de la red, deberá iniciar el escaneo desde fuera de la red. Esto implicará la ejecución de un escaneo de puertos de Nmap con la dirección IP pública del firewall o router. Para obtener su dirección IP pública, utilice un motor de búsqueda, como Google, con la consulta "cuál es mi dirección IP". El motor de búsqueda le devolverá su dirección IP pública.

Para ejecutar un escaneo de los seis puertos más comunes de un router o firewall doméstico, vaya al escáner de puertos en línea de Nmap en <https://hackertarget.com/nmap-online-port-scanner/> e ingrese su dirección IP pública en el cuadro del formulario: *dirección IP para escanear...* y presione *Escaneo rápido de Nmap*. Si la respuesta es *Abierta* para cualquiera de los puertos: 21, 22, 25, 80, 443 o 3389, lo más probable es que esté habilitado el reenvío de puertos en el router o firewall y que ejecute servidores en su red privada, como se muestra en la figura.

### Resultados del escaneo de puertos Nmap

**Service/puerto abierto y SO** → **22/tcp open ssh OpenSSH 6.7p1 Raspbian 5 (protocol 2.0)**

**Servicio/puerto abierto** → **80/tcp open http Apache httpd 2.4.18 ((Raspbian))**

**NIC/Plataforma** → **MAC Address: 88:27:EB:77:E3:EB (Raspbian Pi Foundation)**

**Núcleo del SO** → **Running: Linux 3.X[4.X]**

**OS details:** Linux 3.2 - 4.0

**OS type:** Raspbian

**OS details:** Linux 3.2 - 4.0

**Uptime guess:** 6.004 days (since Tue Mar 01 09:52:48 2016)

**Network Distance:** 1 hop

**TCP Sequence Prediction:** Difficulty=201 (Good luck!)

**IP ID Sequence Generation:** All zeros

**Service Info:** OS: Linux; CPE: cpe:/o:linux:linux\_kernel

**TRACEROUTE**

HOP	RTT	ADDRESS
1	1.90 ms	192.168.3.61

**NSE:** Script Post-scanning.

Initiating NSE at 09:58

Completed NSE at 09:58, 0.00s elapsed

Initiating NSE at 09:58

Completed NSE at 09:58, 0.00s elapsed

### Actividad: Identificar la respuesta de un escaneo de puertos

✓	El host no respondió	▼	Descartada
✓	Un host respondió ini	▼	No escucha
✓	Un host respondió ini	▼	Cerrado
✓	Un host respondió ini	▼	Abierta
✓	El host no respondió	▼	Filtrado
✓	Un host respondió ini	▼	Denegado
✓	Un host respondió ini	▼	Aceptado

## Dispositivos de seguridad

Hoy no existe un dispositivo de seguridad o una tecnología que resuelva todas las necesidades de seguridad de la red por sí solo. Debido a que hay una variedad de dispositivos de seguridad y herramientas que deben implementarse, es importante que trabajen en conjunto. Los dispositivos de seguridad son más efectivos cuando forman parte de un sistema.

Los dispositivos de seguridad pueden ser dispositivos independientes, como un router o firewall, una tarjeta que puede instalarse en un dispositivo de red o un módulo con su propio procesador y memoria en caché. Los dispositivos de seguridad también pueden ser herramientas de software que se ejecutan en un dispositivo de red. Los dispositivos de seguridad se dividen en las siguientes categorías generales:

**Routers:** los routers de servicios integrados (ISR) Cisco, como se muestra en la Figura 1, tienen muchas capacidades similares a las de un firewall además de las funciones de ruteo, entre ellas, el filtrado de tráfico, la capacidad de ejecutar un sistema de prevención de intrusiones (IPS), el cifrado y las capacidades de VPN para las conexiones de cifrado seguro.

**Firewalls:** los firewalls de nueva generación de Cisco tienen todas las capacidades de un router ISR además de análisis y administración de redes avanzadas. El dispositivo de seguridad adaptable (ASA, por sus siglas en inglés) de Cisco con funcionalidades de firewall se muestra en la Figura 2.

**IPS:** los dispositivos IPS de nueva generación, que se muestran en la Figura 3, están dedicados a la prevención de intrusiones.

**VPN:** los dispositivos de seguridad de Cisco cuentan con tecnologías de redes virtuales privadas (VPN) tanto de cliente como servidor. Están diseñados para conexiones de cifrado seguro.

**Malware/antivirus:** Cisco Advanced Malware Protection (AMP) viene en los routers de nueva generación de Cisco, como también en los firewalls, los dispositivos IPS y los dispositivos de seguridad web y de correo electrónico y además puede instalarse como software en los equipos host.

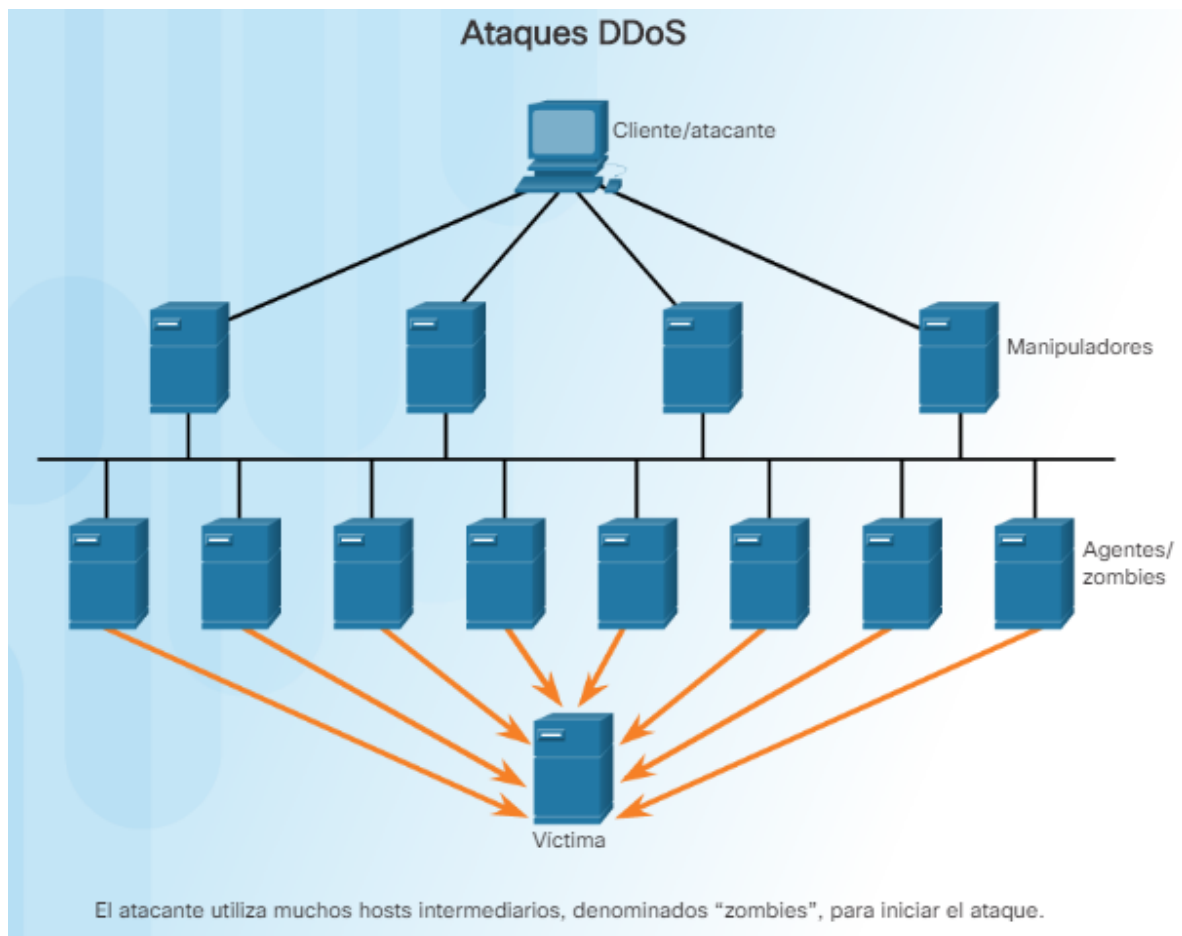
**Otros dispositivos de seguridad:** esta categoría incluye dispositivos de seguridad web y de correo electrónico, dispositivos de descifrado, servidores de control de acceso del cliente y sistemas de administración de seguridad.

