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.

Ejemplos:

- Alteración malintencionada de archivos
- Modificación de informes de ventas (empleados)

Confidencialidad: Un sistema informático es confidencial cuando impide la visualización de datos a los usuarios que no tengan privilegios en el sistema.

Ejemplos:

- Robo de información confidencial por parte de un atacante a través de internet
- Divulgación no autorizada a través de las redes sociales de información confidencial
- Acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no debería tener acceso

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.

Ejemplos:

- Imposibilidad de acceder al correo electrónico corporativo

- Ataque de denegación de servicio, en el que el sistema «cae»impidiendo accesos legítimos.

1.2. ¿Qué queremos proteger?

La seguridad informática pretende **proteger recursos** valiosos de una organización. En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

- **Hardware**: elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, cintas, DVDs,...).
- **Software**: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
- **Datos**: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.
- **Otros**: fungibles, personas, infraestructuras,.. aquellos que se 'usan y gastan' como puede ser la tinta y papel en las impresoras, los soportes tipo DVD o incluso cintas si las copias se hacen en ese medio, etc.

De ellos los mas críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.

Incluso de todos ellos, el activo mas crítico son los **datos**. El resto se puede reponer con facilidad y los datos ... sabemos que dependen de que la empresa tenga una buena política de copias de seguridad y sea capaz de reponerlos en el estado mas próximo al momento en que se produjo la pérdida. Esto puede suponer para la empresa, por ejemplo, la dificultad o imposibilidad de reponer dichos datos con lo que conllevaría de pérdida de tiempo y dinero.

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

1.4. La importancia de los datos

La importancia de la información que manejamos será, en gran medida,relativa a nuestro sector de negocio.

Ámbito sanitario

Gran volumen de información personal de pacientes, a la que se deben aplicar todas las medidas de seguridad para evitar que se pierda, modifique o se acceda a ella sin autorización.

Suele ser necesario llevar un registro de los accesos y modificaciones.

Sector financiero

Se maneja información confidencial tanto de clientes como de operaciones financieras de compras y ventas de activos cuya difusión puede suponer una importante pérdida económica o un perjuicio para nuestros clientes.

Sectores industriales o de desarrollo de productos

Confidencialidad de los procesos y procedimientos que nos pueden aportar una mejora de productividad sobre la competencia.

Hostelería y restauración

Se maneja, además de un volumen de datos de carácter personal muy significativo, información sobre reservas, cuya pérdida nos podría poner en una situación muy complicada con nuestros clientes.

Legislación de datos

La legislación sobre protección de datos de carácter personal, define datos personales como toda información sobre una persona física identificada o identificable.

Una **persona es identificable** si puede determinarse su identidad, directa o indirectamente.

Esta legislación exige la protección de la seguridad de los datos de carácter personal ante posibles riesgos que afecten a la privacidad de las personas por ejemplo: acceso no autorizado, uso ilegítimo, modificación no autorizada, discriminación por perfilado o pérdida de datos.

Datos sensibles

Existen categorías especiales de datos, los denominados **datos sensibles** que exigen una protección reforzada y que están sujetos a un régimen jurídico especial.

Estos datos son datos personales que revelan:

- Ideología, afiliación sindical, opiniones políticas
- Creencias religiosas y otras creencias.
- Origen racial o étnico
- Relativos a la salud o la vida sexual y orientación sexual, datos genéticos y biométricos.
- Datos de condenas penales o administrativas

2. Amenazas

2.1. Tipos de amenazas

Existen 3 tipos de amenazas según su origen:

Amenazas Humanas

Tipos de amenazas humanas más habituales:

- Usuarios con conocimientos básicos
- Hackers
- Antiguos empleados de una Organización

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

El fin de las medidas de seguridad activa es evitar daños a los sistemas informáticos.

Para ello podemos utilizar diferentes 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
- Utilizar protocolos seguros como HTTPS

Enlaces:

- Comprobar si nuestros datos han sido comprometidos
- https://howsecureismypassword.net/

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 cuya finalidad es la de multiplicarse e infectar una red de ordenadores.

