AUTOR: Cuesta Alario David

Seguridad Informática

La seguridad informática es la disciplina que se encarga de proteger la integridad y privacidad de la información almacenada en un sistema informático. Debe tenerse en cuenta que no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema, por lo que para gestionar la seguridad de un sistema informático:

- Debe asegurarse de que los bienes a proteger:
  - Son utilizados como se debe
  - Sólo son accedidos por quien tiene permiso para ello
  - Cumplen la legislación vigente
- Para ello se establecen los siguientes objetivos:
  - Detectar los riesgos y amenazas para evitar que se produzcan o minimizar su efecto
  - Garantizar el uso adecuado de los bienes
  - Limitar las posibles pérdidas y asegurar la recuperación del sistema lo antes posible
  - Cumplir la legislación correspondiente
- Teniendo en cuenta:
  - El valor de los bienes que se van a proteger
  - La probabilidad con la que se puede ver expuesto a determinadas amenazas y el riesgo que ello supone.

En la normativa **ISO 27002:2013** se establecen los estándares para la seguridad de la información

Principios de seguridad CIDAN

Para alcanzar los objetivos es necesario contemplar una serie de servicios o principios de seguridad de la información

- **Confidencialidad:** Se garantiza que la información transmitida o almacenada en un sistema informático sólo podrá ser leída por su legítimo destinatario, por lo que si dicha información cae en manos de terceras personas no podrán acceder al contenido original.
- **Integridad:** Se garantiza desde su creación la información almacenada, procesada o transmitida no ha sido modificada, o en su defecto permite detectar si se ha dañado, añadido o eliminado parte de la información.
- **Disponibilidad:** Mediante un diseño suficientemente robusto frente a ataques e interferencias se garantiza el correcto funcionamiento del sistema informático con la finalidad de que la información esté disponible en todo momento para sus legítimos usuarios y propietarios
- **Autenticidad:** Se puede comprobar la identidad del usuario que crea o accede a la información o a intenta acceder a una red o servicio.
- **No repudio:** Se demuestra la autoría de la información mediante un mecanismo que impida que el usuario que la ha creado y enviado pueda negar dicha circunstancia. Se aplica la misma situación al destinatario de la información

Derivados de los anteriores podemos definir otros principios de seguridad (pueden entrar en conflicto con los anteriores)

- **Autorización:** Permite controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos por el sistema.
- **Audibilidad:** Permite monitorizar el uso de los recursos del sistema por parte de los usuarios autorizados
- **Reclamación de origen:** Permite probar quién ha sido el creador de determinada información
- **Reclamación de propiedad:** Permite probar que un determinado documento o un contenido digital protegido por derechos de autor pertenece a un determinado usuario u organización que ostenta la titularidad de esos derechos
- **Anonimato:** Garantiza que la identidad de los usuarios que acceden a determinados recursos o servicios queda oculta
- **Protección a la réplica:** Impide la realización de “ataques de repetición” consistentes en la interceptación y posterior reenvío de mensajes para tratar de engañar al sistema y provocar operaciones no deseadas.
- **Confirmación:** Permite confirmar la realización de una operación reflejando los usuarios que han intervenido
- **Referencia temporal:** Permite garantizar la autenticación de las partes que intervienen así como el contenido e integridad de los mensajes y la constatación de la realización de una operación o comunicación en un determinado instante

AUTOR: Cuesta Alario David

Copias de seguridad

Consiste en duplicar la información como medida preventiva para poder recuperarla lo antes posible ante posibles pérdidas

Las copias de seguridad pueden tener las siguientes funciones:

- Recuperar la información perdida
- Tener un histórico de la evolución de la información
- Auditorías
- Informática forense

Tipos de copias de seguridad

Completa: Se realiza una copia de todos los datos de modo que la Información estará duplicada.

- Adecuado cuando la información sufre muchas modificaciones
- inadecuado cuando la cantidad de información es muy grande
- Para restaurar la información es suficiente con restaurar la última copia completa.