Actividad: Identificar los dispositivos de seguridad	
Dispositivo de seguridad	Descripción
✓ IPS	Dedicado a la prevención de intrusiones.
✓ AMP	Se ofrece en los dispositivos de nueva generación y también puede instalarse como software en los equipos host.
✓ VPN	Están diseñados para túneles de cifrado seguro.
✓ Router	Tiene muchas capacidades además de las funciones de routing, entre ellas, filtrado de tráfico, cifrado y capacidades para túneles de cifrado seguro.
✓ Firewall	Cuenta con todas las capacidades de un ISR, además de administración y análisis avanzados de red.

## Detección de ataques en tiempo real

El software no es perfecto. Cuando un hacker explota un defecto de un software antes de que el creador pueda corregirlo, se conoce como ataque de día cero. Debido a la complejidad y tamaño de los ataques de día cero que se encuentran actualmente, no es extraño que los ataques a la red tengan éxito y que el éxito de su defensa ahora se mida según la rapidez con la que una red responde ante un ataque. La capacidad de detectar ataques mientras suceden en tiempo real, así como de detenerlos inmediatamente o en cuestión de minutos, es el objetivo ideal. Desafortunadamente, muchas empresas y organizaciones a día de hoy no pueden detectar los ataques sino hasta días o incluso meses después de ocurridos.

- **Análisis en tiempo real de principio a fin:** Detectar ataques en tiempo real requiere el análisis activo mediante el firewall y los dispositivos de red IDS/IPS. También debe usarse la detección de malware de cliente/servidor de nueva generación con conexiones a los centros de amenazas globales en línea. En la actualidad, el software y los dispositivos de análisis activos deben detectar anomalías de red mediante la detección de comportamientos y el análisis basado en el comportamiento.
- **Ataques DDoS y respuesta en tiempo real:** El ataque DDoS es una de las mayores amenazas que requiere la detección y respuesta en tiempo real. Es extremadamente difícil defenderse contra los ataques de DDoS porque los ataques se originan en cientos o miles de hosts zombis y aparecen como tráfico legítimo, como se muestra en la figura. Para muchas empresas y organizaciones, los ataques DDoS ocurren de forma regular y paralizan los servidores de Internet y la disponibilidad de la red. La capacidad para detectar y responder a los ataques DDoS en tiempo real es crucial.



## Protección contra el malware

¿Cómo proporciona la defensa contra la presencia constante de ataques de día cero y las amenazas persistentes avanzadas (APT, por sus siglas en inglés) que roban datos durante largos períodos de tiempo? Una solución es utilizar una aplicación de detección de malware avanzada de nivel empresarial que ofrezca detección de malware en tiempo real.

Los administradores de red deben monitorear constantemente la red para detectar signos de malware o comportamientos que revelan la presencia de una APT. Cisco cuenta con Advanced Malware Protection (AMP) Threat Grid, que analiza millones de archivos y los correlaciona con cientos de millones de otros objetos de malware analizados. Esto brinda a los clientes una vista global de las campañas, la distribución y los ataques de malware. AMP es un software de Cliente/Servidor implementado en terminales de host, como servidor independiente, o en otros dispositivos de seguridad de la red. La figura muestra los beneficios de AMP Threat Grid.



## Buenas prácticas de seguridad

Muchas organizaciones nacionales y profesionales han publicado listas de buenas prácticas de seguridad. La siguiente es una lista de algunas de las buenas prácticas de seguridad:

- **Realizar una evaluación de riesgos:** conocer el valor de lo que protege ayuda a justificar los gastos de seguridad.
- **Crear una política de seguridad:** cree una política que delimite claramente las reglas de la empresa, las tareas y las expectativas.
- **Medidas de seguridad física:** restringen el acceso a los centros de datos, a las ubicaciones de servidores y a los extintores.
- **Medidas de seguridad de recursos humanos:** los empleados deben ser correctamente investigados con comprobaciones de antecedentes.
- **Efectuar y probar las copias de respaldo:** realice copias de respaldo periódicas y pruebe los datos recuperados de las copias de respaldo.
- **Mantener parches y actualizaciones de seguridad:** actualice periódicamente los servidores, computadoras, los programas y sistemas operativos de los dispositivos de red.
- **Implementar controles de acceso:** configure los roles de usuario y los niveles de privilegio, así como una autenticación de usuario sólida.

- **Revisar periódicamente la respuesta ante incidentes:** utilice un equipo de respuesta ante incidentes y pruebe los escenarios de respuesta ante emergencias.
- **Implementar una herramienta de administración, análisis y supervisión de red:** seleccione una solución de monitoreo de seguridad que se integre con otras tecnologías.
- **Implementar dispositivos de seguridad de la red:** utilice routers de nueva generación, firewalls y otros dispositivos de seguridad.
- **Implementar una solución de seguridad integral para terminales:** utilice software antivirus y antimalware de nivel empresarial.
- **Informar a los usuarios:** educar a los usuarios y a los empleados sobre los procedimientos seguros.
- **Cifrar los datos:** cifrar todos los datos confidenciales de la empresa, incluido el correo electrónico.

Algunas de las pautas más útiles se encuentran en los depósitos organizacionales, como el Centro de Recursos de Seguridad Informática del Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés), según se muestra en la figura.

Una de las organizaciones más conocidas y respetadas para la capacitación en ciberseguridad es el SANS Institute. Haga clic [aquí](#) para obtener más información sobre SANS y los tipos de capacitación y certificaciones que ofrece.



