PRINCIPIOS DE SEGURIDAD Y ALTA DISPONIBILIDAD

TEMA 1

Profesor: Israel Caldito

Curso: 2022-2023

Fuente: María Botón

ÍNDICE

- Introducción a la seguridad informática
- Fiabilidad. Confidencialidad. Integridad. Disponibilidad
- Elementos vulnerables
- Amenazas. Tipos
- Medidas de seguridad
- Análisis forense en sistemas informáticos

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

¿ POR QUÉ PROTEGER?

"El único sistema seguro es aquel que está apagado en el interior de un bloque de hormigón, protegido en una habitación sellada rodeada por guardias armados"

Eugene H. Spafford

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

- La informática se utiliza en muchos ámbitos de la vida.
- El número de usuarios y profesionales de la informática ha crecido exponencialmente en los últimos años.
- Las necesidades de comunicación y comunicación de recursos en la red también ha aumentado.
- Surgen **dos grandes problemáticas**:
  - Asegurar los sistemas y la información que contienen.
  - Tener acceso a los servicios el mayor tiempo posible, sin interrupciones y con cierta calidad.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Por parte de los usuarios finales sigue existiendo, además, mucha desinformación en términos de seguridad.

EJEMPLO

- Un conocido nos trae su ordenador porque va lento. No cree que sea un virus porque le puso un antivirus.
- Le preguntamos por la contraseña de administrador y nos dice que no tiene ningún usuario así, solo el suyo. Además, su usuario no tiene contraseña.
- No tiene miedo de que nadie entre sin su permiso, porque solo lo usa él. Tampoco teme que nadie entre a través de Internet porque la wifi de casa tiene contraseña.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

EJEMPLO

- Analizamos su ordenador. Tiene el antivirus caducado.
- Quitamos el antivirus e instalamos otro actualizado. El antivirus encuentra un troyano en el ordenador.

Teniendo en cuenta el enunciado del ejemplo, determina los defectos de seguridad e indica cómo los resolverías.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

EJEMPLO

- Conclusión
  - **La protección** de los sistemas y redes de ordenadores **es crítica**.

- Actualmente las estrategias en materia de seguridad buscan adelantarse al atacante y utilizar **medidas preventivas**.
- Será fundamental asegurar la infraestructura, la información y las comunicaciones.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

DEFINICIÓN DE LA SEGURIDAD INFORMÁTICA

La seguridad informática consiste en **asegurar** que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el **acceso** a la información allí contenida, así como su modificación, solo sea posible a las **personas** que se encuentren **acreditadas** y, siempre, dentro de los límites de **autorización**.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Los **principales objetivos de la seguridad informática** son:

- Detectar los posibles problemas y amenazas a la seguridad, minimizando y gestionando los riesgos.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
- Limitar las perdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos a nivel organizativo.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

- La comunidad de usuarios y profesionales en materia de seguridad informática mantienen al día al resto de usuarios mediante noticias y post en blogs y webs especializadas.

- Como ejemplo podemos destacar el blog de seguridad informática del Instituto Nacional de Ciberseguridad:

  https://www.incibe.es/protege-tu-empresa/blog

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

- La clave de los ataques informáticos es **la motivación**, es decir, quién está interesado en nuestra información.
- Por lo general, son más atractivas las empresas que una persona particular para estas actividades delictivas. Por ello existen las **auditorías de seguridad**.
- Debemos tener en cuenta que los mecanismos de seguridad deben estar adaptados a cada caso particular.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Ejemplo real donde se mezcla lo personal y profesional:

- Una persona regala a su pareja un teléfono móvil de su empresa.
- La pareja no lo sabe, pero el dispositivo lleva preinstalado un troyano que registra las llamadas y mensajes que efectúa el teléfono.
- Con esa información el programa realiza un informe que cuelga en una web donde se accede con usuario y contraseña.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Ejemplo real donde se mezcla lo personal y profesional:

- De esta manera descubre que su pareja le engaña con un/a amigo/a común que trabaja en la empresa.
- Le regala otro móvil al amigo/a con el mismo troyano y así espiar a ambos.
- La empresa de telefonía que da servicio a la empresa tiene un equipo de vigilancia efectivo que detecta el tráfico extraño de informes. Notifica las actividades a la empresa
- El empleado es denunciado.