Progresiva: Se realiza una copia de todos los datos modificados desde la última copia completa o progresiva

- Puede ser muy rápida
- Optimiza el espacio
- Para restaurar la información se restaura la última copia completa y posteriormente se restauran una a una todas las copias progresivas siguiendo el orden

Diferencial: Se realiza una copia de todos los datos modificados desde la última copia completa

- Necesita menos espacio que una copia completa, pero más que una progresiva
- El sistema de recuperación de la información es más sencillo.
- Para restaurar la información se restaura la última copia completa y posteriormente se restaura la última copia diferencial.

Planificación del sistema

Para el correcto funcionamiento de una copia de seguridad hay establecer:

- Qué datos se van a copiar
  - Aquellos que son únicos
  - Aquellos que se modifican constantemente
- Dónde se van a almacenar las copias
- Cada cuánto tiempo se van a actualizar
- Establecer un mecanismo de recuperación que permita restablecer la información
- Establecer un plan de protección para la información copiad

AUTOR: **Cuesta Alario David**

Cifrado de la información

Estenografía

Trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos dentro de otros, de modo que no se perciba su existencia. De esta forma se puede establecer un canal encubierto de comunicación que pase inadvertido ante aquellos observadores que tienen acceso a ese canal

La estenografía clásica se basaba únicamente en el desconocimiento del canal encubierto utilizado, mientras que en la era moderna también se emplean canales digitales (imagen, video, audio y protocolos de comunicaciones) para alcanzar el objetivo. En muchos casos, el objeto contenedor es conocido, y lo que se ignora es el algoritmo de inserción de la información en dicho objeto.

Criptografía

Trata el estudio y aplicación de los algoritmos, protocolos y sistemas que permiten ocultar la información de un mensaje mediante un código que permite alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. De esta forma se consigue proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican independientemente de quien acceda al canal e intercepte los mensajes.

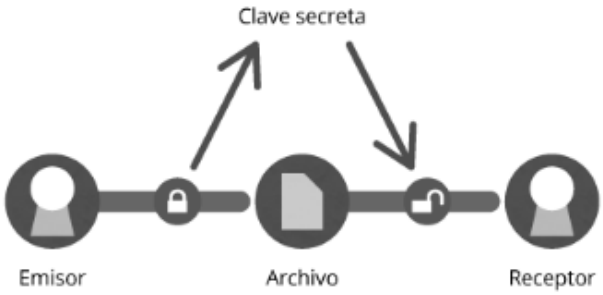
Los grandes avances producidos en el mundo de la criptografía se basan en técnicas matemáticas han sido posibles gracias a la evolución que se han producido en el campo de la matemática y la informática.

Sistemas simétricos

Se trata de un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor.

Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. A continuación el remitente cifra el mensaje usando la clave y lo envía al destinatario. Finalmente el destinatario puede descifrar dicho mensaje utilizando la misma clave con la que se cifro originalmente

Este sistema requiere que ambas partes tengan acceso a la clave lo que genera un problema de seguridad al transmitirla



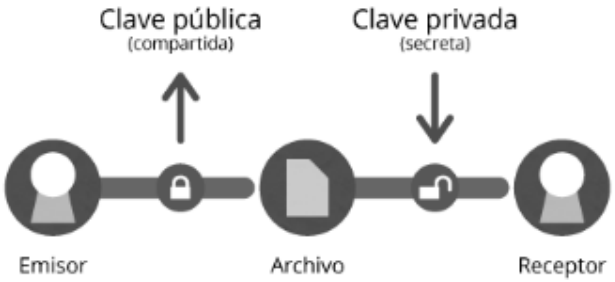
Sistemas asimétricos

Se trata de un método criptográfico basado en el uso de dos claves:

- Una clave pública que será difundida públicamente a todas las personas que necesiten mandar un mensaje cifrado
- Una clave privada que solo será conocida por el receptor del mensaje

De este modo el receptor comunica su clave pública al emisor por un canal que no tiene por qué ser seguro. A continuación el emisor cifra el mensaje utilizando dicha clave pública y lo envía al destinatario. Finalmente el receptor descifra el mensaje utilizando su clave privada.