Las 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

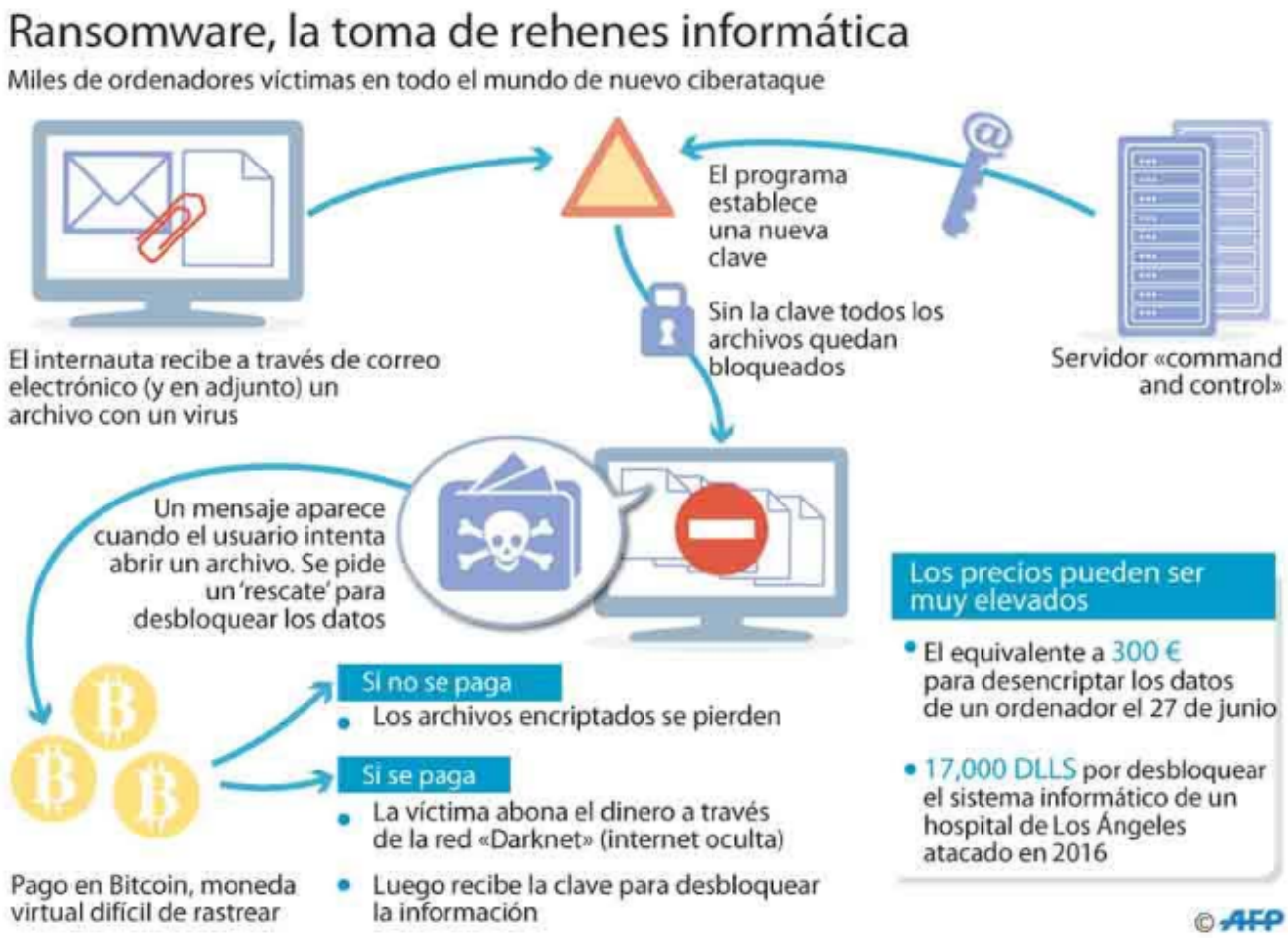
Software que se esconde en los anuncios de Internet. Tras acceder los equipos y dispositivos, este malware roba la información de las empresas y usuarios.

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.