Botnet

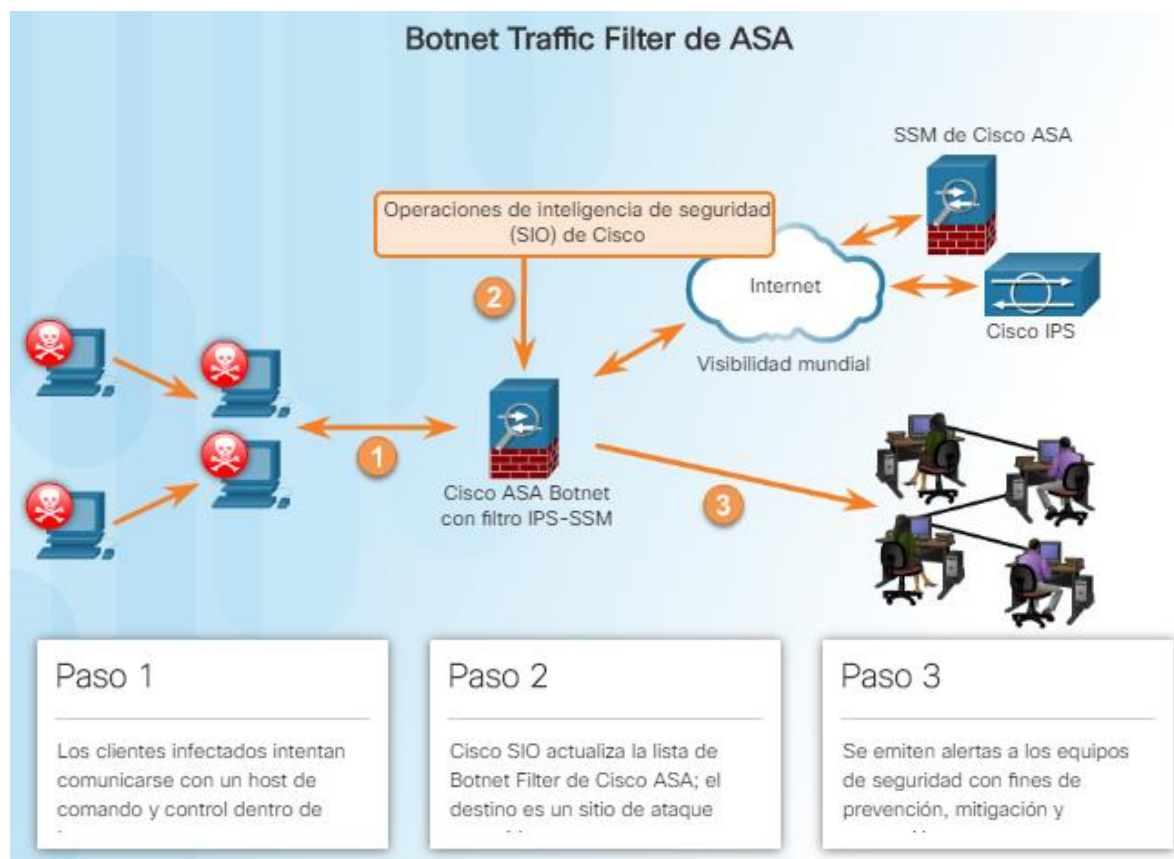


Un botnet es un grupo de bots conectados a través de Internet con la capacidad de ser controlados por un individuo o grupo malicioso. Una computadora bot se infecta generalmente por visitar un sitio web, abrir un elemento adjunto de correo electrónico o abrir un archivo de medios infectado.

Un botnet puede tener decenas de miles o incluso cientos de miles de bots. Estos bots se pueden activar para distribuir malware, lanzar ataques DDoS, distribuir correo electrónico no deseado o ejecutar ataques de contraseña por fuerza bruta. Los botnets por lo general se controlan a través de un servidor de comando y control.

Los delincuentes cibernéticos alquilan a menudo los botnets, por un monto, a otros proveedores para fines infames.

La figura muestra cómo un filtro de tráfico de botnet se utiliza para informar a la comunidad de seguridad mundial las ubicaciones de los botnets.



## Cadena de eliminación o proceso de ataque (Kill Chain) en la ciberdefensa

En la ciberseguridad, la cadena de eliminación o proceso de ataque (Kill Chain) representa las etapas de un ataque a los sistemas de información. Desarrollada por Lockheed Martin como marco de seguridad para la respuesta y la detección de incidentes, la cadena de eliminación consta de los siguientes pasos:

**Etapas 1. Reconocimiento:** el atacante recopila información sobre el objetivo.

**Etapla 2. Armamentización:** el atacante crea un ataque y contenido malicioso para enviar al objetivo.

**Etapla 3. Entrega:** el atacante envía el ataque y la carga maliciosa al objetivo por correo electrónico u otros métodos.

**Etapla 4. Explotación:** se ejecuta el ataque.

**Etapla 5. Instalación:** el malware y las puertas traseras se instalan en el objetivo.

**Etapla 6. Mando y control:** se obtiene el control remoto del objetivo mediante un servidor o canal de comando y control.

**Etapla 7. Acción:** el atacante realiza acciones maliciosas, como el robo de información, o ejecuta ataques adicionales en otros dispositivos desde dentro de la red a través de las etapas de la cadena de eliminación nuevamente.

Para defendernos de la cadena de eliminación, existen acciones de seguridad diseñadas en torno a las etapas de la cadena de eliminación. Estas son algunas preguntas sobre las defensas de seguridad de una empresa en función de la cadena de eliminación:

- ¿Cuáles son los indicadores de ataque en cada etapa de la cadena de eliminación?
- ¿Qué herramientas de seguridad son necesarias para detectar los indicadores de ataque en cada una de las etapas?
- ¿Hay brechas en la capacidad de la empresa para detectar un ataque?