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

ACTIVIDAD 1. Aplicaciones espía e implicaciones legales.

- Realiza en Internet una búsqueda de apps y formas de espiar el móvil a otra persona mediante WhatsApp.
- Realiza una búsqueda de apps espía. Averigua qué son los programas stalkerware.
- Averigua qué dice la ley sobre espiar el móvil de otra persona.

ÍNDICE

- Introducción a la seguridad informática
- **Fiabilidad. Confidencialidad. Integridad. Disponibilidad**
- Elementos vulnerables
- Amenazas. Tipos
- Medidas de seguridad
- Análisis forense en sistemas informáticos

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

- Aunque la seguridad es un concepto que se asocia a la certeza o falta de riesgo, debemos aclarar que **la seguridad absoluta no existe**.

- La seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

- A grandes rasgos se entiende que mantener un sistema seguro consiste básicamente en garantizar tres aspectos:
  - Confidencialidad
  - Integridad
  - Disponibilidad
- Además, en los sistemas informáticos se habla de **fiabilidad**, probabilidad de que un sistema se comporte tal y como se espera de él.
- Se suele hablar de tener sistemas fiables en lugar de sistemas seguros.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

Confidencialidad

Capacidad de garantizar que la información almacenada en el sistema informático o transmitida por la red estará disponible únicamente para aquellas personas autorizadas a acceder a dicha información.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

Integridad

Capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. Es decir, cualidad de mensaje, comunicación o datos, que permite comprobar que no se ha producido manipulación alguna en el original, es decir, que no ha sido alterado.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

Disponibilidad

Capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.

Supone que la información pueda ser recuperada en el momento que se necesite, evitando su pérdida o bloqueo.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

- Dependiendo del entorno, en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad.
- Por ejemplo, en un **sistema militar** se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad.
- En cambio, en un **servidor de archivos en red**, se priorizará la disponibilidad frente a la confidencialidad.
- En un **entorno bancario**, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

ACTIVIDAD 2. Integridad en Windows y Linux.

- Averigua formas de comprobar la integridad de un sistema Windows y sus archivos.
- Averigua con qué comandos podemos comprobar la integridad de archivos en un sistema Linux.
- ¿Qué es el hashing? ¿Qué son los algoritmos de cifrado hash?

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

- Junto a estos tres conceptos fundamentales se suelen estudiar conjuntamente la **autenticación** y el **no repudio**.

NO REPUDIO

Garantizar la participación de las partes en una comunicación. Hay dos tipos de repudio:

- **En origen**: garantiza que quien envía el mensaje no puede negar que es el emisor. El receptor tendrá pruebas del envío.
- **En destino**: el receptor no puede negar que recibió el mensaje. El emisor tiene pruebas de la recepción del mismo.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

AUTENTICACIÓN

Verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice.

