1. La seguridad de la información

La **seguridad informática** es el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático (conjunto de hardware, software, personas y procedimientos) de integridad, confidencialidad y disponibilidad

1.1. Principios de la seguridad informática

- **Integridad:** Un sistema informático es íntegro cuando impide la modificación de la información a cualquier usuario que no haya sido autorizado con anterioridad.
- **Confidencialidad:** Un sistema informático es confidencial cuando impide la visualización de datos a los usuarios que no tengan privilegios en el sistema.
- **Disponibilidad:** Un sistema informático es disponible cuando está en todo momento en funcionamiento y accesible para que los usuarios autorizados puedan hacer un uso adecuado de ellos.

1.2. ¿Qué queremos proteger?

La seguridad informática pretende **proteger recursos** valiosos de una organización. Los 3 pilares fundamentales a proteger son:

- La información

- El hardware
- El software

Para ello se establecen **planes de seguridad** que garantizan los tres principios establecidos con anterioridad. Estos nos ayudan a identificar **vulnerabilidades** e implementar planes de contingencia adecuados.

1.3. Contra qué nos tenemos que proteger

- **nosotros mismos**: Borramos archivos sin darnos cuenta, eliminamos programas necesarios para la seguridad o aceptamos correos electrónicos perjudiciales para el sistema.
- **accidentes y averías**: Pueden hacer que se estropee nuestro ordenador y perdamos datos necesarios.
- **usuarios intrusos**: Bien desde el mismo ordenador, bien desde otro equipo de la red, puedan acceder a datos de nuestro equipo.
- **software malicioso o malware**: Programas que aprovechan un acceso a nuestro ordenador para instalarse y obtener información, dañar el sistema o incluso llegar a inutilizarlo por completo

2. Amenazas

2.1. Tipos de amenazas

Amenazas Humanas

- Ataques Pasivos
    - Usuarios con conocimientos básicos
    - Hackers
- Ataques Activos
    - Antiguos empleados de una Organización
    - Crackers y otros Atacantes

Amenazas Lógicas

- Software Malicioso
- Vulnerabilidades del Software

Amenazas Físicas

- Fallos en los dispositivos
- Accidentes

- Catástrofes Naturales

2.2. Conductas de seguridad

Técnicas de seguridad activa

Su fin es evitar daños a los sistemas informáticos:

Estrategias:

- Empleo de **contraseñas** adecuadas y seguras (elegir una contraseña segura, comprobar la seguridad de una contraseña)
- **Encriptación** de los datos (codificar la información con una contraseña, cualquier persona que la intercepte no pueda ver el mensaje original)
- El uso de **software de seguridad** informática
- Control de Acceso
- Firmas y Certificados Digitales
- Protocolos Seguros

Técnicas o prácticas de seguridad pasiva

Su fin es minimizar los efectos causados por un accidente, un usuario o un malware.

Estrategias:

- Hardware adecuado frente a accidentes y averías (refrigeración del sistema, conexiones eléctricas adecuadas, etc.)
- Realización de copias de seguridad (backup) de los datos (en más de un soporte y en distintas ubicaciones físicas)
- Herramientas de Limpieza
- Sistemas de Alimentación Ininterrumpida (SAI)
- Sistemas Redundantes

3. Malware

Se trata de un programa malicioso, potencialmente peligroso. Tiene la capacidad de hacer daño a un equipo y posibilidad de propagación

Los **ciberataques** combinan habitualmente varios tipos.

3.1. Tipos de malware más conocidos

Enlace: los 8 virus más famosos de todos los tiempos.

https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html

Virus

Programa que se instala en el ordenador sin el conocimiento del usuario Finalidad de propagarse a otros equipos. Puede provocar desde pequeñas bromas hasta la destrucción total de discos duros.

Gusano

Tipo de virus Finalidad Multiplicarse e infectar una red de ordenadores. Consecuencias No suelen implicar la destrucción de archivos pero sí ralentizan el funcionamiento.

