Universidad Autónoma De Chiapas

Análisis de Vulnerabilidades

- **Alumno:** Tomás Álvarez Gómez
- **Actividad:** 1.3
- **Tarea:** Investigación de conceptos
- **Maestro:** Luis Gutiérrez Alfaro
- **Grupo:** 7 M
- **Fecha:** Tuxtla Gutiérrez a 28/08/23
- **Matricula:** A200369

CONTENIDO

¿Qué es vulnerabilidad?

una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas y pueden ser explotadas o utilizadas por intrusos o atacantes (Santander).

Para entenderlo mejor, una vulnerabilidad puede ser, por ejemplo:

- Un servicio de un sistema de computación corriendo en un determinado puerto lógico.
- Sistemas y aplicaciones no actualizados o parcheados que presentan múltiples vulnerabilidades.
- Una red Wifi abierta.
- Un puerto abierto en un firewall.
- Un insuficiente o inexistente control de acceso físico a las instalaciones.
- La no aplicación de una política de gestión de contraseñas.

Tipos de vulnerabilidad informática

Algunos tipos de vulnerabilidades típicas de sistemas y aplicaciones son:

- **Buffer overflow o desbordamiento de buffer**: se da cuando las aplicaciones no controlan la cantidad de datos que copian en el buffer y que al sobrepasar el tamaño de este pueden modificar zonas de memoria contiguas afectando a los datos que albergan.
- **Condición de carrera:** las aplicaciones o sistemas no implementan exclusiones mutuas en el acceso a recursos compartidos, como por ejemplo una variable, y varios procesos acceden a ella al mismo tiempo obteniendo valores no esperados.
- **Error de formato en cadenas:** cuando las aplicaciones no validan los datos de entrada que introduce el usuario a las mismas, pudiendo ejecutar por ejemplo comandos o instrucciones que pueden permitir al atacante obtener datos confidenciales o dañar el sistema.
- **Cross Site Scripting:** se basa en que los atacantes incrustan scripts en páginas web legítimas afectadas por esta vulnerabilidad y por las que navega el usuario. Este introduce datos como por ejemplo, su usuario y su contraseña, pero no en la web legítima si no en la del atacante, que roba así sus datos.
- **Inyección de SQL:** cuando no se validan los datos de entrada a formularios que se comunican con bases de datos se podría ejecutar código SQL malicioso que por ejemplo permitiera obtener datos confidenciales o corromper los datos de las tablas.

¿Qué es seguridad?

La seguridad informática —también llamada ciberseguridad— se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros.

Es por esto que esta disciplina del área de la informática encargada de la protección de la privacidad de datos dentro de los sistemas informáticos se ha convertido en una parte indispensable para los negocios y la operación de las empresas. © UNIR - Universidad Internacional de La Rioja (2023)

Pilares de la seguridad

1. Integridad

El pilar de Integridad se encarga de mantener las características originales de los datos, tal y como se configuraron en su creación. Por tanto, la información no se puede modificar sin autorización.

Si existe una alteración indebida en los datos, significa que ha habido una pérdida de integridad, y es necesario implementar mecanismos de control para evitar la alteración no autorizada de la información.

2. Confidencialidad

Este pilar protege la información del acceso no autorizado, estableciendo privacidad para los datos de su empresa, previniendo ciberataques o situaciones de espionaje.

La base de este pilar es el control de acceso mediante autenticación de contraseña, que también puede ocurrir mediante escaneo biométrico y cifrado, lo que ha generado resultados favorables en este sentido.

3. Disponibilidad

Lo ideal en un sistema de información es que los datos estén disponibles para lo que sea necesario, asegurando el acceso de los usuarios a tiempo completo. Esto requiere estabilidad y acceso permanente a los datos del sistema mediante un mantenimiento rápido, actualizaciones constantes y depuración.

Es importante recordar la vulnerabilidad de los sistemas que son susceptibles a apagones, incendios, ataques de negación y muchas otras posibles amenazas que existen en este contexto.