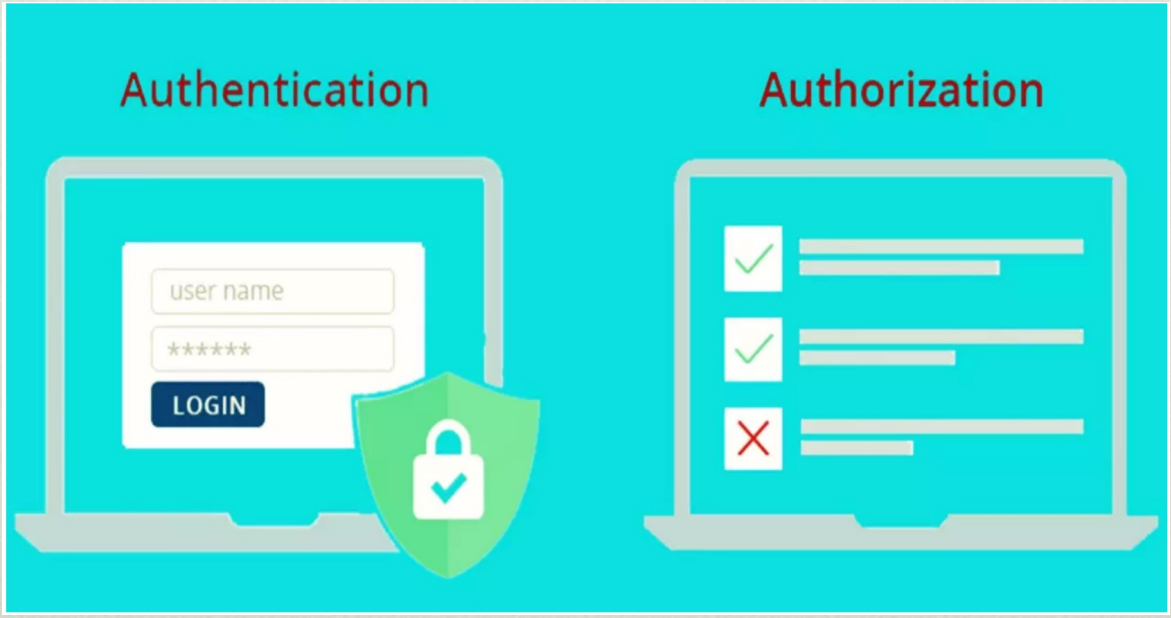
En informática se aplica a la verificación de la identidad de un usuario. Se suele realizar mediante un usuario o *login* y una contraseña o *password*. El usuario puede aportar algún modo que permite verificar que es quien dice ser.

Permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o servicio.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

AUTORIZACIÓN

Controla el acceso de los usuarios a zonas restringidas tras haber superado la autenticación.



FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

SABES-TIENES-ERES

- **La autenticación** es especialmente importante en el ámbito de la seguridad.
- Un esquema muy utilizado para analizar la autenticación es clasificar las medidas en base a los criterios **sabes-tienes-eres**.
- Hoy día muchos servicios en Internet han integrado este concepto para mejorar la seguridad de su producto/servicio.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

SABES-TIENES-ERES

- **Algo que sabes**: para acceder al sistema necesitas conocer alguna palabra secreta (una contraseña).
- **Algo que tienes**: aportar algún elemento material.
- **Algo que eres**: el sistema solicita reconocer alguna característica del individuo (biometría): huella, escáner de retina, reconocimiento de voz, etc.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

SABES-TIENES-ERES

EJEMPLOS

- Para entrar en casa nos solicitan en el portal un código y en la puerta una llave. **(código-llave-persona)**
- Para acceder a un ordenador necesitamos un usuario y una contraseña. **(contraseña-credenciales-persona)**
- Para sacar dinero del cajero necesitamos una tarjeta e introducir un Pin. **(pin-tarjeta-persona)**
- Para operar online en el banco necesitamos un usuario y un Pin. **(pin-credenciales-persona)**

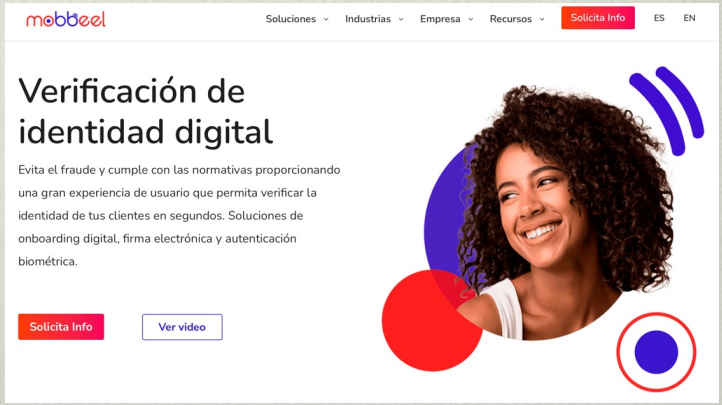
FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