En este sistema las claves se generan por pares, de modo que todo lo que una clave cifre solo su pareja lo puede descifrar.



Ventajas

- Sólo el destinatario puede leer el mensaje
- Sólo hay que almacenar una clave
- Cualquiera puede cifrar con la clave pública
- No son necesarios canales seguros para comunicar la clave

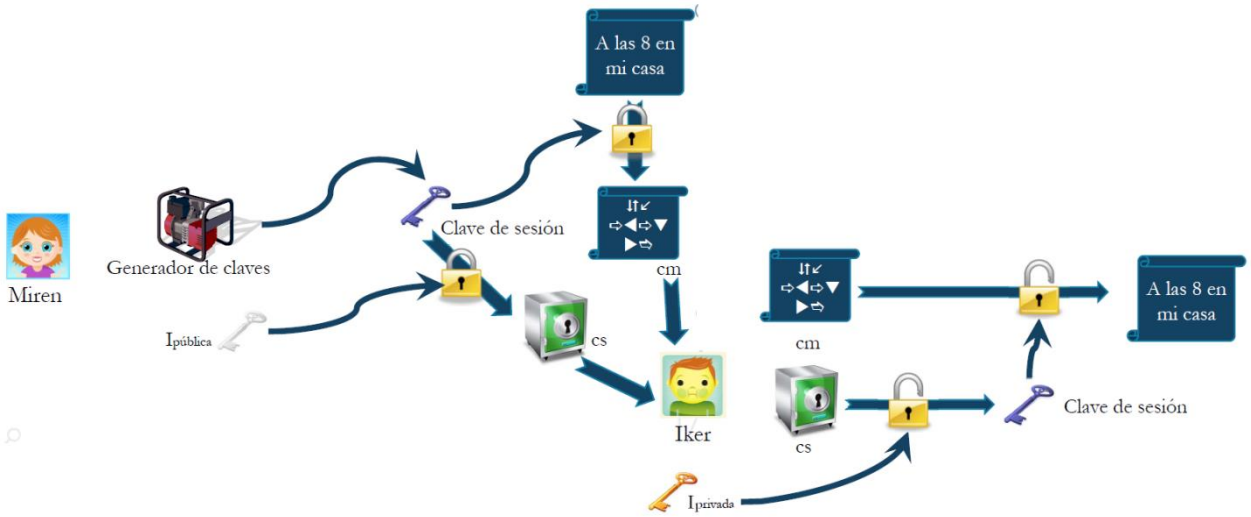
Desventajas

- El cifrado y descifrado son más lentos que en los sistemas de clave única
- Debemos certificar la autenticidad de la clave pública del destinatario para evitar suplantaciones de identidad
- No debería ser posible obtener la clave privada a partir de la clave publica
- Un mensaje cifrado con la clave privada lo podría descifrar cualquiera