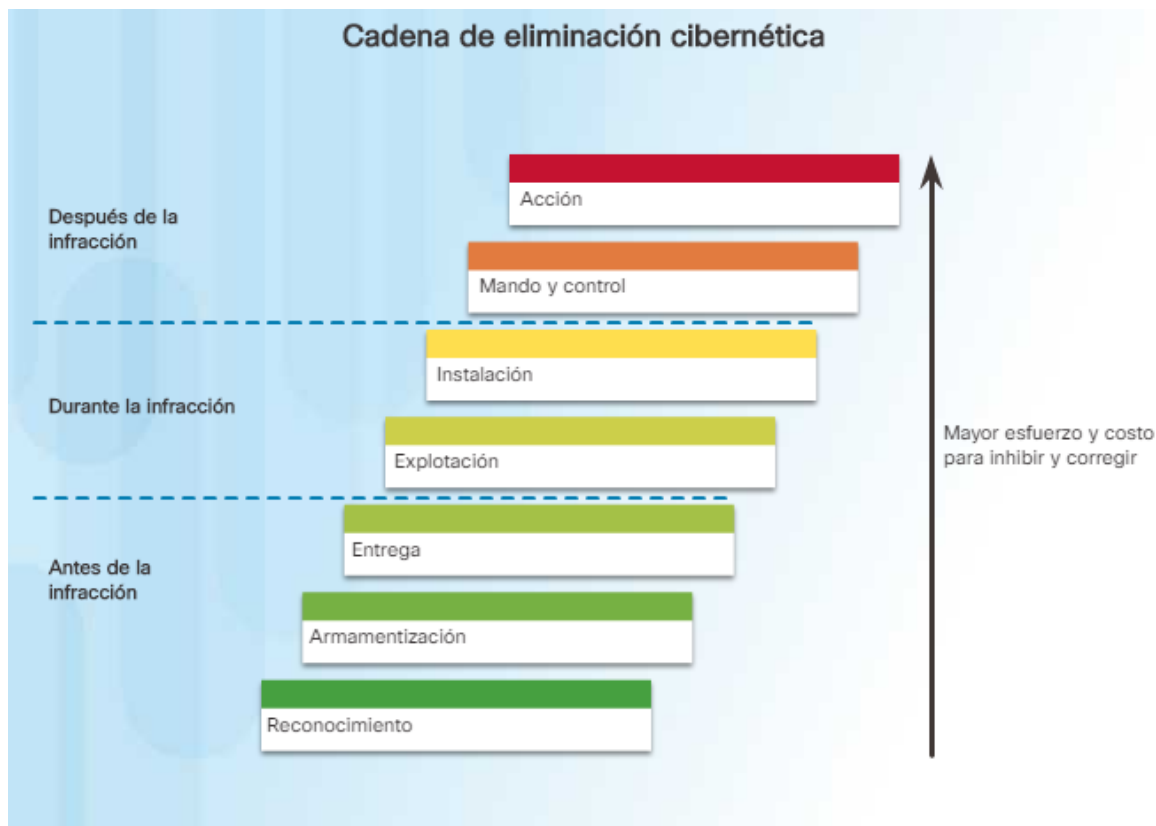
Según Lockheed Martin, comprender las etapas de la cadena de eliminación permite poner obstáculos defensivos, demorar el ataque y, finalmente, evitar la pérdida de datos. La figura muestra cómo cada etapa de la cadena de eliminación equivale a un aumento en la cantidad de esfuerzo y costos para impedir y corregir ataques.



## Actividad: Ordenar las etapas de la cadena de destrucción

e la

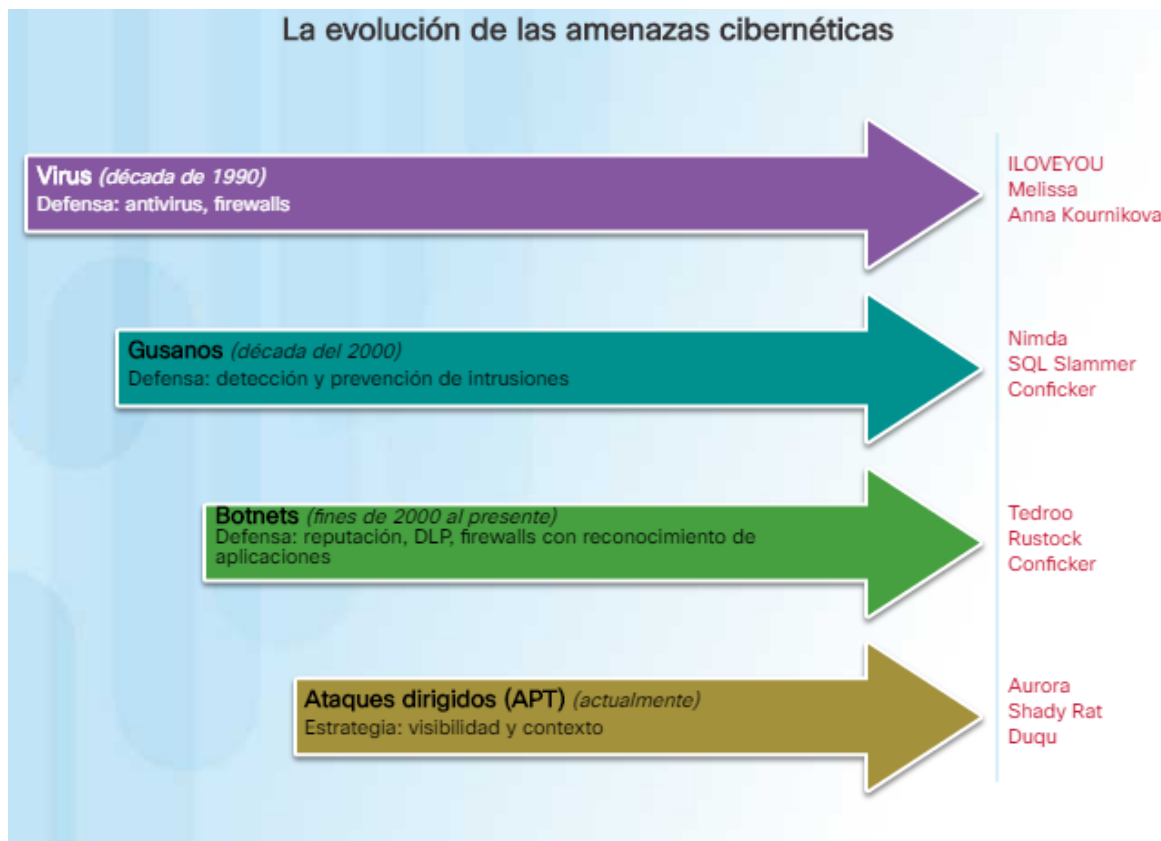
Término	Descripción
 Etapa 3	Entrega
 Etapa 7	Acción
 Etapa 6	Comando y control
 Etapa 1	Reconocimiento
 Etapa 5	Instalación
 Etapa 4	Ataque
 Etapa 2	Armamentización



## Seguridad basada en el comportamiento

La seguridad basada en el comportamiento es una forma de detección de amenazas que no depende de las firmas malintencionadas conocidas, pero que utiliza el contexto informativo para detectar anomalías en la red. La detección basada en el comportamiento implica la captura y el análisis del flujo de comunicación entre un usuario de la red local y un destino local o remoto. Estas comunicaciones, cuando se detectan y analizan, revelan el contexto y los patrones de comportamiento que se pueden usar para detectar anomalías. La detección basada en el comportamiento puede detectar la presencia de un ataque mediante un cambio en el comportamiento normal.