SABES-TIENES-ERES

EJEMPLOS

En Extremadura también se trabaja en la seguridad biométrica como forma de verificación de identidad. La empresa **Mobbeel** ofrece soluciones que verifican la identidad del usuario de un teléfono móvil mediante la combinación de características únicas de las personas: iris, la voz o la firma manuscrita.

https://www.mobbeel.com



FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

SABES-TIENES-ERES

- La autenticación será más fiable cuantos más criterios distintos cumpla.
- Los sistemas biométricos no solo se utilizan en entornos de alta seguridad. Pueden aplicarse en el comedor de la empresa para distinguir entre empleados y personal externo para solicitar el menú.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

ACCOUNTING

- El Accounting se refiere a la información interna que los sistemas generan acerca de sí mismos, especialmente sobre el uso que se hace de sus servicios.
- Con esta información se pueden establecer limitaciones y penalizaciones.
- Con esta información también se puede verificar la eficacia de las medidas de autenticación y autorización.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

ACCOUNTING

- Tras un ataque, y mediante análisis forense, se puede seguir el rastro y localizar por dónde se accedió a los servicios.

- Es importante que el registro del accounting se haga en una máquina diferente para que el hacker no pueda borrar sus huellas.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

ACCOUNTING

EJEMPLO

- Supongamos que se han borrado ciertos archivos de un proyecto importante.
- El equipo de sistemas de la empresa revisará la información de accounting. Así se podrá determinar cuándo, cómo y con qué usuario se realizó el borrado.
- El empleado correspondiente será penalizado.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

Actividad 3. La Red TOR: Deep Web, Darknet y Dark Web.

Vamos a investigar sobre la red TOR:

Primero lee los siguientes artículos y realiza un resumen con tus palabras sobre

Deep Web, Darknet diferencias

Que es la dark-web

Después averigua qué es TOR y cómo funciona. Redacta un resumen con tus palabras y prepara un esquema con su funcionamiento.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

Actividad 3. La Red TOR: Deep Web, Darknet y Dark Web.

Por último, nos vamos a informar sobre cómo se espía a los usuarios de TOR:

Lee el siguiente artículo y redacta un resumen con tus palabras.

Como espía la NSA a los usuarios de TOR

Averigua qué fue el caso Snowden. Realiza un resumen con tus palabras e indica tu opinión sobre el mismo.

Averigua si en otros países se ha realizado algún tipo de espionaje a la población por parte del gobierno

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

ALTA DISPONIBILIDAD

- La alta disponibilidad (*High Availability*) se refiere a la **capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones**, **debido principalmente a su carácter critico**.

- El objetivo de la misma es mantener nuestros sistemas funcionando las 24 horas del día, 7 días a la semana, 365 días al año, manteniéndolos a salvo de interrupciones.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

ALTA DISPONIBILIDAD

- Se diferencian dos **tipos de interrupciones**:
  - Las **interrupciones previstas**, que se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.
  - Las **interrupciones imprevistas**, que suceden por acontecimientos imprevistos (como un apagón, un error del hardware o del software, problemas de seguridad, un desastre natural, virus, accidentes, caídas involuntarias del sistema).

ÍNDICE

- Introducción a la seguridad informática
- Fiabilidad. Confidencialidad. Integridad. Disponibilidad
- **Elementos vulnerables**
- Amenazas. Tipos
- Medidas de seguridad
- Análisis forense en sistemas informáticos

ELEMENTOS VULNERABLES

- Los problemas de seguridad informática no deben ser tratados de manera aislada. Sería como si en casa pusiéramos una puerta blindada pero no se protegieran las ventanas.