4. Autenticidad

Confirmación de que los datos tienen legitimidad, es decir, no existe manipulación o intervenciones externas por parte de terceros que se hacen pasar por colaboradores. Para ello, es necesario documentar las acciones realizadas por los usuarios en la red y los sistemas.

Los datos corporativos deben tener procesos para identificar su autenticidad y esta es una de las tareas del equipo de Seguridad de la Información. La configuración de un registro de acceso ayuda a confirmar la veracidad de un registro en particular.

5. Legalidad

Finalmente, es necesario contar con una Política de Seguridad que asegure que todos los trámites relacionados con la información dentro de la empresa se realicen de conformidad con la ley. Esto evita la aparición de impedimentos operativos, investigaciones y auditorías por parte de los organismos de inspección.

La adecuación de los contenidos protegidos a la legislación es fundamental, principalmente porque en agosto de 2020 entra en vigor la nueva Ley General de Protección de Datos de Carácter Personal, que requerirá un mayor rigor por parte de todas las empresas.

Algunos ataques sobre los datos

1.Phishing

El término phishing viene de fish, que significa ‘pesca’ en inglés. Es uno de los tipos de ataques informáticos más frecuentes. Probablemente hasta lo hayas sufrido. El phishing es un tipo de ataque malicioso que consiste en recibir correos electrónicos que parecen provenir de fuentes fiables pero que, en realidad, contienen un enlace que pone en riesgo información y otros datos personales o empresariales.

2. Spear Phishing

El spear phishing es una variante del anterior. Significa ‘pesca con arpón’. En lugar de un solo correo electrónico, este tipo de phishing trata de ganarse la confianza del destinatario a base de correos electrónicos. En el spear phishing los correos suelen estar personalizados y tienen principalmente un objetivo.

3. Whaling

El whaling es otra variante del phishing. Sin embargo, este tipo de ataque informático está específicamente dirigido a CEOs y CFOs de empresas, además de hacia otros altos cargos en general dentro de una empresa. El whaling puede ser muy persuasivo: el robo de datos se hace de forma en que parezca que las comunicaciones fraudulentas provienen de una persona importante o que tiene un cargo de nivel superior dentro de la organización.

Por ejemplo, el atacante puede hacerse pasar por uno de los directivos o consejeros de la empresa y solicitarle al CEO información confidencial a través del correo electrónico. Si es inteligente…no picará el anzuelo.

º4. Malware

El malware es lo que suele ir acompañando a los correos electrónicos de phishing que roban la información. Es decir, es el programa informático que perjudica y deshabilita un ordenador o un sistema informático. Lo hace de manera maliciosa y, por supuesto, silenciosa.

Dentro de la categoría de malware podemos encontrar múltiples ejemplos de estos softwares maliciosos. Seguro que alguno te suena:

- Ransomware
- Adware
- Spyware
- Criptomalware
- Troyanos
- Gusanos
- Virus
- Keylogger
- Bots
- Bombas lógicas

Como hemos visto con otros tipos de fraude, las formas más comunes de propagación de un malware son los correos electrónicos, las alertas emergentes o las descargas ocultas.

¿De qué nos protegemos?

Proteger el uso no autorizado de un sistema informático.

Prevenir el robo de información importante como números de cuentas bancarias o contraseñas es imprescindible hoy en día. Los datos que se dan en las comunicaciones informáticas hoy en día pueden ser mal utilizados por intrusos no autorizados.

En la actualidad existen ciberdelincuentes que intentan acceder a los ordenadores de otras personas con intenciones maliciosas para conseguir sus propios intereses.

Amenazas que se concrete por medio de una vulnerabilidad

Amenazas de Malware

Los programas maliciosos son una de las mayores ciber amenazas a la que se exponen las empresas. Dentro del malware existen distintos tipos de amenazas, siendo las principales.

Virus. Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento.

Gusanos. Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello.

Troyanos. Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.

Ransomware. El ransomware se ha convertido en el malware más temido en la actualidad por las empresas. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins).

Keyloggers. Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares.