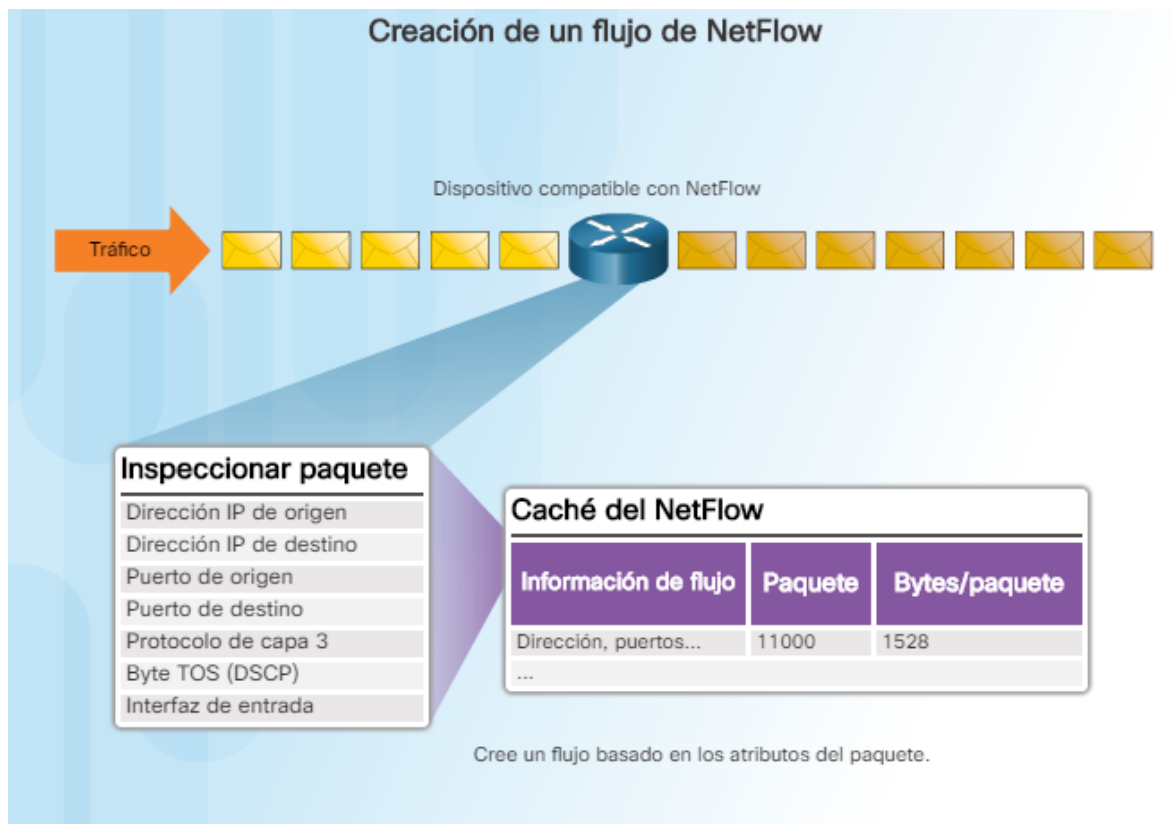
- **Honeypot:** una honeypot es una herramienta de detección basada en el comportamiento que primero atrae al atacante apelando al patrón previsto de comportamiento malicioso del atacante; una vez dentro de la honeypot, el administrador de la red puede capturar, registrar y analizar el comportamiento del atacante. Esto permite que un administrador gane más conocimiento y construya una mejor defensa.
- **Arquitectura de Cyber Threat Defense Solution de Cisco:** esta es una arquitectura de seguridad que utiliza la detección basada en el comportamiento e indicadores para proporcionar mayor visibilidad, contexto y control. El objetivo es definir quién, qué, dónde, cuándo y cómo se produce un ataque. Esta arquitectura de seguridad utiliza muchas tecnologías de seguridad para lograr este objetivo.



## NetFlow

La tecnología NetFlow se usa para recopilar información sobre los datos que atraviesan la red. La información de NetFlow se puede comparar con una factura telefónica por el tráfico de la red. Muestra quién y qué dispositivos están en la red también como y cuando los usuarios y dispositivos tuvieron acceso a la red. NetFlow es un componente importante del análisis y la detección basados en el comportamiento. Los switches, routers y firewalls equipados con NetFlow pueden comunicar información sobre los datos que ingresan, egresan y viajan por la red. La información se envía a los recopiladores de NetFlow que recopilan, almacenan y analiza los registros de NetFlow.

NetFlow puede recopilar información sobre el uso a través de muchas características diferentes de cómo se transportan los datos por la red, como se muestra en la figura. Mediante la recopilación de la información sobre los flujos de datos de la red, NetFlow puede establecer comportamientos de línea base en más de 90 atributos diferentes.



## CSIRT

Muchas organizaciones grandes tienen un Equipo de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) para recibir, revisar y responder a informes de incidentes de seguridad informática, como se muestra en la Figura 1. La función principal del CSIRT es ayudar a proteger la empresa, el sistema y la preservación de datos realizando investigaciones integrales de los incidentes de seguridad informática. Para evitar incidentes de seguridad, el CSIRT de Cisco proporciona una evaluación de amenazas proactiva, planificación de la mitigación, análisis de tendencias de incidentes y revisión de la arquitectura de seguridad, como se muestra en la Figura 2.

El CSIRT de Cisco colabora con el Foro de respuesta ante los incidentes y los equipos de seguridad (FIRST), el Intercambio de información de seguridad nacional (NSIE), el Intercambio de información de seguridad de defensa (DSIE) y el Centro de Investigación y Análisis de operaciones DNS (DNS-OARC).

Hay organizaciones de CSIRT nacionales y públicas, como la División CERT del Instituto de Ingeniería de Software de la Universidad Carnegie Mellon, que están dispuestos a ayudar a las organizaciones, y a los CSIRT nacionales, a desarrollar, utilizar y mejorar sus capacidades de administración de incidentes.

## Organizaciones CSIRT



Software Engineering Institute

Carnegie Mellon University

## CSIRT de Cisco



### Respuesta del CSIRT de Cisco contra el Heartbleed

#### Preparación

- Se escanearon 1,2 millones de servidores vulnerables; 300 necesitaron reparación.
- Ayudó a desarrollar firmas para Sourcefire y los IDS de Cisco.
- Firmas implementadas en los IDS.

#### Supervisión y respuesta

- Se descubrieron 25 ataques: 21 benignos, 4 maliciosos.
- Ataque investigado vía NetFlow para determinar las conexiones normales de las anomalías y maliciosas.

# Libro de estrategias de seguridad

---

La tecnología cambia constantemente. Esto significa que los ciberataques también evolucionan. Continuamente se descubren nuevas vulnerabilidades y métodos de ataque. La seguridad se ha convertido en una preocupación importante para las empresas debido a la reputación y el impacto financiero resultantes de las violaciones a la seguridad. Los ataques están dirigidos a redes críticas y datos confidenciales. Las organizaciones deben tener planes para prepararse, para tratar las violaciones a la seguridad y recuperarse de estas.