AUTOR: Cuesta Alario David

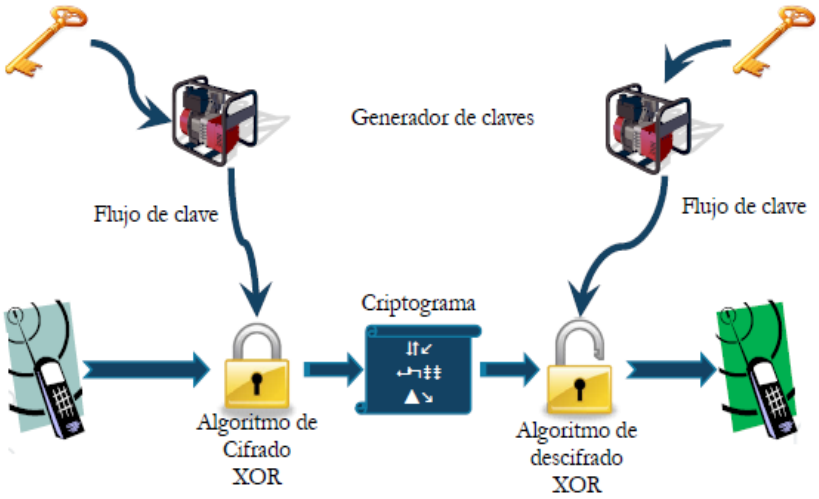
Sistemas híbridos

Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando su propia clave privada, luego el mensaje cifrado se envía al destinatario. Ya que compartir una clave simétrica no es seguro, ésta es diferente para cada sesión.



Cifrado de flujo

Para aquellas aplicaciones en las que se requiera un intercambio de información a tiempo real el cifrado en bloques es inapropiado. Para estas aplicaciones se emplea un algoritmo que permiten realizar el cifrado bit a bit de forma incremental mediante una secuencia de bits de tamaño arbitrario empleados para oscurecer el contenido de un flujo de datos combinando el flujo de clave con el flujo de datos mediante la función XOR.



Se puede construir un generador de flujo de clave iterando una función matemática sobre un rango de valores de entrada para producir un flujo continuo de valores de salida. Los valores de salida se concatenan para construir bloques de texto en claro, y los bloques se cifran empleando una clave compartida por el emisor y el receptor.

- Si el flujo de clave es seguro, el flujo de datos cifrados también lo será.
- Para conservar la calidad de servicio del flujo de datos
  - Los bloques del flujo de clave deberían producirse con un poco de antelación
  - El proceso que los produce no debiera exigir demasiado esfuerzo de procesamiento

Método de Vernam

- El flujo de clave es de un solo uso
- Hay que enviar la clave al receptor del mensaje
- Está demostrado matemáticamente que es irrompible
- No es practico

Métodos con claves pseudoaleatorias

- Emplea claves pseudoaleatorias generadas a partir de una semilla y un algoritmo de generación
- Se podría reconstruir la clave conociendo la semilla y el algoritmo de generación pseudoaleatorio
- **Ejemplos:** RC4 (ARC4) usado en TLS/SSL WEP y WPA A5/1 usado en comunicaciones GSM

Métodos de cifrado por bloques

- Consiste en partir el mensaje original en bloques de tamaño fijo lo suficientemente pequeños. De este modo, se genera un bloque de mensaje cifrado por cada bloque del mensaje original con la posibilidad de añadir iteraciones, permutaciones y operaciones entre los distintos bloques
- **Ejemplos:** DES y Triple DES (empleando tres veces el algoritmo DES con dos o tres claves distintas)
  IDEA KASUMI AES 4G

AUTOR: Cuesta Alario David

Claves débiles

Según las características del algoritmo algunas claves pueden mostrar las siguientes debilidades:

- Al encriptar un mensaje resulte un mensaje muy parecido al mensaje original $E_{Clave}(M_{ensaje}) = M_{ensaje}$
- Al encriptar un mensaje dos veces con el mismo algoritmo resulte el original $E_{Clave}(E_{Clave}(M_{ensaje})) = M_{ensaje}$
- Que exista más de una clave capaz de descifrar el mensaje $D_{Clave\,2}(E_{Clave\,1}(M_{ensaje})) = M_{ensaje}$

En un buen criptosistema el número de claves débiles y semidébiles es cercano a cero

