CIBERSEGURIDAD

¿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.

DATOS PERSONALES

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.

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.

Está prohibido el uso de redes sociales en el trabajo.

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.

DATOS EN LA ORGANIZACIÓN

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.

GUIA PARA LA SEGURIDAD INFORMATICA EN UNA ORGANIZACIÓN **(revisar si es necesario colocar)**

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

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.

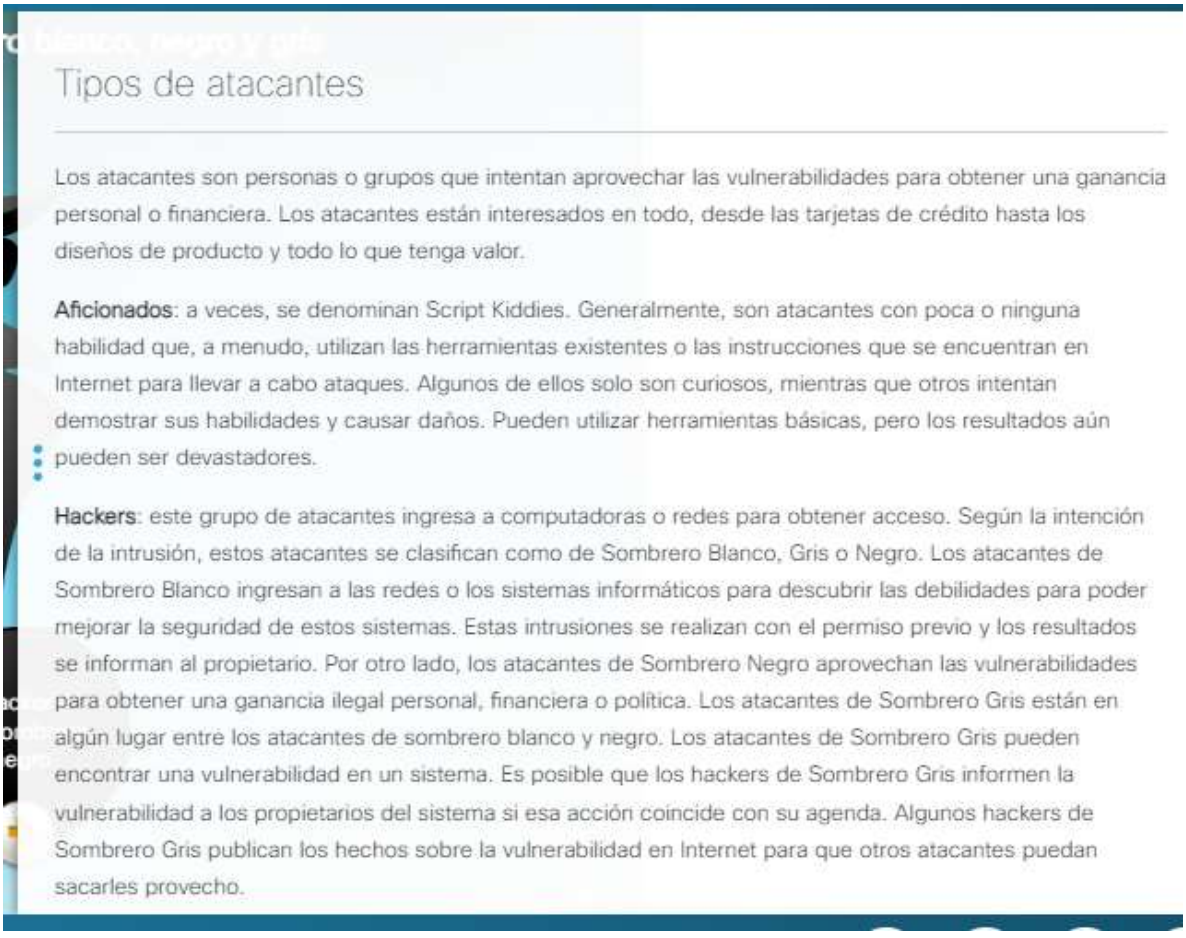
Integridad

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.

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.

ATACANTES DE LA CIBERSEGURIDAD



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

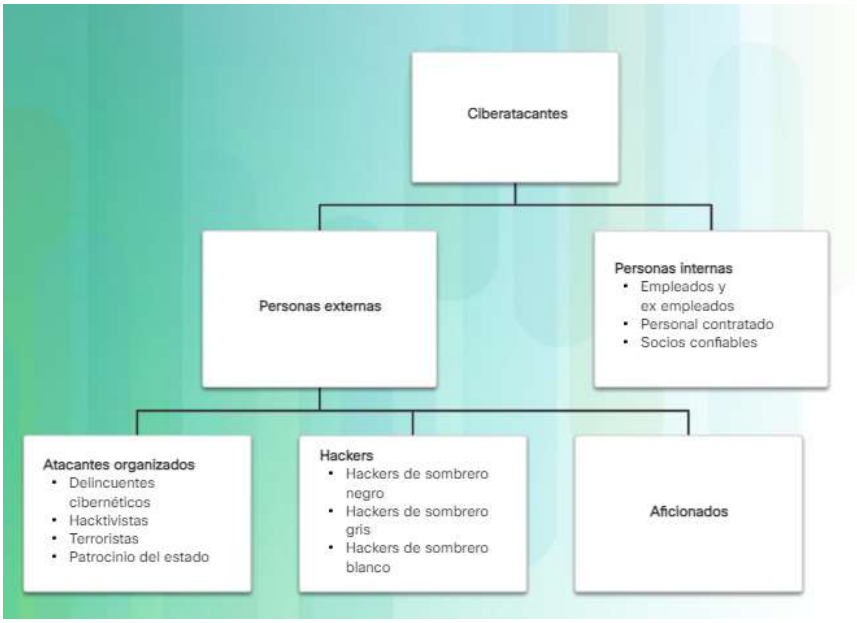
Los ataques pueden originarse dentro de una organización o fuera de ella, como se muestra en la figura. Un usuario interno, como un empleado o un partner contratado, puede de manera accidental o intencional:

- 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.