Tipos de vulnerabilidades

Vulnerabilidades del sistema

Los sistemas y aplicaciones informáticos siempre tienen algún error en su diseño, estructura o código que genera alguna vulnerabilidad. Por muy pequeño que sea ese error, siempre podrá generar una amenaza sobre los sistemas y la información, siendo la puerta de entrada para recibir ataques externos o internos. Las principales vulnerabilidades suelen producirse en:

- Errores de configuración.
- Errores en la gestión de recursos.
- Errores en los sistemas de validación.

- Errores que permiten el acceso a directorios.

Errores en la gestión y asignación de permisos.

Vulnerabilidades producidas por contraseñas

Con el teletrabajo y el cloud computing la gestión de contraseñas se ha convertido en uno de los puntos más importantes en ciberseguridad. Para acceder a las plataformas de trabajo de las empresas es necesario utilizar un usuario y contraseña. Utilizar contraseñas poco seguras genera vulnerabilidades en los sistemas, pues si son fácilmente descifrables pueden generar incursiones de terceros no autorizados que pueden robar, modificar o eliminar información, cambiar configuraciones si disponen de los privilegios apropiados, o incluso apagar equipos.

La generación de contraseñas seguras es una de las claves para incrementar el nivel de ciberseguridad de las empresas.

Vulnerabilidades producidas por usuarios

Una de las principales causas de los ataques informáticos está relacionada con un uso incorrecto o negligente por parte de un usuario. Una mala asignación de privilegios o permisos puede hacer que un usuario tenga acceso a opciones de administración o configuración para las que no está preparado, cometiendo errores que suponen una amenaza para la empresa.

El error humano es otra causa de riesgos en ciberseguridad. El usuario siempre tiene el riesgo de cometer un error que pueda generar una vulnerabilidad que suponga una amenaza informática. Por eso en ciberseguridad se tiende a automatizar procesos críticos para minimizar o eliminar el factor de riesgo del error humano.

Las malas prácticas o la falta de formación en ciberseguridad también generan vulnerabilidades, como la apertura de ficheros de dudosa procedencia, engaños por publicidad falsa, apertura de correos fraudulentos y similares. Estas acciones son una amenaza a sufrir ataques como el phishing (suplantación de identidad) o similares.

¿Por qué aumentan las amenazas?

1- Uso masivo de tecnología

El primer factor que se considera para el desarrollo de una amenaza informática es, sin duda, el número de usuarios de una tecnología: a mayor cantidad de usuarios, la probabilidad de éxito de un ataque se incrementa.

Con más usuarios aumenta la probabilidad de éxito de un ataque

2- Vulnerabilidades en el software

Las vulnerabilidades pueden estar asociadas a la tecnología y con mayor frecuencia se pueden identificar en el software, es decir, fallas o errores en su programación.

Nada es infalible y en el software esta premisa se cumple, por lo que cualquier herramienta es susceptible de contener fallas, casi de manera inherente

3- Conectividad a Internet

El aumento de la conectividad de los dispositivos a Internet también juega un papel relevante para que se desarrollen amenazas. Las conexiones, con todos los beneficios que contraen, también han significado que los atacantes distribuyan de forma masiva sus amenazas informáticas, al tiempo que pueden afectar sistemas que se encuentran en distintas ubicaciones geográficas.

4- Ganancias económicas para atacantes

Otro factor que determina el desarrollo de nuevas amenazas y ataques está asociado a los réditos económicos que generan para sus creadores. En la actualidad, códigos maliciosos como el ransomware buscan generar ganancias en el menor tiempo posible, sobre todo si se compara con campañas masivas de malware que roban información y posteriormente buscan monetizarla.

5- Usuarios poco conscientes de los riesgos

Las amenazas de la actualidad utilizan técnicas de Ingeniería Social que pretenden engañar y persuadir a los usuarios para que realicen actividades que no tenían previstas hacer, y que los ponen en riesgo. Sumando esto a las condiciones anteriores, la probabilidad de que los usuarios resulten afectados por distintas amenazas informáticas se incrementa.