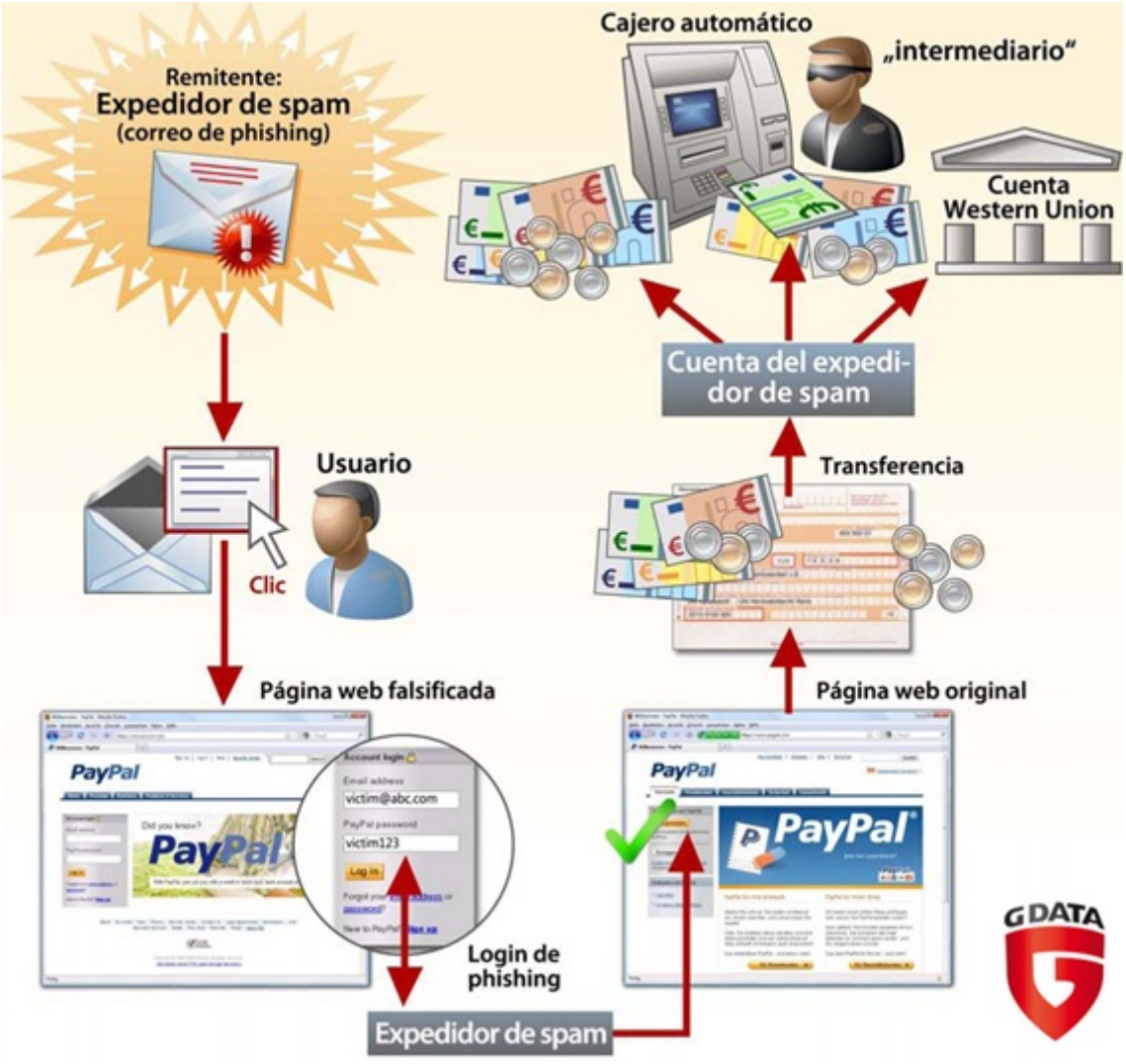


3.2. Otras amenazas malware

Phishing

Es un tipo de fraude ejecutado a través de un **correo electrónico** en el que se solicita la actualización de los datos personales (usualmente vinculados a cuentas u otros instrumentos financieros).

Aparece un **enlace** para que se haga clic de acceso a una página falsa que tendrá prácticamente la **misma apariencia** de la página de la institución simulada.



Pharming

Se instala un código malicioso introducido premeditadamente que permite **redireccionar** un nombre de dominio a otra máquina diferente.

Si el usuario ha sido redireccionado, cuando introduzca el nombre de dominio ingresará a una página 'web' falsa (en apariencia similar a la que deseaba ingresar) permitiéndole al estafador obtener todos los datos personales del cliente.