ANALISIS DE UN CIBERATAQUE

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.

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.

TIPOS DE MALWARE Y SINTOMAS

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.

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.

METODOS DE INFILTRACIÓN

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:

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.

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:

DENEGACIÓN DE SERVICIO

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.

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.

PROTEJA SUS DISPOSITIVOS Y RED

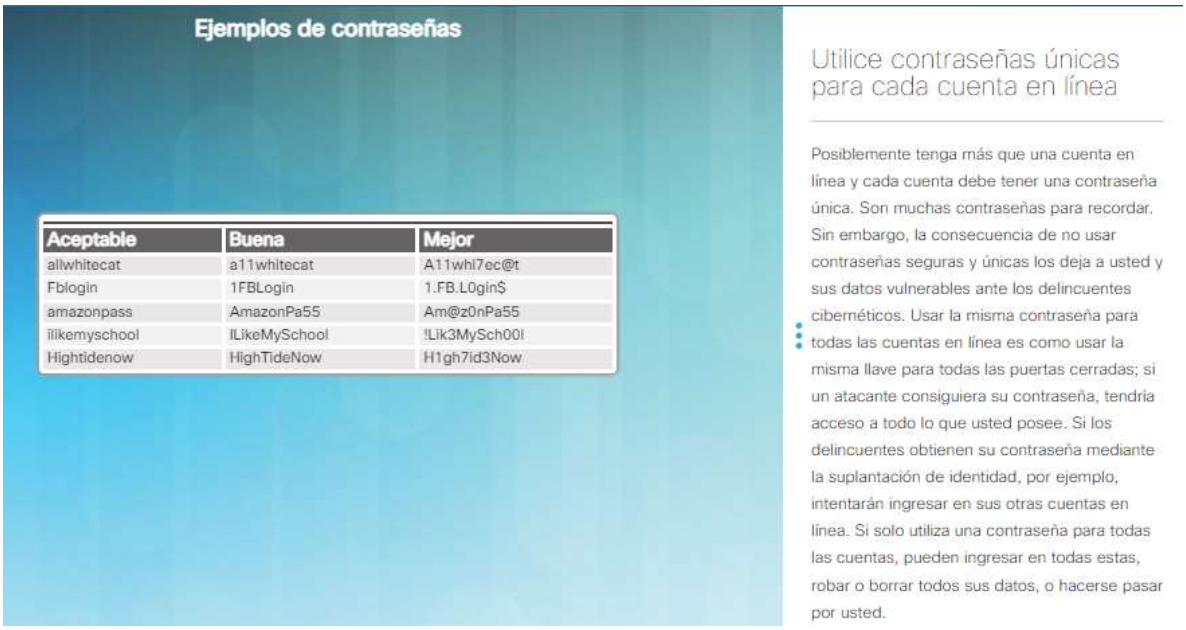
Proteja sus dispositivos informáticos

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.

CONTRASEÑAS SEGURAS



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.

CONTRASEÑAS (FRASES)

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:

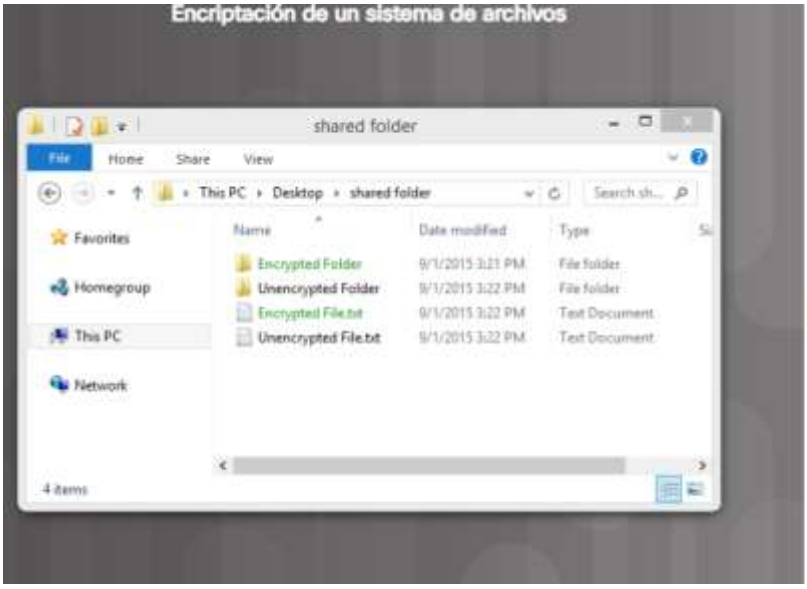
NOTA: CAMBIAR A POLITICA LOCAL

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.

3.1.2. MANTENIMIENTO DE LOS DATOS



¿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,

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.

NOTA: Complementar con; cómo se respalda en Woco .

3.2.1 AUTENTICACIÓN SOLIDA

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.

4.1 FIREWALLS

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).

CUESTIONES LEGALES Y ETICAS EN LA CIBERSEGURIDAD

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.

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.