Protecciones más usadas:

1. Controles de acceso a los datos más estrictos

Una de las principales medidas de seguridad es limitar el acceso a la información. Cuantas menos personas accedan a una información, menor será el riesgo de comprometerla

2. Realizar copias de seguridad

Poseer un sistema de copias de seguridad periódico permite que la empresa garantice que puede recuperar los datos ante una incidencia de carácter catastrófico, impidiendo la pérdida de los mismos y permitiendo la recuperación de la normalidad en el trabajo en apenas unos minutos.

3. Utilizar contraseñas seguras

El acceso a las distintas plataformas que utiliza la empresa (correo electrónico, servidor de copias de seguridad NAS, etc.) debe realizarse utilizando claves de seguridad (contraseñas) seguras, que impidan que puedan ser fácilmente descubiertas por piratas informáticos.

4. Proteger el correo electrónico

Hoy en día, la mayoría de comunicaciones de nuestra empresa la realizamos utilizando el correo electrónico. Por lo tanto, otra medida de seguridad es utilizar filtros antispam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de toda esa información.

5. Trabajar en la nube

Trabajar en la nube permite, entre otras ventajas, contar con los sistemas de seguridad de la información que posee el proveedor de servicios. Además, este proveedor será responsable de esa seguridad.

6. Involucrar a toda la empresa en la seguridad

Debemos involucrar en su participación a todos los estamentos que participan en la misma, incluyendo a los agentes externos como puedan ser clientes, proveedores, etc.

7. Monitorización continua y respuesta inmediata

Debemos implantar en nuestra empresa un sistema que permita monitorizar la gestión de los datos y detectar aquellos posibles fallos o actuaciones incorrectas. Este sistema de control permitirá actuar rápidamente para solventar cualquier incidencia y minimizar su repercusión.

¿Qué es amenaza?

Cuando hablamos de amenazas a la seguridad nos referimos a la explotación de una vulnerabilidades o fallos que se utilizan para afectar la operatividad de un sistema, con la intención de sacar algún provecho.

¿Qué es la ingeniera social?

Se llama ingeniería social a las diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios.

Los ciberdelincuentes engañan a sus víctimas haciéndose pasar por otra persona. Por ejemplo, se hacen pasar por familiares, personas de soporte técnico, compañeros de trabajo o personas de confianza. El objetivo de este engaño es apropiarse de datos personales, contraseñas o suplantar la identidad de la persona engañada.

¿Qué es un virus informático?

Un virus informático, como un virus de gripe, está diseñado para propagarse de un host a otro y tiene la habilidad de replicarse. De forma similar, al igual que los virus no pueden reproducirse sin una célula que los albergue, los virus informáticos no pueden reproducirse ni propagarse sin programar, por ejemplo, un archivo o un documento.

En términos más técnicos, un virus informático es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro. Los virus se insertan o se adjuntan a un programa o documento legítimo que admite macros a fin de ejecutar su código. En el proceso, un virus tiene el potencial para provocar efectos inesperados o dañinos, como perjudicar el software del sistema, ya sea dañando o destruyendo datos.

Define el concepto de autenticación:

En ciberseguridad, la autentificación es el proceso de verificar la identidad de alguien o algo. La autentificación suele tener lugar mediante la comprobación de una contraseña, un token de hardware o algún otro dato que demuestre la identidad. Como cuando un trabajador de una aerolínea comprueba un pasaporte o una tarjeta de identificación para verificar la identidad de una persona cuando sube a un avión, los sistemas informáticos tienen que estar seguros de que una persona es realmente quién dice ser.

Métodos de seguridad informática

Los ataques informáticos son un gran problema para las empresas, ya que ponen en riesgo su información confidencial y las obligan a gastar millones de dólares para recuperar el control de sus sistemas y datos.

Para que puedas prevenirlos, te recomendamos tomar estas 7 medidas de seguridad para reducir el riesgo de ataque al mínimo.

Mecanismos preventivos de la seguridad informática:

1. Inteligencia artificial

Sin embargo, la implementación de la inteligencia artificial como método de seguridad ha disminuido los ataques de manera significativa.