Una de las mejores maneras de prepararse para una violación a la seguridad es prevenirla. Se deben tener pautas sobre cómo identificar el riesgo de la ciberseguridad en los sistemas, los activos, los datos y las funcionalidades, proteger el sistema mediante la implementación de protecciones y capacitaciones del personal, y detectar el evento de ciberseguridad lo más rápidamente posible. Cuando se detecta una violación a la seguridad, deben adoptarse las acciones adecuadas para minimizar el impacto y los daños. El plan de respuesta debe ser flexible con múltiples opciones de acción durante la violación. Una vez contenida la violación y restaurados los sistemas y servicios comprometidos, las medidas de seguridad y los procesos deben actualizarse para incluir las lecciones aprendidas durante la violación.

Toda esta información se debe recopilar en un libro de estrategias de seguridad. Un libro de estrategias de seguridad es un conjunto de consultas repetidas (informes) de fuentes de datos de eventos de seguridad que conducen a la detección y la respuesta ante los incidentes. Idealmente, el libro de estrategias de seguridad debe cumplir las siguientes acciones:

- Detectar equipos infectados con malware.
- Detectar actividad de red sospechosa.
- Detectar intentos de autenticación irregulares.
- Describir y entender el tráfico entrante y saliente.
- Proporcionar información de resumen que incluya tendencias, estadísticas y recuentos.
- Proporcionar acceso rápido y utilizable a estadísticas y métricas.
- Establecer una correspondencia de eventos en todas las fuentes de datos relevantes.

## Herramientas para prevención y detección de incidentes

---

Estas son algunas de las herramientas utilizadas para detectar y evitar incidentes de seguridad:

- **SIEM:** un sistema de administración de información y eventos de seguridad (SIEM) es un software que recopila y analiza las alertas de seguridad, los registros y otros datos históricos y en tiempo real de los dispositivos de seguridad de la red.
- **DLP:** el software Data Loss Prevention (DLP) es un sistema de hardware o software diseñado para evitar el robo o la fuga de datos confidenciales de la red. El sistema DLP puede concentrarse en la autorización de acceso a los archivos, el intercambio de datos, la copia de datos, la supervisión de la actividad del usuario y más. Los sistemas DLP están diseñados para supervisar y proteger los datos en tres diferentes estados: datos en uso, datos en movimiento y datos almacenados. Los datos en uso se centran en el cliente, los datos en movimiento se refieren a los datos mientras viajan a través de la red y los datos almacenados se refieren al almacenamiento de datos.

- **Cisco ISE y TrustSec:** Cisco Identity Services Engine (Cisco ISE) y Cisco TrustSec aplican el acceso a los recursos de red mediante la creación de políticas de control de acceso basado en roles que segmenta el acceso a la red (usuarios temporales, usuarios móviles, empleados) sin complejidad agregada. La clasificación del tráfico se basa en la identidad del usuario o el dispositivo. Haga clic en Reproducir en la figura para obtener más información sobre el ISE.
- Haga clic [aquí](#) para leer la transcripción de este video.

## IDS e IPS

---

Un sistema de detección de intrusiones (IDS), que se muestra en la figura, es un dispositivo de red exclusivo, o una de varias herramientas en un servidor o firewall que analiza los datos de una base de datos de reglas o firmas de ataque, que busca tráfico malicioso. Si se detecta una coincidencia, el IDS registrará la detección y creará una alerta para el administrador de la red. El sistema de detección de intrusiones no adopta medidas cuando se detecta una coincidencia, por lo que no evita que se produzcan los ataques. El trabajo del IDS es simplemente detectar, registrar y generar informes.

El análisis que realiza el IDS ralentiza la red (esto se denomina latencia). Para evitar el retraso de la red, el IDS generalmente se configura sin conexión, separado del tráfico de red común. Los datos se copian o duplican mediante un switch y luego se reenvían a los IDS para la detección sin conexión. También existen herramientas del IDS que pueden instalarse sobre un sistema operativo de la computadora host, como Linux o Windows.

Un sistema de prevención de intrusiones (IPS) tiene la capacidad de bloquear o denegar el tráfico en función de las coincidencias positivas de la regla o la firma. Uno de los IPS/IDS más reconocidos es Snort. La versión comercial de Snort es Sourcefire de Cisco. Sourcefire tiene la capacidad de realizar el análisis de tráfico y puerto en tiempo real, registrar, buscar y comparar contenido; puede detectar sondas, ataques y escaneos de puertos. También se combina con otras herramientas de terceros para informar y analizar el rendimiento y los registros.



## Actividad: Identificar la terminología del enfoque en ciberseguridad

Término	Descripción
✓ DLP	Un sistema de hardware o software diseñado para evitar el robo o la fuga de datos confidenciales en la red.
✓ Libro de estrategias de seguridad	Un conjunto de consultas repetitivas contra fuentes de datos de eventos de seguridad que conduce a la detección y respuesta ante incidentes.
✓ ISE y TrustSec	Refuerza el acceso a los recursos de red mediante la creación de políticas de control de acceso basadas en roles que segmentan el acceso a la red.
✓ CSIRT	Ayuda a garantizar la preservación de la empresa, el sistema y los datos mediante extensas investigaciones de los incidentes en seguridad informática.
✓ IDS	Analiza la información dentro de la base de datos de reglas o firmas de ataque, registra lo encontrado y crea una alerta para el administrador de red.
✓ SIEM	Software que recopila y analiza alertas de seguridad, registros y otros datos históricos en tiempo real de dispositivos de seguridad en la red.
✓ IPS	Bloquea o niega el tráfico de acuerdo a una regla positiva o una coincidencia de firmas.

## Capítulo 5: ¿Su futuro estará relacionado con la ciberseguridad?

Este capítulo examina las cuestiones legales y éticas que surgen cuando se trabaja en ciberseguridad. También se analizan trayectorias educativas y profesionales en el ámbito de la ciberseguridad. Hay una trayectoria educativa para las certificaciones que desee obtener con Cisco Networking Academy (NetAcad). Algunas de estas certificaciones son requisitos previos a los certificados de especialización en muchas áreas de red, incluida la ciberseguridad.

La página Networking Academy Talent Bridge ([netacad.com](https://netacad.com) en Recursos) proporciona información útil para escribir un excelente currículum y prepararse para una entrevista de trabajo. También contiene listas de trabajos de Cisco y de partners de Cisco. Se presentan tres motores de búsqueda de trabajo en Internet externos para que explore.

## Cuestiones legales en la ciberseguridad

Los profesionales de la ciberseguridad deben tener las mismas habilidades que los hackers, especialmente que los hackers de Sombrero Negro, para ofrecer protección contra los ataques. Una diferencia entre un hacker y un profesional de la ciberseguridad es que el profesional de la ciberseguridad debe trabajar dentro de los límites legales.

### Asuntos legales personales

Ni siquiera tiene que ser un empleado para estar sujetos a las leyes de la ciberseguridad. En su vida privada, puede tener la oportunidad y las habilidades de hackear la computadora o la red de otra persona. Hay un antiguo dicho, "Solo porque puede no significa que deba hacerlo". Tenga en cuenta esto. La mayoría de los hackers dejan huellas, lo sepan o no, y estas huellas pueden rastrearse hasta el hacker.