Finalidad:

- Obtener datos bancarios
- Cometer delitos económicos

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

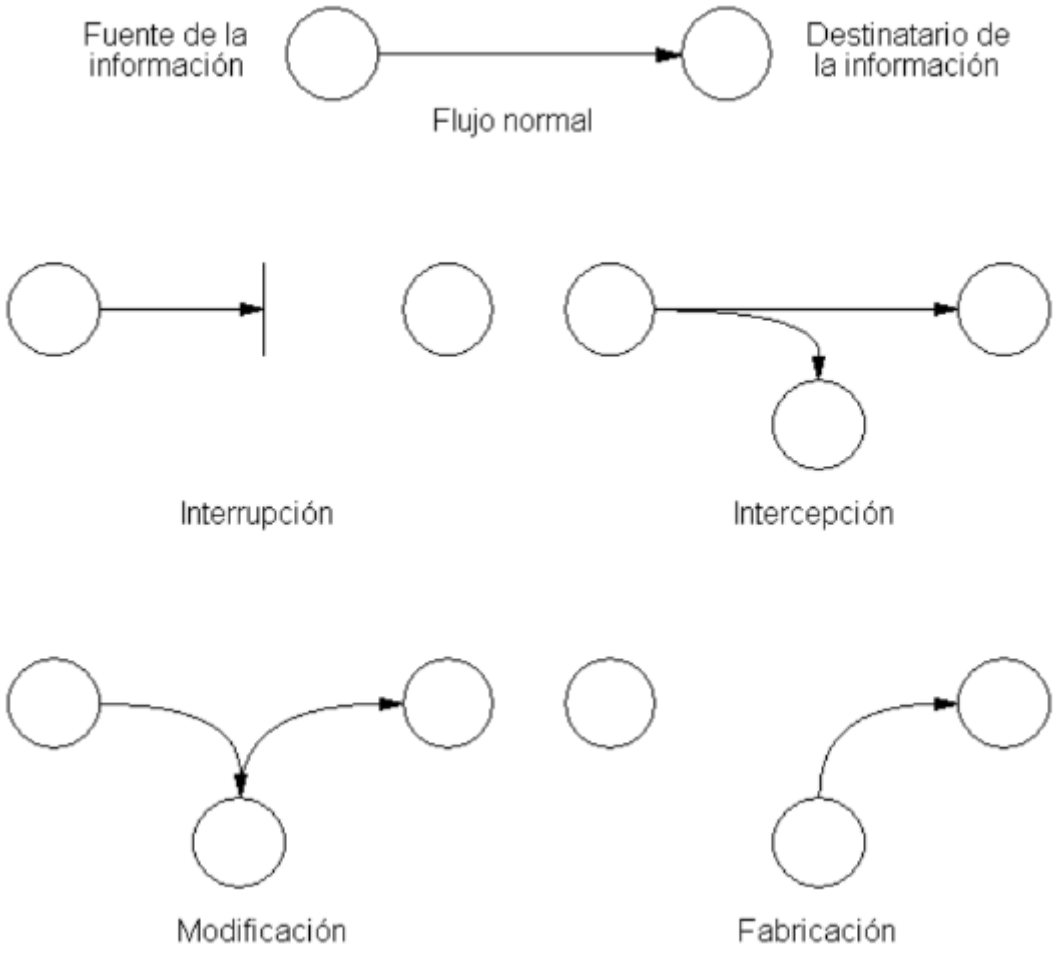
Mensajes de correo distribuidos en cadena, cuyo objetivo es realizar engaños masivos. Por ejemplo:

- 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

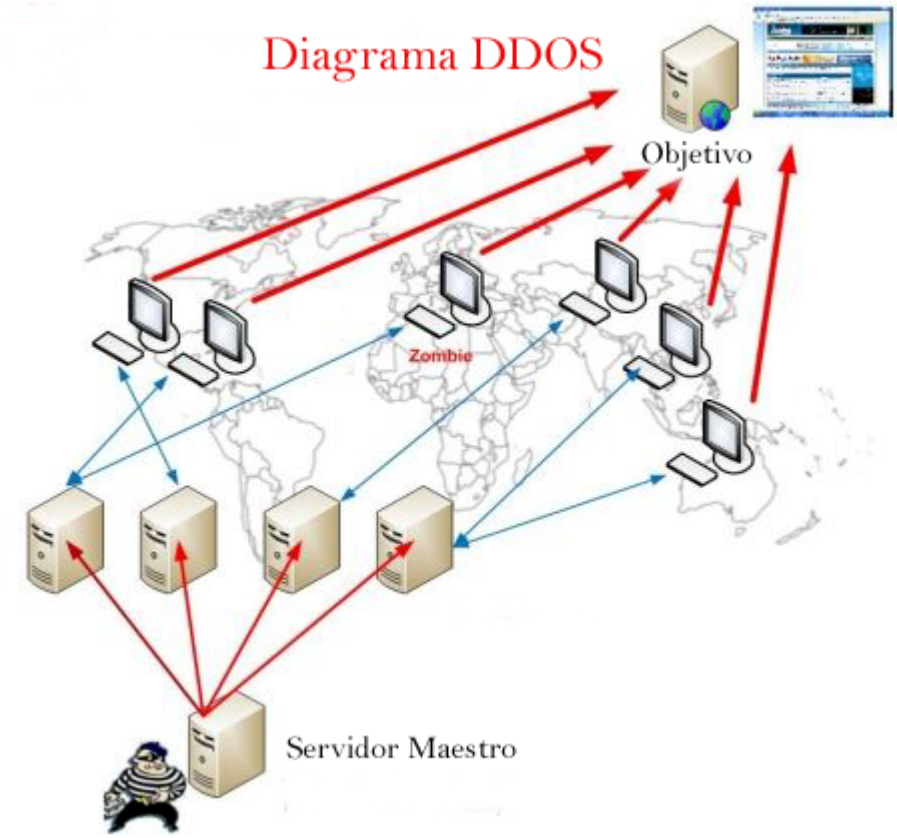
Se trata de un conjunto de técnicas utilizadas para intentar acceder a un sistema informático a distancia. Se suele utilizar software malicioso que aprovecha vulnerabilidades de seguridad de programas o del sistema operativo.

- **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.

Ejemplos:

- SQL Injection

Diagrama de un ataque DDos:



5. Protección contra malware

5.1. Políticas de seguridad

Es el conjunto de normas y procedimientos que definen las diferentes formas de actuación recomendada con el fin de garantizar un cierto nivel de seguridad.

Es imposible tener un sistema de seguridad totalmente seguro porque además de que no se podría acceder a muchos sitios es muy caro tener el nivel total 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 el 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

La criptografía (del griego 'escritura oculta') es la ciencia de cifrar y descifrar información con técnicas especiales, usado frecuentemente en mensajes que solo puedan ser leídos por las personas a las que van dirigidos.

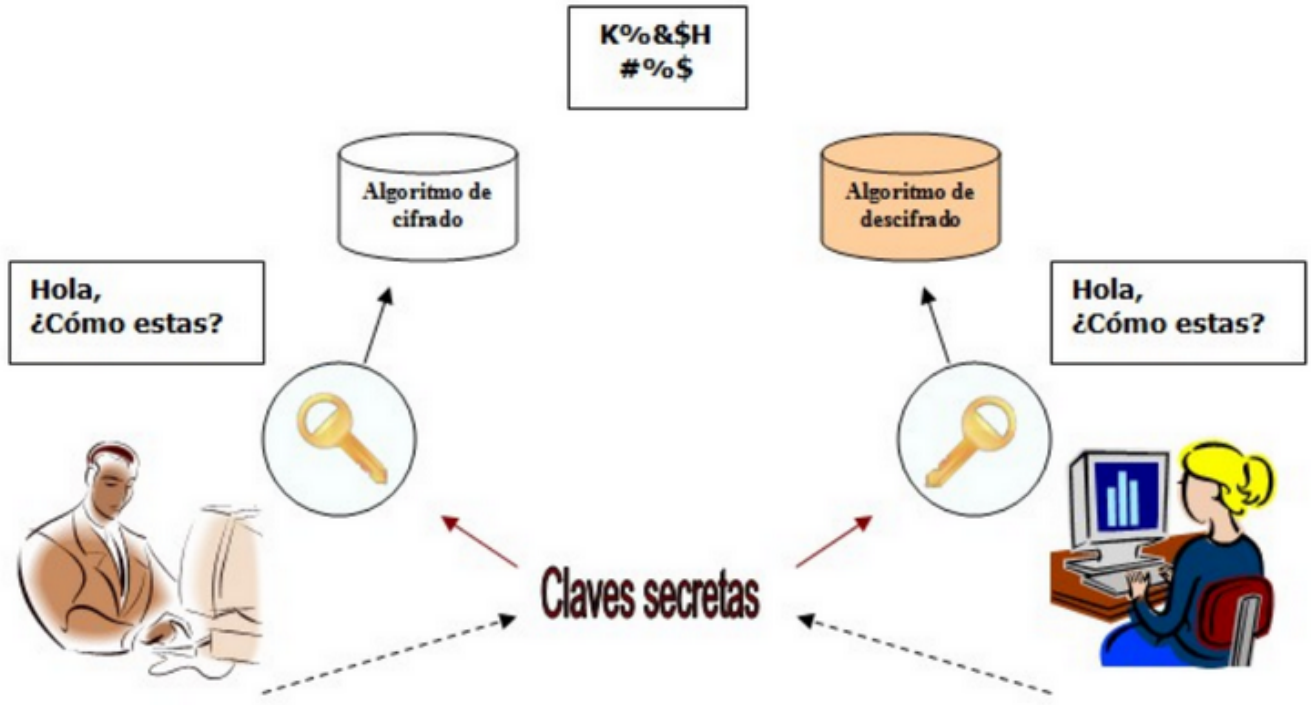
Al hablar de este área se debería hablar de criptologia que a su vez engloba:

- Las técnicas de cifrado (**criptografía**)
- Sus técnicas complementarias donde se incluye el **criptoanalisis** (técnica que estudia los métodos para romper textos cifrados con objeto de recuperar la información original en ausencia de claves).

Criptografía simétrica

La criptografía simétrica usa la misma clave para cifrar y descifrar mensajes.

Dado que toda la seguridad recae en la clave, esta debe ser muy difícil de adivinar, para ello se usa la longitud y el conjunto de caracteres que use.

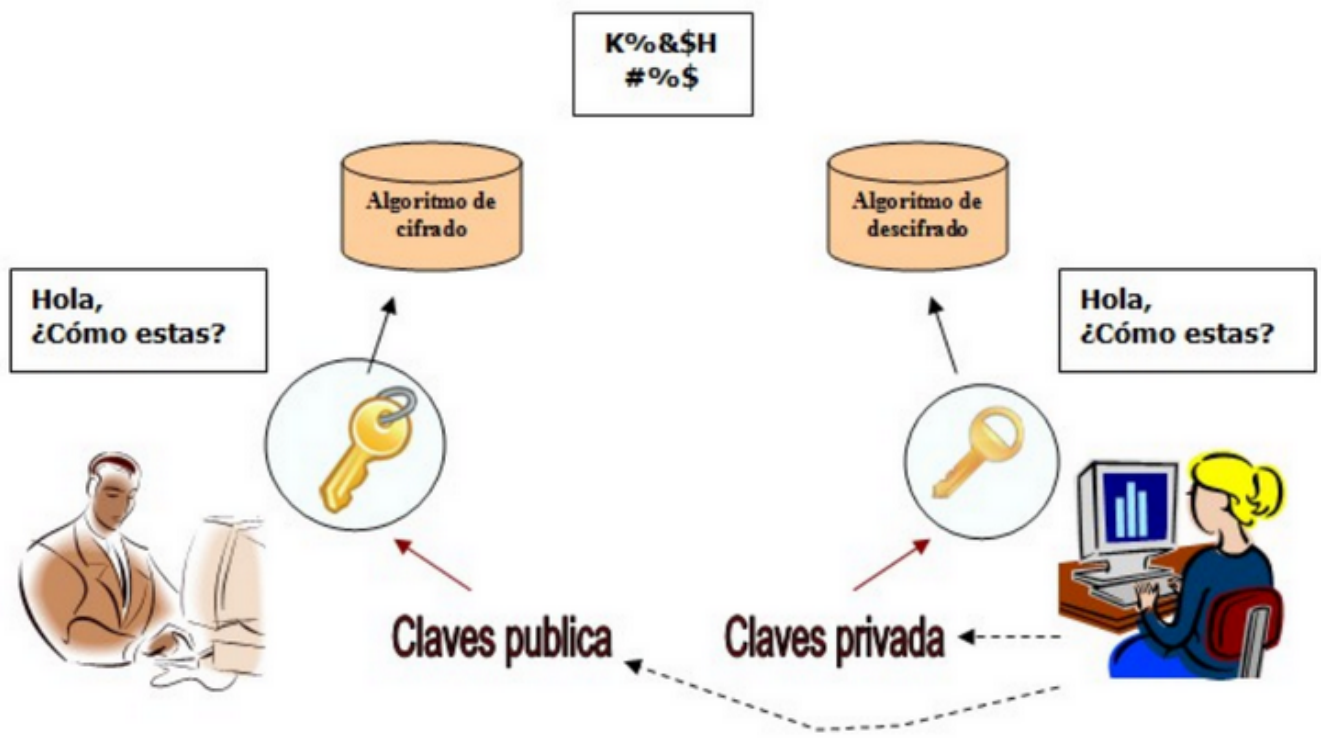


Criptografía asimétrica

Cada usuario del sistema criptográfico ha de poseer una pareja de claves:

- Clave privada: sera custodiada por su propietario y no se dará a conocer a ningún otro.
- Clave publica: sera conocida por todos los usuarios.

Esta pareja de claves es complementaria: lo que cifra una solo lo puede descifrar la otra y viceversa.