- La seguridad informática precisa de un **nivel organizativo**, que facilite unas normas y pautas comunes para los usuarios de la empresa

Sistema de seguridad = Tecnología + Organización

ELEMENTOS VULNERABLES

- Los tres elementos principales que se deben **proteger** en un sistema informático son:
  - El **software**.
  - El **hardware**.
  - Los **datos**.
- Otros elementos, con menos relevancia, que también se aconsejan proteger son los **fungibles** (aquellos que se gastan o desgastan con el uso continuo).

ELEMENTOS VULNERABLES

- De los tres elementos mencionados **los datos son el principal elemento a proteger**, por ser el **más amenazado** y el **más difícil de recuperar**.

- Por ejemplo, un servidor estará ubicado en un lugar de acceso físico restringido o, por lo menos, controlado. Además, en caso de pérdida este software se puede restaurar sin problema desde su medio original.

- En otros casos (una BD o un proyecto) no tenemos un medio original y se recurre a las copias de seguridad para evitar perder la información en su totalidad.

ELEMENTOS VULNERABLES

- Contemplaremos distintos **niveles** de profundidad relativos a la seguridad informática:
  - **Seguridad pasiva**: seguridad física y ambiental junto con copias de seguridad. Complementa la seguridad activa.
  - **Seguridad activa**: conjunto de medidas que previenen e intentan evitar daños en los sistemas informáticos.
  - **Seguridad en redes corporativas**: utilizando ciertos protocolos como SSH, TLS/SSL, uso de VPN, cortafuegos, proxy, etc.
  - **Normativa legal** en seguridad informática como LOPD y LSSICE.

ELEMENTOS VULNERABLES

- Dentro del **nivel de seguridad pasiva** hay que destacar la:
  - **Seguridad física**: Es aquella que trata de proteger el hardware de los posibles desastres naturales, incendios, sobrecargas eléctricas, robos, etc.
- Dentro del **nivel de seguridad activa** hay que destacar la:
  - **Seguridad lógica**: Complementa la seguridad física, protegiendo el software de los equipos informáticos. Control de acceso a los sistemas, gestión de sistemas operativos, cifrado, software antimalware, etc.
- Por otro lado ayudan las:
  - **Configuraciones de alta disponibilidad** que utilizan el concepto de redundancia con RAIDs, balanceo de carga, virtualización, etc.

ELEMENTOS VULNERABLES

Actividad 4. Amenazas a elementos vulnerables.

1. Busca en internet los siguientes términos: hacker, cracker, newbie, wannaber y grey hat.

2. ¿Qué problemas crees que podrían causarse por un uso inadecuado del software?

3. Averigua qué son las vulnerabilidades TEMPEST

ÍNDICE

- Introducción a la seguridad informática
- Fiabilidad. Confidencialidad. Integridad. Disponibilidad
- Elementos vulnerables
- **Amenazas. Tipos**
- Medidas de seguridad
- Análisis forense en sistemas informáticos

AMENAZAS. TIPOS

Posibles amenazas a un sistema informático

- Los posibles tipos de ataques a los elementos que acabamos de comentar se pueden englobar en:
  - Intercepción
  - Modificación
  - Interrupción
  - Generación

AMENAZAS. TIPOS

Posibles amenazas a un sistema informático

- **Intercepción**: Una persona, programa o proceso accede a una parte del sistema a la que no está autorizado. Sniffers, keyloggers, etc.
- **Modificación**: Además de tener acceso, modifica, destruye, reemplaza o cambia los datos o el funcionamiento del sistema.
- **Interrupción**: Consiste en impedir que la información llegue a su destino.
- **Generación**: Se refiere a la posibilidad de incluir campos y registros en una base de datos, añadir líneas de código a un programa, añadir programas completos en un sistema (virus), introducir mensajes no autorizados por una línea de datos

AMENAZAS. TIPOS

- Las amenazas a un sistema informático pueden ser provocadas por:
  - Personas
  - Condiciones físicas-ambientales
  - Lógicas (Software)

AMENAZAS. TIPOS

Amenazas provocadas por personas

- Generalmente se tratará de piratas informáticos, hackers o crakers, que intentan aprovechar las vulnerabilidades del software.

