**¿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.

La ciberseguridad es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. Y pues también se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

Sabiendo este concepto podemos andentrarnos un poco mas en el tema y hablar de los atacantes y como estos se dividen segun sus actividades.

Antes que nada, debemos saber que son los atacantes, estos se definen como 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. Algunos tipos de ciberatacantes son conocidos como:

* **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.
  + 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 accion coincide con su agenda.
* **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.

**Datos que pueden ser comprometidos**

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**: Este contiene información sensitiva sobre los pacientes, la cual puede ser usada clonar identidades.
* **Historial educativo**: 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, todo es.
* **Historial financiero y de empleo** este puede incluir información sobre sus ingresos y gastos. El historial de impuestos puede 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.

**Los 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.

**Recomendaciones para proteger sus dispositivos**

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.
* **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.

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.

# 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.

# 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.

¿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.

# 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 descifraran. 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.

# 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.

**Vulnerabilidades de hardware**

Las vulnerabilidades de hardware se presentan a menudo mediante defectos de diseño del hardware.

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 del software

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 validada:** 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.

# ¿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.

# 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.

# 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.

**Actualidad**

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.

**Conclusiones**

Hoy en día la ciberseguridad es cada vez un tema de mayor importancia en la tecnología, para las grandes, medianas, y pequeñas empresas, también para los usuarios que la consumimos. Basicamente sin ciberseguridad no deberia funcionar ninguna empresa ya que con el minimo error la información de la empresa y sus clientes estará comprometida. En fin la seguridad informática busca mitigar lo mayor posible el riesgo de un ataque, ya que ningun sistema es 100% seguro; porque asi como los sistemas de seguridad perimetral avanzan y mejoran, tambien lo hacen las tecnicas y formas de relizar un ataque informático.