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

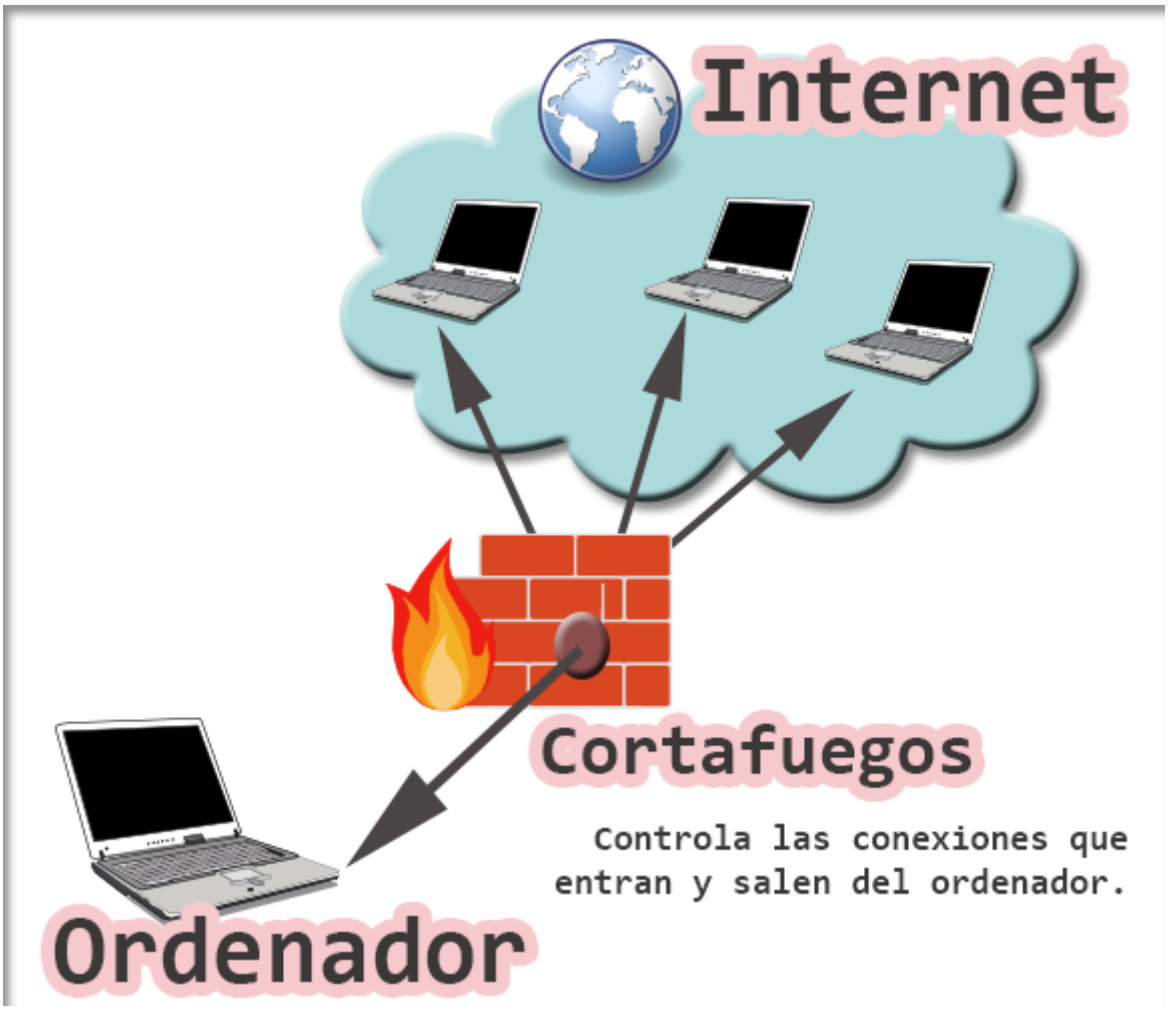
9.3. Borrar archivos de forma segura

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.

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

11.1 Seguridad en Bluetooth

Bluetooth es la palabra que define un estándar global de comunicaciones inalámbricas para **redes de área persona**l y que permite la transmisión de voz y de datos entre diferentes equipos por medio de un enlace por radiofrecuencia en entornos de comunicaciones móviles.

La tecnología Bluetooth tiene un alcance de unos **diez metros**, por lo que se ha integrado en dispositivos de la vida cotidiana que forman parte de las redes personales (PAN) como teléfonos y relojes inteligentes.

Los ciberatacantes que emplean estas comunicaciones suelen utilizar antes que amplían el campo de acción de la señal. Algunos de los ataques son los siguientes:

- **Bluejacking**. Consiste en el envío de spam al usuario por medio del intercambio con este de una vCard, de una nota o de un contacto.
- **Bluesnarfing**. Aprovecha las vulnerabilidades del protocolo para sustraer información del dispositivo atacado.
- **Bluebugging**. Utiliza técnicas de ingeniería social para que la victima acepte una conexión inicial para infectar el dispositivo con malware de control remoto.

A partir de ahí el usuario dispondrá de acceso remoto al teléfono del usuario y podrá utilizar sus funciones.

La adopción de algunas medidas de seguridad sencillas puede evitar los ataques. Por esta razón, deberían de formar parte de la conducta habitual de un usuario de dispositivos Bluetooh.

Algunas de ellas son:

- Activar bluetooh cuando sea necesario realizar algún tipo de comunicación a través de este medio y desactivarlo cuando se deje de utilizar.
- Cambiar el **nombre del dispositivo** para que no desvele datos personales y configurarlo para que permanezca oculto.