La inteligencia artificial tiene la cualidad de adelantarse y predecir futuros ataques en los sistemas más vulnerables

2. Software antivirus

Este es uno de los métodos más antiguos de protección contra amenazas cibernéticas, pero no el menos importante. Un software antivirus es un recurso imprescindible en cualquier equipo informático, ya sea personal o corporativo.

3. Firewall o cortafuegos

El firewall es el encargado de inspeccionar la intranet para identificar el tráfico de internet, reconocer a los usuarios y restringir el acceso a aquellos no autorizados.

4. Plan de seguridad informática

Generar un plan de seguridad informática es imprescindible para cualquier organización, ya que le permitirá a las empresas detectar vulnerabilidades en sus sistemas y establecer medidas para prevenir ataques.

5. Infraestructura de clave pública o PKI

La PKI, o infraestructura de clave pública, es la herramienta que permite el intercambio de información entre usuarios de una manera segura. Gracias a esta tecnología, se pueden distribuir e identificar las claves de cifrado público.

6. Pentesting

El pentesting, o testeo de penetración, consiste en realizar ataques a los sistemas de defensa que posees. Este método es una de las formas de verificación de eficiencia más utilizadas actualmente.

El proceso consiste en formar dos grupos y probar las defensas de la empresa en cada uno. Básicamente, es una auditoría de seguridad informática que pone a prueba tu protección.

Mecanismos correctivos de la seguridad informática

Parches y Actualizaciones: Mantener el software y los sistemas actualizados con las últimas versiones y parches de seguridad es esencial para corregir las vulnerabilidades conocidas.

Respuesta a Incidentes: Tener un plan de respuesta a incidentes en su lugar permite a las organizaciones reaccionar rápidamente ante incidentes de seguridad.

Escaneo y Evaluación de Vulnerabilidades: Utilizar herramientas de escaneo y evaluación de vulnerabilidades para identificar debilidades en sistemas y redes.

Monitorización Continua: Implementar sistemas de monitorización de seguridad en tiempo real para detectar actividades sospechosas o no autorizadas

Aislamiento y Segmentación de Redes: Segmentar las redes en subredes aisladas puede ayudar a contener un ataque y evitar que se propague a través de toda la infraestructura.

Restauración de Copias de Seguridad: Mantener copias de seguridad regulares y probadas es crucial.

Análisis de Malware y Forense: Realizar análisis forenses y de malware después de un incidente ayuda a entender cómo ocurrió y qué datos se vieron comprometidos.

Auditorías de Seguridad: Realizar auditorías de seguridad de manera regular para identificar posibles debilidades en la infraestructura y en las prácticas de seguridad implementadas.

Entrenamiento y Concienciación: Educar a los empleados y usuarios sobre las mejores prácticas de seguridad informática puede reducir la probabilidad de ataques exitosos debido a errores humanos.

Bloqueo y Suspensión de Cuentas: En caso de actividad maliciosa o compromiso de cuentas, bloquear o suspender esas cuentas puede prevenir daños adicionales.

¿Qué es el aumento de privilegios?

El "aumento de privilegios" en seguridad informática se refiere a una técnica utilizada por atacantes para elevar el nivel de acceso o permisos que tienen en un sistema o red. En términos simples, significa que un atacante intenta obtener más control y acceso a recursos que normalmente no le estarían permitidos.

Técnicas de aumento de privilegios en Windows

Explotación de Vulnerabilidades de Día Cero: Si un atacante descubre una vulnerabilidad no parcheada en el sistema operativo o en una aplicación, podría usarla para ejecutar código malicioso con privilegios elevados.

Explotación de Servicios y Aplicaciones: Algunos servicios o aplicaciones de Windows pueden ejecutarse con privilegios elevados por defecto. Si un atacante encuentra una vulnerabilidad en uno de estos servicios, puede utilizarla para obtener acceso con privilegios más altos.

Explotación de Configuraciones Incorrectas: Las configuraciones incorrectas en servicios, permisos de archivos y configuraciones de seguridad pueden ser aprovechadas por atacantes para ganar acceso elevado.

Uso de Exploits y Herramientas: Los atacantes pueden usar exploits y herramientas de aumento de privilegios específicas que aprovechan vulnerabilidades conocidas en el sistema.