Troyano

Código malicioso que se oculta dentro de un archivo inofensivo y útil o llamativo para el usuario. Requieren la intervención de sus víctimas para propagarse.

Existen una gran variedad de troyanos, en función de sus acciones y utilidades:

- **Downloader** (descarga otros programas maliciosos)
- **Clicker** (busca beneficio económico a través de clicks en publicidad)
- **Keylogger** (registra las actividades que se realizan en el sistema)
- **Backdoor** (abre puertos en el sistema)
- **Bot** (controla el equipo de forma remota), etc.

Spyware

Programa que se instala en el ordenador sin conocimiento del usuario con la finalidad de recopilar información sobre el usuario para enviarla a servidores de Internet gestionados por compañías de publicidad.

Adware

Software que se esconde en los anuncios de Internet. Tras acceder los equipos y dispositivos, este malware roba la información de las empresas y usuarios.

Ransomware

El **ransomware** es un tipo de malware que toma a sus archivos como rehenes.

Lanzado en septiembre de 2013, **CryptoLocker** se extendió a través de archivos adjuntos de correo electrónico y cifró los archivos del usuario para que no pudieran acceder a ellos.

Luego, los piratas informáticos envian supuestamente una clave de descifrado a cambio de una suma de dinero.

Rogue

Rootkit

3.2. Otras amenazas malware

Pharming

Suplantación de páginas web por parte de un servidor instalado en el equipo sin que el usuario lo sepa.

Finalidad:

- Obtener datos bancarios
- Cometer delitos económicos

Phishing

Obtener información confidencial de los usuarios de banca electrónica mediante el envío de correos electrónicos.

Spam

Envío de correo electrónico publicitario de forma masiva a cualquier dirección de correo electrónico existente. Su finalidad en general suele ser la de vender productos.

Hoax

Mensajes de correo distribuidos en cadena, cuyo objetivo es realizar engaños masivos. Por ejemplo:

- Historias solidarias inventadas
- Mensajes que traen mala suerte
- Alertas falsas sobre virus

4. Ataques a los sistemas informáticos

4.1. Tipos de ataques

- **Interrupción**: Destruir o dejar inutilizable los dispositivos.
- **Interceptación**: Acceder a recursos para los que no tiene autorización.
- **Modificación**: Acceder a los recursos y manipularlos.
- **Suplantación o fabricación**: Inserta objetos falsificados. Pueden ser:
    - Suplantación de identidad
    - Suplantación de una dirección web
    - Suplantación de una dirección IP

4.2. Ingeniería social

Técnica que explota ciertos comportamientos y conductas de los seres humanos. Se utiliza para conseguir información, privilegios o acceso a sistemas engañando al usuario mediante simulaciones:

- Empleado de banco

- Comercial de una empresa
- Compañero de trabajo
- Un técnico Etc..

4.3. Ataques remotos

Se trata de un conjunto de técnicas utilizadas para intentar acceder a un sistema informático a distancia. Se suele utilizar software malicioso que aprovecha vulnerabilidades de seguridad de programas o del sistema operativo.

- **Inyección de Código:** Añade o borra información en sitios remotos
- **Escaneo de Puertos**: Averigua los puertos abiertos para atacar.
- **Denegación de Servicios (DoS):** Satura los recursos de un equipo o de una red para que deje de responder. Escuchas de Red: Captura e interpreta el tráfico de una red.
- **Spoofing**: Suplanta la identidad del usuario.
- **Fuerza Bruta:** Probar todas las combinaciones posibles de claves de un sistema.
- **Elevación de Privilegios:** El atacante se hace root o administrador para controlar más.

5. Protección contra malware

5.1. Políticas de seguridad

5.2. Soluciones antivirus

Un antivirus es un software que tiene como finalidad prevenir,detectar y eliminar el malware del sistema. Cuando hay una amenaza, el antivirus manda un mensaje al usuario dándole la oportunidad de acabar con ella.