- Podemos dividirlos en:
  - **Atacantes pasivos**: fisgonean el sistema sin modificarlo ni destruirlo.
  - **Atacantes activos**: dañan o modifican el sistema o elemento atacado.

AMENAZAS. TIPOS

Amenazas físicas-ambientales

- Este tipo de amenazas afectan a las instalaciones y/o el hardware contenido en ellas.
- Suponen el primer nivel de seguridad a proteger para garantizar la disponibilidad de los sistemas.

AMENAZAS. TIPOS

Amenazas lógicas (software)

- Una amenaza lógica es software que puede afectar o dañar nuestro sistema y que ha sido creado bien con esa finalidad o bien por error.

- Como amenazas lógicas encontramos:
  - **Herramientas de seguridad**: pueden detectar fallos para solucionarlos o para aprovecharlos.
  - **Rogueware**: son falsos programas de seguridad como antivirus o antiespías.
  - **Backdoors**: son atajos que se añaden por parte de los administradores que no tienen un nivel de seguridad adecuado.

AMENAZAS. TIPOS

Amenazas lógicas (software)

- Como amenazas lógicas encontramos (continuación):
  - **Virus**: código insertado en un fichero ejecutable, de manera que cuando se ejecuta dicho archivo lo hace también el virus.
  - **Gusano**: programa que se ejecuta y propaga por sí mismo a través de redes, normalmente mediante correo spam.
  - **Troyanos**: aplicaciones que aparentan ejecutar unas tareas pero que llevan asociadas otras ocultas.
  - **Programas bacterias**: no hacen nada pero se "reproducen" hasta saturar los recursos del sistema.

FIABILIDAD. CONFIDENCIALIDAD. INTEGRIDAD. DISPONIBILIDAD

Actividad 5. Virus informáticos.

1. Haz una búsqueda sobre los distintos virus más importantes de la historia. Haz una lista con ellos (mínimo 5).

2. Escoge un virus y busca información más detallada de él, como el año de aparición, comportamiento y noticias relacionadas con él. Prepara un documento con todo lo que encuentres.

AMENAZAS. TIPOS

Técnicas de ataque

- Acabamos de ver quién o qué puede generar una amenaza para el sistema informático que estemos administrando.
- Ahora vamos a analizar estas amenazas en función de la técnica que se emplee para realizarlo.
- Se van a mencionar las más usuales, aunque no debemos olvidar que hay que estar al día en estos temas, pues pueden aparecer técnicas nuevas.

AMENAZAS. TIPOS

Técnicas de ataque

- **Malware**
  - Son las amenazas más conocidas, en parte por llevar mucho tiempo con nosotros.
  - Aquí englobamos virus, espías, gusanos, troyanos, etc.
  - Tienen como finalidad controlar el sistema, realizar ciertas tareas en remoto, dejarlo inutilizable, etc.
  - Es importante tener cuidado con los falsos antivirus.

https://www.youtube.com/watch?v=NPsjN8AvNQM

AMENAZAS. TIPOS

Técnicas de ataque

- **Malware**
  - Uno de los malware más dañinos hoy día es el **Ransomware**.
  - Es un programa malicioso que se hace con el control del sistema y exige un pago para recuperarlo.
  - Su funcionamiento es variable: desde mensajes emergentes continuos solicitando un pago hasta el bloqueo completo del equipo.

AMENAZAS. TIPOS

Técnicas de ataque

- **Ingeniería social**
  - Al crear una contraseña solemos utilizar datos nuestros o lugares relacionados con nuestro entorno.
  - Si obtenemos información de la persona o si se la conoce se puede intentar averiguar su contraseña utilizando este tipo de información.
  - Se trata de obtener información confidencial a través de la manipulación y la confianza del usuario.