- No emparejar ni aceptar conexiones entrantes de **dispositivos desconocidos**, ya que la información podría estar infectada de software malicioso.
- Verificar periódicamente la lista de **dispositivos de confianza** para eliminar los que no se utilizan habitualmente.

11.2 Seguridad en redes wifi

Las redes wifi utilizan una tecnología inalámbrica que realiza la conexión entre dispositivos situados en un área relativamente pequeña, como una habitación, una oficina, una casa o un edificio, a través de ondas electromagnéticas.

Algunas de las medidas de seguridad basicas que se pueden configurar en el router para mantener una red wifi segura son las siguientes:

- **Personalizar la contraseña de acceso:** las contraseñas por defecto de algunos routers suelen ser muy vulnerables o se pueden averiguar rápidamente en Internet.
- **Cambiar el SSID:** el nombre de la red es el identificador con el que se etiqueta la red inalámbrica para que cada usuario pueda localizarla.
- **Revisar el cifrado:** la señal inalámbrica puede ser interceptada más fácilmente por una red cableada, por lo que es necesario utilizar estándares de cifrado como WPA2.
- **Desactivar el acceso por WPS:** el estándar WPS facilita la configuración de una red segura con WPA2 a sus usuarios.
- **Filtrar las MAC:** las direcciones MAC son establecidas por el fabricante y únicas apra cada dispositivo de la red.
- **Actualizar el firmware:** el fimware es el software que controla los circuitos de los dispositivos electrónicos.
- **Comprobar el historial de actividad:** la actividad del router puede desvelar información sobre posibles intrusiones, ya que muestra los datos de los equipos conectados, los horarios, la duración de la sesión, etc...
- **Utilizar software de auditoría:** en el mercado existen herramientas diseñadas para evaluar la seguridad de una red y detectar sus posibles vulnerabilidades. Una de las mas populares es Nmap.