Los profesionales de la ciberseguridad desarrollan muchas habilidades que se pueden utilizar para bien o mal. Los que utilizan sus habilidades dentro del sistema legal, para proteger la infraestructura, las redes y la privacidad siempre tienen alta demanda.



## Asuntos legales corporativos

La mayoría de los países tienen algunas leyes de ciberseguridad. Pueden tener relación con la infraestructura crítica, las redes, y la privacidad corporativa e individual. Las empresas deben cumplir estas leyes.

En algunos casos, si infringe las leyes de ciberseguridad mientras realiza su trabajo, es posible que sea la empresa la que resulte castigada y usted podría perder su trabajo. En otros casos, podría ser procesado, multado y posiblemente condenado.

Generalmente, si tiene dudas sobre si una acción o un comportamiento pueden ser ilegales, suponga que son ilegales y no los lleve a cabo. Su empresa puede tener un departamento legal o alguien del departamento de Recursos Humanos que puede contestar su pregunta antes de hacer algo ilegal.

## Derecho internacional y ciberseguridad

El área de la ley de ciberseguridad es mucho más nueva que la ciberseguridad en sí. Como se mencionó anteriormente, la mayoría de los países tienen algunas leyes, y habrá más leyes por venir.

## Cuestiones éticas en ciberseguridad

---

Además de trabajar dentro de los límites de la ley, los profesionales de la ciberseguridad también deben demostrar un comportamiento ético.

### Asuntos éticos personales

Una persona puede actuar de manera no ética y no someterse a un proceso legal, multas ni encarcelamiento. Esto se debe a que es posible que la acción no haya sido técnicamente ilegal. Pero eso no significa que el comportamiento sea aceptable. El comportamiento ético es muy fácil de verificar. Es imposible enumerar todos los distintos comportamientos no éticos que puede exhibir alguien con habilidades de ciberseguridad. A continuación, presentamos solo dos. Hágase las siguientes preguntas:

- ¿Me gustaría descubrir que alguien hackeó mi computadora y alteró las imágenes de mis sitios de red social?
- ¿Me gustaría saber que un técnico de TI en el que confiaba para reparar mi red, divulgó a colegas mi información personal, lo que obtuvo mientras trabajaba en mi red?

Si responde 'no' a cualquiera de estas preguntas, entonces no haga esas cosas a los demás.

### Cuestiones éticas corporativas

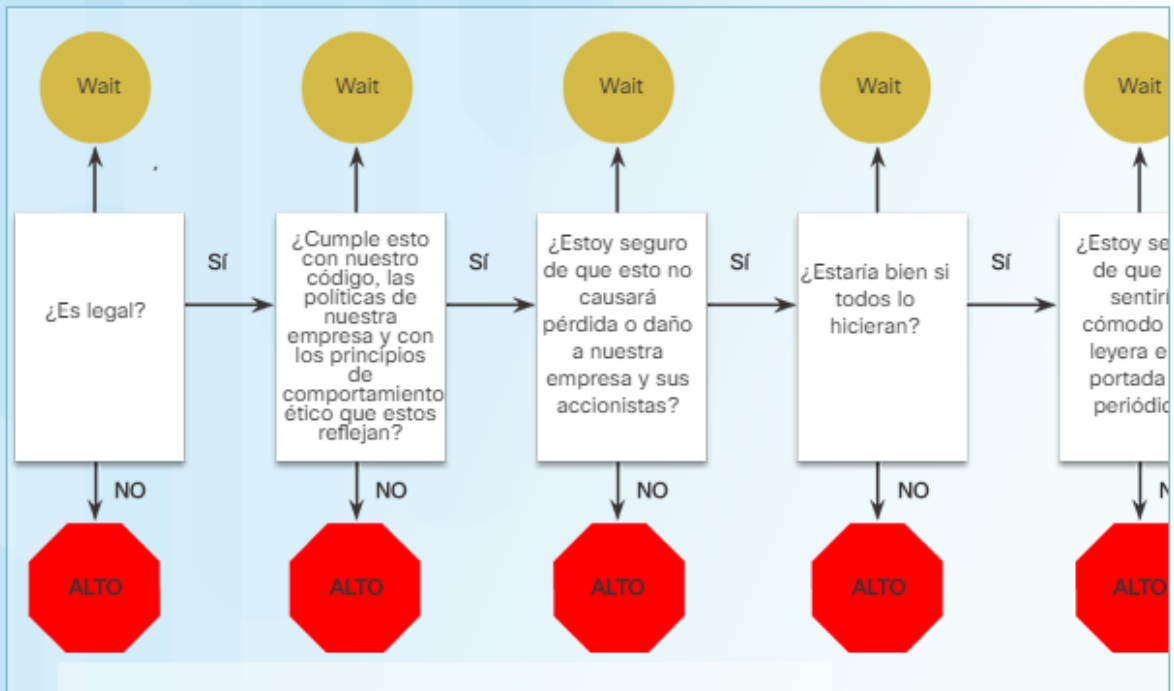
La ética representa los códigos de comportamiento que se aplican a veces por las leyes. Existen muchas áreas en ciberseguridad que no están cubiertas por las leyes. Esto significa que hacer algo que es técnicamente legal puede sin embargo no ser algo ético. Debido a que muchas áreas de ciberseguridad no están (o aún no están) cubiertas por las leyes, muchas organizaciones profesionales de TI han creado códigos de ética para las personas del sector. A continuación, se muestra una lista de tres organizaciones con códigos de ética:


- El Instituto de ciberseguridad (CSI, por sus siglas en inglés) ha emitido un código de ética que puede leer [aquí](#).
- La Asociación de seguridad de sistemas de información (ISSA, por sus siglas en inglés) tiene un código de ético que se encuentra [aquí](#).
- La Asociación de profesionales de la tecnología de la información (AITP, por sus siglas en inglés) tiene un código de ética y un estándar de conducta que se encuentran [aquí](#).


Cisco tiene un equipo dedicado exclusivamente al comportamiento ético comercial. Vaya [aquí](#) para leer más sobre esto. Este [sitio](#) contiene un libro electrónico sobre el Código de conducta comercial de Cisco y un archivo PDF. En los dos archivos hay un “Árbol de decisiones de ética”, como se muestra en la figura. Aunque usted no trabaje para Cisco, las preguntas y respuestas que se encuentran en este árbol de decisiones se pueden aplicar fácilmente a su lugar de trabajo. Al igual que con las preguntas legales, generalmente, si tiene dudas sobre si una acción o un comportamiento podrían resultar inmorales, suponga que lo son y no los lleve a cabo. Puede haber alguien en el departamento de Recursos Humanos o Legal de su empresa que pueda aclarar su situación antes de hacer algo que se consideraría no ético.