AMENAZAS. TIPOS

Técnicas de ataque

- **Scam**
  - Es una estafa electrónica utilizando donaciones, transferencias, compra de productos fraudulentos, etc.
  - Las cadenas de emails se consideran scam cuando hay pérdida monetaria por parte de los usuarios afectados por el engaño.
  - En caso de que solo sea un bulo y no afecte económicamente al usuario se las conoce como hoax (bulo).

AMENAZAS. TIPOS

Técnicas de ataque

- **Spam**
  - Correo electrónico o mensaje basura, es decir, correos que no han sido solicitados ni son deseados para el destinatario, además el remitente puede no ser conocido.
  - Hoy día se engloban aquí los correos publicitarios.
  - Este tipo de emails podría utilizarse dentro de la ingeniería social, pues basándose en la confianza que dé el supuesto remitente puede llevar adjunto un ataque scam, phishing, hoax o malware.

AMENAZAS. TIPOS

Técnicas de ataque

- **Sniffing**
  - Técnica que consiste en monitorizar el tráfico de una red para hacerse con información confidencial.
  - El atacante se conecta a un tramo de red del equipo y acceder a todas sus comunicaciones.
  - Hay programas de escucha que pueden ser empleados para esta finalidad nada legítima, a pesar de no ser ese su objetivo.

AMENAZAS. TIPOS

Técnicas de ataque

- **Spoofing**
  - Suplantación de identidad o falsificación, por ejemplo encontramos IP, MAC, tabla ARP, web o *mail Spoofing*.
  - Es decir, alteramos el comportamiento de algún elemento de nuestra máquina para hacernos pasar por otra.
  - Por ejemplo, un hacker puede usar spoofing para conseguir datos sensibles de la víctima, o utilizar sus recursos computacionales, haciéndole creer que es una fuente fiable.
  - En su forma más primitiva se refiere a la suplantación telefónica.

AMENAZAS. TIPOS

Técnicas de ataque

- **Pharming**
  - Redirigir un nombre de dominio a otra máquina, falsificada y fraudulenta.
  - Es similar al phishing donde el tráfico de un sitio web es manipulado para permitir el robo de información confidencial.
  - Un hacker puede instalar, por ejemplo, un virus o troyano en el ordenador de la víctima para dirigir el tráfico a una web falsa. Otra forma es manipulando un servidor DNS para que redirija al sitio falso en cuestión.

AMENAZAS. TIPOS

Técnicas de ataque

- **Phishing**
  - Estafa basada en la suplantación de identidad y el uso de la ingeniería social para adquirir acceso a datos sensibles de un usuario, como acceso a su cuenta bancaria.
  - El atacante se hace pasar por un tercero con el que la víctima tiene relación.
  - En el contenido del mensaje intenta que el usuario acceda a un enlace falso desde donde solicitar datos de acceso.

AMENAZAS. TIPOS

Técnicas de ataque

- **Password cracking**
  - Consiste en descifrar contraseñas de sistemas y comunicaciones.
  - Los métodos más comunes son mediante sniffing, observando directamente la introducción de credenciales, ataques de fuerza bruta, etc.

AMENAZAS. TIPOS

Técnicas de ataque

- **Botnet**
  - Conjunto de robots o bots que se ejecutan de manera autónoma y automática en multitud de hosts, normalmente infectados, permitiendo controlar dichos equipos infectados de forma remota.
  - Sus fines normalmente son rastrear información confidencial o incluso cometer actos delictivos.

AMENAZAS. TIPOS

Técnicas de ataque

- **DoS**
  - También conocido como Denegación de servicio.
  - Busca que un servicio o un recurso sea inaccesible a usuarios legítimos.
  - Por ejemplo, un hacker puede provocar la caída de un servidor saturándolo con peticiones falsas.
  - Una ampliación de este ataque, conocida como DDoS (distribuido), utiliza una botnet para el mismo fin. Hoy día es más usual y eficaz que su predecesora.

ANÁLISIS FORENSE EN SISTEMAS INFORMÁTICOS

ACTIVIDAD 6. Técnicas de ataque.