Ataques de Diccionario y Fuerza Bruta: Si un atacante puede obtener acceso a una cuenta con privilegios bajos, puede intentar adivinar contraseñas o realizar ataques de fuerza bruta para obtener acceso a cuentas con mayores privilegios.

Ataques a Cuentas de Servicio: Las cuentas de servicio a menudo tienen privilegios elevados y pueden ser atacadas si sus credenciales son débiles o si sus configuraciones no son seguras.

Uso de Malware y Troyanos: Los troyanos y el malware pueden ser utilizados para instalar puertas traseras en sistemas y, así, permitir a los atacantes obtener acceso a niveles más altos de privilegios.

Manipulación de Tokens: Los tokens de seguridad son utilizados para verificar la identidad y los privilegios de un usuario. Los atacantes pueden intentar manipular estos tokens para elevar sus propios privilegios.

Elevación de Privilegios Lateral: Una vez que un atacante tiene acceso a un sistema, puede intentar moverse lateralmente a otros sistemas y usar técnicas similares para aumentar sus privilegios en esos sistemas.

CONCLUSION

Después de leer detenidamente estos conceptos referentes la seguridad informática tenemos un amplio conocimiento acerca de los riesgos que corren nuestros sistemas o dispositivos al menos de manera teórica.

Es por eso que es importante que nos actualicemos, que conozcamos las diferentes vulnerabilidades que se pueden presentar en los sistemas, ya que en alguno momento nos tocara lidiar con un sistema y sus vulnerabilidades. Es necesario tomar conciencia que al utilizar dispositivos electrónicos estamos propensos a ser atacados y ser víctimas de los delincuentes cibernéticos, es por eso que debemos utilizar con cuidado nuestros dispositivos ya que son los que tienen nuestra información personal que también puede ser explotada para uso delincuente.

Pero para protegernos debemos saber valga la redundancia de qué nos protegemos exactamente, es decir saber la naturaleza de las amenazas conocerlas bien para así poder darle seguridad a un sistema o cuidar nuestros dispositivos, bien sabemos que son múltiples las amenazas que existen hoy en día en los sistemas informáticos, pero basta con que tengamos cierto contacto con las mismas amenazas para entender como operan.

Los conceptos antes presentados son conceptos que tendremos que manejar muy bien si deseamos ser en algún momento administradores de sistemas informáticos, es muy necesario conocer bien las amenazas actuales y saber utilizar los mecanismos preventivos de seguridad.

BIBLIOGRAFÍA

Unir, V. (2022, 13 octubre). ¿Qué es la seguridad informática y cuáles son sus tipos? *Universidad Virtual. | UNIR Ecuador - Maestrías y Grados virtuales*. https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/

Blog, F. L. (2021). 5 pilares de la ciberseguridad. *Blog Fast Lane LATAM*. https://www.flane.com.pa/blog/5-pilares-de-la-seguridad-en-la-informacion/#:~:text=Hay%205%20pilares%20de%20la,%2C%20disponibilidad%2C%20autenticidad%20y%20legalidad.

Ciberseguridad: 4 tipos de ataques informáticos. (s. f.). Fundación Telefónica España. https://www.fundaciontelefonica.com/noticias/ciberseguridad-4-tipos-de-ataques-informaticos/

Team, A. (s. f.). *Tipos de vulnerabilidades y amenazas informáticas*. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Technologies, G. (2021, 24 junio). Vulnerabilidades informáticas: qué son y tipos | Ginzo Technologies. *GINZO TECHNOLOGIES SL*. https://ginzo.tech/vulnerabilidades-informaticas-que-son-tipos/

¿Qué es la ingeniería social Y cómo me protejo? (2023, 6 junio). Argentina.gob.ar. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte

What is a computer virus? (s. f.). https://mx.norton.com/blog/malware/what-is-a-computer-virus

De DocuSign, C. (2022, 28 diciembre). Conoce los 7 mejores métodos de seguridad informática para tu empresa. *DocuSign*. https://www.docusign.mx/blog/seguridad-informatica