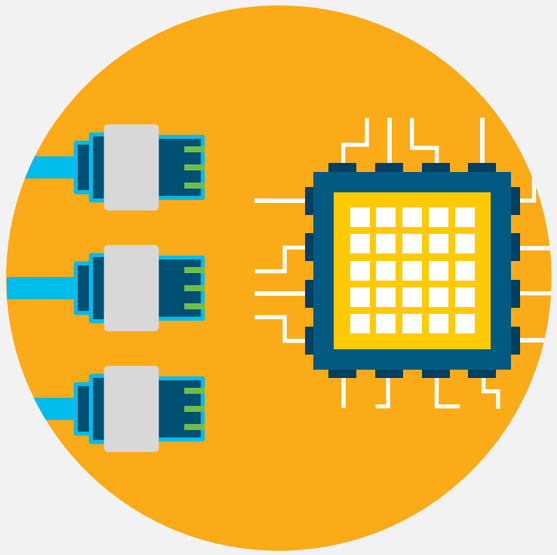
Ciberseguridad

También conocida como seguridad informática, es el conjunto de políticas, procesos y herramientas de *hardware* y *software*, que se encargan de proteger la privacidad, la disponibilidad y la integridad de la información y los sistemas en una red.

A continuación, presentamos un resumen de los principales conceptos asociados a la seguridad que se manejan en la industria de TI.

Antes



Hace más de dos décadas, cuando se empezó a hablar de seguridad informática, ésta se enfocaba en la protección del sistema operativo de los equipos de cómputo, para evitar que su rendimiento se viera afectado por algún virus que lograra entrar a la red. Adicionalmente el perfil de los atacantes y de los ataques, era mucho más simple.

Ahora

En la actualidad, los ataques son mucho más sofisticados y los atacantes, también conocidos como *hackers*, están aprovechando las brechas de seguridad ocasionadas por tendencias como el *IoT* y las soluciones en la nube. Las empresas necesitan soluciones integrales que permitan prevenir los ataques, bloquearlos cuando ocurren y remediar los daños en el menor tiempo posible.

Amenazas Cibernéticas

Son estrategias digitales que usan los criminales cibernéticos para entrar en su red. Así pueden secuestrarla o acceder a información confidencial para obtener beneficios económicos que podrían traerle consecuencias graves a su organización. Conozca algunas de las amenazas más frecuentes.

Malware

Es un *software* malicioso que tiene como objetivo infiltrarse o dañar un sistema de información sin el consentimiento de su propietario. Existen diferentes tipos de *malware* como los troyanos, los *worms*, los *bots*, el *spyware*, el *ransomware*, entre otros.

Ransomware

El *ransomware* es un *malware* que restringe el acceso a determinada información o a ciertas funciones del sistema infectado y pide un rescate a cambio de quitar esa restricción. Es muy similar a un secuestro digital. *Wannacry* es uno de los ejemplos más conocidos de los últimos años.

Malvertising

Es el uso de publicidad en línea para propagar *malware*. Por lo general, implica inyectar anuncios maliciosos en sitios *web* legítimos, que motivan la descarga y en consecuencia provocan la difusión del *malware* a través de su red.

Phishing

También conocido como suplantación de identidad, es una estafa electrónica donde el criminal cibernético intenta adquirir información confidencial de forma fraudulenta. Es muy usado para robar contraseñas y números de tarjetas de crédito, entre otros datos sensibles.

Soluciones de Seguridad

Son herramientas de *hardware* y *software* que le permiten prevenir, bloquear y remediar las amenazas cibernéticas y proteger su activo más valioso que es la información.

A continuación, conozca algunas de las soluciones que usted debería considerar.

Firewall

Es un sistema diseñado para bloquear el acceso no autorizado hacia o desde una red privada. Protege su red de los ataques desde internet, revisando todo lo que entra y sale.

Antivirus

Los antivirus son programas cuyo objetivo es detectar o eliminar virus informáticos. Éstos han ido evolucionando y actualmente son capaces de bloquear el virus, desinfectar archivos y prevenir una infección de los mismos. Pueden reconocer varios tipos de *malware* como *spyware*, gusanos y troyanos.

IPS

Es unn sistema de prevención de intrusos. Controla el acceso a una red informática para proteger los sistemas de ataques y abusos. El *IPS* no sólo bloquea la actividad maliciosa, también es capaz de rastrear los archivos sospechosos y el *malware* para evitar su dispersión.

DLP

Es un sistema de prevención de pérdida de datos. Está diseñado para detectar y prevenir la fuga de datos a través del monitoreo, la detección y el bloqueo de información sensible o confidencial mientras está en uso, en movimiento y en reposo.

Email Security

El correo electrónico sigue siendo la herramienta de comunicación más utilizada y es a su vez un medio a través del cual los *hackers* pueden propagar *software* malicioso con bastante facilidad, engañando a los destinatarios con tácticas de ingeniería social. Una aplicación de seguridad de correo electrónico bloquea los ataques entrantes y controla los mensajes de salida para evitar que se pierdan datos confidenciales.

Web Security

Las soluciones de seguridad *web* controlan la navegación de su personal, bloquean las amenazas basadas en la *web* y niegan el acceso a sitios maliciosos. Además, protegen su arquitectura local o en la nube.

Conozca las soluciones de seguridad de Cisco

Visite nuestro sitio

Únase a la conversación

Oficinas Centrales en América:
Cisco Systems, Inc.
San José, CA

Oficinas Centrales en Asia Pacífico:
Cisco Systems
Pte. Ltd. Singapur

Oficinas Centrales en Europa:
Cisco Systems
International BV Amsterdam Holanda

Argentina: 0800 555 3456 · **Bolivia:** 800 10 0682 · **Chile:** 1230 020 5546 · **Colombia:** 1 800 518 1068 · **Costa Rica:** 0800 011 1137
República Dominicana: 866 777 6252 · **El Salvador:** 800 6600
Guatemala: 1 800 288 0131 · **México:** 001 888 443 2447 · **Perú:** 0800 53967 · **Venezuela:** 0800 102 9109