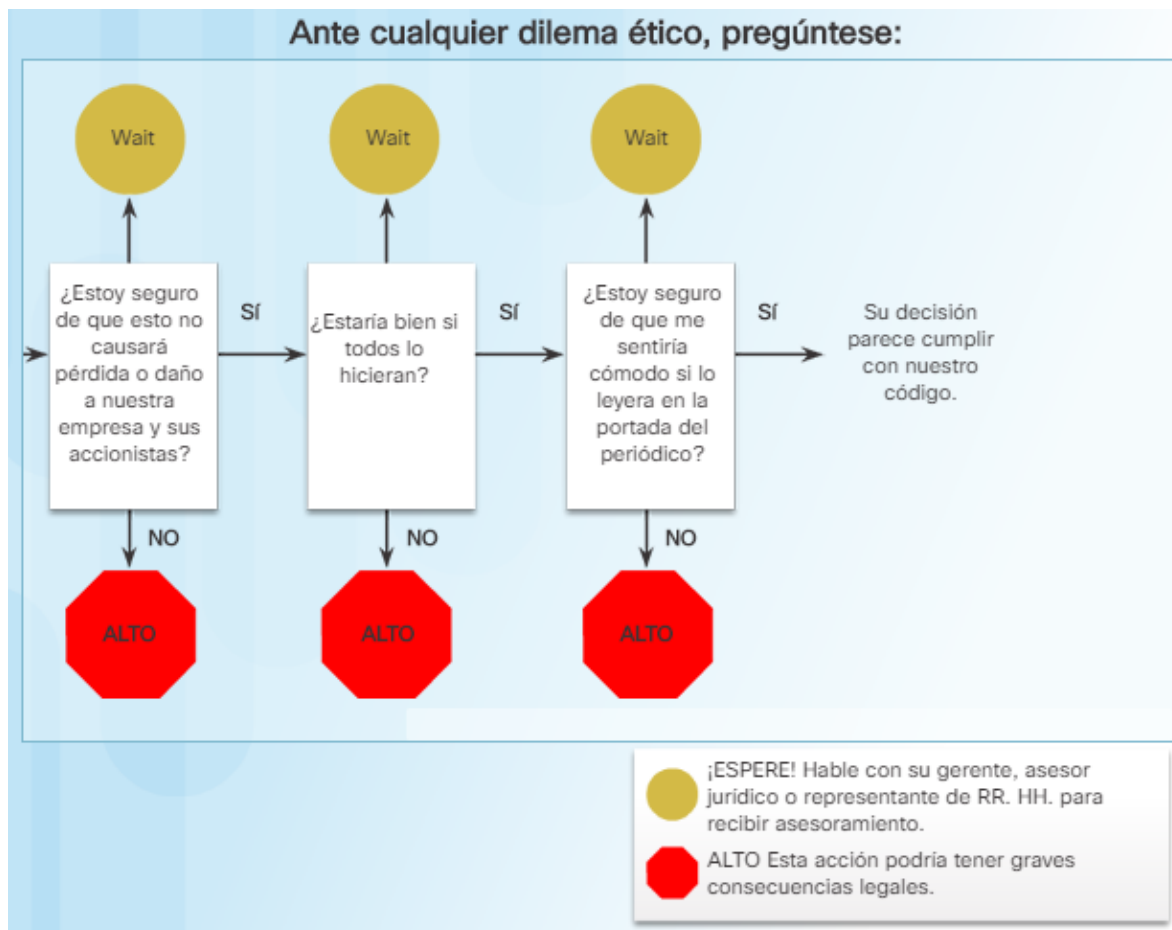
Busque en línea para encontrar otras organizaciones relacionadas con TI con códigos de ética. Intente encontrar lo que tienen en común.

## Ante cualquier dilema ético, pregúntese:



 ¡ESPERE! Hable con su gerente, asesor jurídico o representante de RR. HH. para recibir asesoramiento.

 **ALTO** Esta acción podría tener graves consecuencias legales.



## Puestos de trabajo en ciberseguridad

Muchos otros negocios y sectores están contratando profesionales de la ciberseguridad. Existen varios motores de búsqueda en línea para ayudarlo a encontrar el trabajo correcto en ciberseguridad:

- [ITJobMatch](#) : El motor de búsqueda ITJobMatch se especializa en trabajos de TI de todo tipo, en todo el mundo.
- [Monster](#) : Monster es un motor de búsqueda para todo tipo de trabajo. El enlace provisto va directamente a los trabajos de ciberseguridad.
- [CareerBuilder](#) : CareerBuilder también es un motor de búsqueda para todo tipo de trabajo. El enlace provisto va directamente a los trabajos de ciberseguridad.

Estos son solo tres de muchos sitios diferentes de búsqueda de trabajo en línea. Aunque recién esté comenzando sus estudios en TI y ciberseguridad, utilizar los motores de búsqueda laboral es una buena forma de ver qué tipo de trabajos están disponibles, en todo el mundo.

Según su interés en la ciberseguridad, puede haber distintos tipos de trabajo disponibles para usted, y es posible que requieran certificaciones de habilidades especializadas. Por ejemplo, un analizador de penetración, también conocido como hacker ético, busca y ataca las vulnerabilidades en la seguridad de aplicaciones, redes y sistemas. Para convertirse en analizador de penetración, deberá obtener experiencia en otros trabajos de TI, como administrador de seguridad, administrador de red y administrador del sistema.

Cada uno de estos trabajos requiere su propio conjunto de habilidades que lo ayudarán a convertirse en un activo valioso para una organización.

Esperamos que este curso haya ganado su interés para que se capacite en TI y ciberseguridad, y que, luego, continúe con una carrera emocionante. Cisco Networking Academy ofrece muchos cursos para que pueda continuar su educación en ciberseguridad. Lo invitamos a inscribirse en el curso siguiente, Cybersecurity Essentials, para seguir adquiriendo una base de conocimientos sólidos en ciberseguridad. Visite Cisco Networking Academy y consulte la lista de [cursos](#) que se encuentran disponibles. Además, también puede tener acceso a [recursos profesionales](#) disponibles en Cisco Networking Academy.

Solo por diversión, haga clic [aquí](#) para leer una novela gráfica de un superhéroe de la ciberseguridad.

Actividad: Identificar el color del sombrero			
Características de un hacker	Sombrero blanco	Sombrero gris	Sombrero negro
Después de hackear las computadoras de ATM en forma remota con una PC portátil, trabajó con los fabricantes de ATM para resolver las vulnerabilidades de seguridad encontradas.		✓	
Desde mi PC portátil, transferí \$10 millones a mi cuenta bancaria con los números de cuenta y PIN de la víctima después de ver las grabaciones de las víctimas que ingresaban los números.			✓
Mi trabajo es identificar las debilidades en el sistema informático de mi empresa.	✓		
Utilicé el malware para comprometer varios sistemas corporativos para robar la información de tarjetas de crédito y vendí esa información al mejor postor.			✓
Durante mi investigación de ataques a la seguridad, encontré una vulnerabilidad en la seguridad en una red corporativa a la que puedo acceder.	✓		
Estoy trabajando con empresas de tecnología para resolver un defecto con DNS.	✓		