Lee el siguiente artículo sobre cómo realizar un Phishing:

Crear página de Phishing

1. Averigua qué son y qué uso tienen las herramientas Blackeye y Ngrok.
2. Échale un vistazo a los pasos indicados. Pon ejemplos de cinco web que Blackeye puede imitar.
3. Busca herramientas relacionadas con los ataques sniffing. Menciona al menos dos

Crea un documento con las respuestas.

ÍNDICE

- Introducción a la seguridad informática
- Fiabilidad. Confidencialidad. Integridad. Disponibilidad
- Elementos vulnerables
- Amenazas. Tipos
- **Medidas de seguridad**
- Análisis forense en sistemas informáticos

MEDIDAS DE SEGURIDAD

- La mayoría de las acciones que realizan las empresas generan un gran volumen de información confidencial.
- Implementar unas medidas de seguridad informática es vital para que la empresa pueda trabajar de forma correcta y para que cumpla con las medidas vigentes de protección de datos.
- Hemos de diseñar unas políticas de seguridad que definan las reglas a seguir para evitar amenazas o minimizar daños, en caso de que se produzcan.

MEDIDAS DE SEGURIDAD

- A continuación vamos a mencionar algunas de las medidas que se recomiendan implementar en una empresa:
  - **Control de acceso a los datos**. Limitar el acceso a información sensible a los usuarios imprescindibles, para evitar comprometerla.
  - **Realizar copias de seguridad de manera periódica** para evitar pérdidas de información y restaurar sistemas.
  - **Utilizar contraseñas seguras**, **dinámicas** (cambiarse periódicamente) y **aleatorias**, evitando utilizar información personal en las mismas.

MEDIDAS DE SEGURIDAD

- A continuación vamos a mencionar algunas de las medidas que se recomiendan implementar en una empresa:
  - **Proteger el correo electrónico.** Utilizar filtros antispam y sistemas de encriptación de mensajes.
  - **Contratar servicios de seguridad integral**.
  - **Asegurar las comunicaciones** y el uso de Internet no solo para los casos en que los equipos de la empresa naveguen, también por los teléfonos.
  - **Involucrar**, en la medida de lo posible, **a toda la empresa** en la implantación y uso de las medidas de seguridad.

ÍNDICE

- Introducción a la seguridad informática
- Fiabilidad. Confidencialidad. Integridad. Disponibilidad
- Elementos vulnerables
- Amenazas. Tipos
- Medidas de seguridad
- **Análisis forense en sistemas informáticos**

ANÁLISIS FORENSE EN SISTEMAS INFORMÁTICOS

- El análisis forense informático permite conocer dónde se ha producido el problema y quién está detrás del mismo.

- Un análisis forense está estructurado en una serie de fases, siendo las principales:
  - **Fase de protección**: su objetivo es impedir que ninguna persona externa pueda alterar el sistema una vez que comienza la investigación.
  - **Fase de identificación**: el forense debe recolectar una serie de pruebas o indicios que le ayuden a constatar las irregularidades que se han producido.
  - **Recolección de datos**: la fase más delicada porque puede suponer una alteración de las evidencias.

ANÁLISIS FORENSE EN SISTEMAS INFORMÁTICOS

- **Análisis**: una vez se ha recolectado la información relevante se procede a analizarla. Se estudian ficheros con información eliminada, registros, logs, accesos al sistema, etc.
- **Informe de resultados**: cuando se relacionan procesos con indicios se redacta un informe de tipo pericial donde se incluyen las conclusiones finales.

ANÁLISIS FORENSE EN SISTEMAS INFORMÁTICOS

ACTIVIDAD 7. Análisis forense.

Busca información sobre las funciones de un perito informático forense. Determina lo siguiente:

1. ¿Cuáles son sus funciones?
2. ¿Qué es la ciencia forense digital? ¿Cuál es su objetivo?
3. ¿Cómo conseguimos este tipo de certificación?
4. Averigua las fases del peritaje informático forense.