Los antivirus se encuentran en constante actualización, debido a la aparición de nuevos virus. Los antivirus, además, suelen incorporar otras funciones como:

- Antispam
- Cortafuegos
- Cifrado de datos
- Monitor de red

Existe una gran variedad de antivirus, entre los más destacados están:

- Avast
- Avira
- Gdata
- KAspersky,etc.

5.3. Síntomas de una infección

Algunos síntomas de infección habituales de que un equipo puede estar infectado por algún tipo de malware:

- El sistema va mas lento.
- Desaparece información privada.

- Te sale publicidad indeseada.
- El ratón o las ventanas se mueve sin que tu hagas nada.
- Mal funcionamiento de algunas aplicaciones.
- Conexiones a Internet no intencionadas.
- Cambio del buscador predeterminado.
- Barras nuevas en el navegador sin tu consentimiento.
- Envío de mensajes sin tu mandarlos.
- Aumento de la actividad de tu equipo.

5.4. Pasos que debe darse en caso de infección

- Restaurar e sistema a un estado anterior: De esta manera no se pierde información, pero si se elimina el virus.
- Actualizar la base de datos del antivirus y realizar un análisis del sistema.
- Arrancar el sistema con un LiveCD o Live USB: permite analizar el equipo con un sistema que no está contaminado y recuperar información.
- Ejecutar utilidades de desinfección específicas, que eliminas amenazas concretas: esto sirve cuando ya ha sido detectada la amenaza.

6. Cifrado de la información

6.1. Orígenes

6.2. Criptografía

Criptografía simétrica

Criptografía asimétrica

Criptografía de clave pública

7. Firma electrónica y certificado digital

7.1 Firma electrónica

Firma de documentos electrónicos.

7.2. certificado digital

Autoridades de certificación

8. Navegación segura

8.1. Buenas prácticas

8.2. Navegación privada

8.3. Proteger la privacidad en la red con un proxy

8.4. Navegación anónima

9. Privacidad de la información

9.1. Amenazas a la privacidad

9.2. Antiespías

9.3. Borrar archivos de forma segura

Los archivos borrados, incluso después de ser borrados, pueden ser recuperados mediante software adecuado.

Existen programas para ello, así como para asegurar que los archivos se eliminan de forma segura e irrecuperable.

10. Protección de las conexiones de red

10.1. Cortafuegos

Es un hardware o software que controla la información entrante y saliente del equipo, actuando como defensa en caso de amenaza.fr

Este se encarga de examinarla y comprueban que superen los criterios de seguridad. estos criterios pueden establecerse en función de las preferencias de cada uno.

Se utiliza en los dispositivos con internet y suelen incluirse con los antivirus, aunque algunos sistemas operativos como Windows ya llevan instalado el suyo propio.

10.2. Redes privadas virtuales

Consiste en conectarse a Internet a través de una red privada, estableciendo una conexión cifrada y así evita que el buscador guarde tus datos.

- VPN de acceso remoto: acceso a una red privada con una red pública. Ejemplos son conexiones desde lugares públicos como hoteles o cafeterías.
- VPN de sitio a sitio: conectar redes a través de internet, pudiendo comunicarse entre ellas.

10.3. Certificados de servidor web y HTTPS

SSL es un protocolo criptográfico en el que se otorgan certificados a las páginas para garantizar la integridad y confidencialidad de las comunicaciones de esta.

Cuando TSL y SSL se combinan, forman el protocolo de navegación HTTPS. Este es indicador de que se trata de un lugar seguro, en el que se asegura como un sito de comercio electrónico seguro.

En los navegadores aparece como un candado verde, y si además el nombre de la web están en verde es que se trata de una versión extendida de este protocolo.

11. Seguridad en comunicaciones inalámbricas

Seguridad en Bluetooth, seguridad en redes wifi.