Conviene conocer las claves débiles de un criptosistema para evitar su uso

Criptografía Cuántica

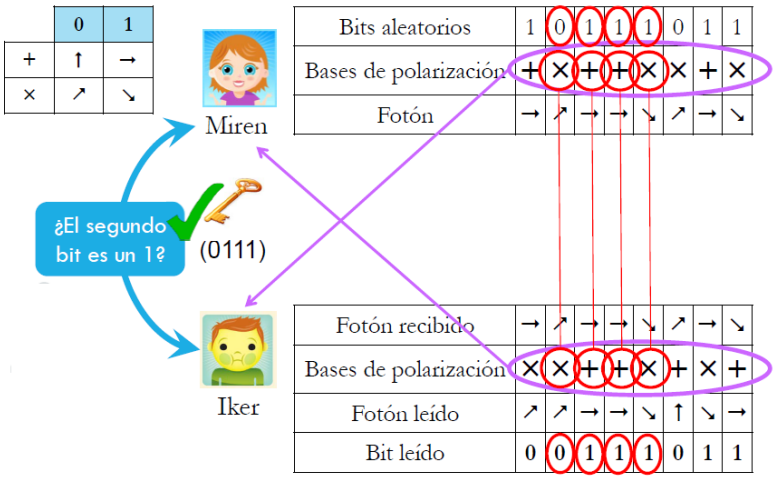
Se basa en los principios de mecánica cuántica para garantizar la absoluta confidencialidad de la información transmitida

Se usa fotones polarizados con las siguientes características:

- Una partícula puede tener varios estados a la vez dado que se utilizan bases de polarización
- La medición altera el sistema por lo que si un tercero intenta espiar durante la creación de la clave secreta, el proceso se altera advirtiéndose al intruso antes de que se transmita información privada
- Necesita un canal cuántico (por ejemplo, fibra óptica) para enviar la información

Protocolo BB84

- El emisor codifica los fotones y las bases de polarización, a continuación genera una cadena binaria aleatoria para polarizar cada fotón y manda los fotones polarizados al destinatario.
- El remisor y el receptor intercambian las bases de polarización por un canal publico
- Los fotones de las bases que coincidan especifican la clave
- Para asegurar que los bits que usan ambos son los mismos (que no hubo espías) se intercambian ciertos bits de la clave



La seguridad de la criptografía cuántica descansa en las bases de la mecánica cuántica, a diferencia de la criptografía de clave pública tradicional la cual descansa en supuestos de complejidad computacional no demostrada de ciertas funciones matemáticas.

Criptoanálisis

Trata el estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas que permitan romper su seguridad sin el conocimiento de información secreta. (Obteniendo la clave a partir de uno o varios mensajes encriptados)

Los métodos y técnicas del criptoanálisis han cambiado drásticamente a través de la historia de la criptografía, adaptándose a una creciente complejidad criptográfica. El criptoanálisis clásico se basaba en métodos estadísticos y lógicos mientras que los métodos actuales implican resolver un problema cuidadosamente construido en el dominio de la matemática pura tales como la factorización de enteros

Ataques por fuerza bruta

Se trata de un tipo de ataques que consiste en probar todas las claves posibles, por lo que siempre encuentra la solución.

- Este tipo de ataques no siempre es posible debido al coste temporal que implica
- Hay que conocer el algoritmo de cifrado y el espacio de claves

Se puede hacer un ataque por fuerza menos bruta y más inteligente probando primero los patrones más típicos en las claves o conociendo información personal del objetivo

AUTOR: Cuesta Alario David

Algoritmos de resumen Funciones hash

Son funciones de dispersión que generan un criptograma de un tamaño determinado que representa todo el contenido original de un mensaje.

Se caracteriza porque no se puede invertir el proceso

- Es imposible obtener el mensaje original partiendo del criptograma, ni siquiera por fuerza bruta dado que al no tratarse de un sistema de encriptación no existe una clave que descifrar

Integridad de contenidos

Cuando se quiere almacenar o transmitir información protegida frente a errores fortuitos en el almacenamiento o transmisión se suele acompañar el mensaje con los valores obtenidos a partir de una función hash con ciertas propiedades. A este dato se le denomina checksum (suma de verificación) y se emplea para comparar su valor con el obtenido al aplicar la misma función hash al mensaje recibido en la maquina destinataria, de este modo si los valores no coinciden implica que ha habido una alteración con respecto al mensaje original

Verificación de la información

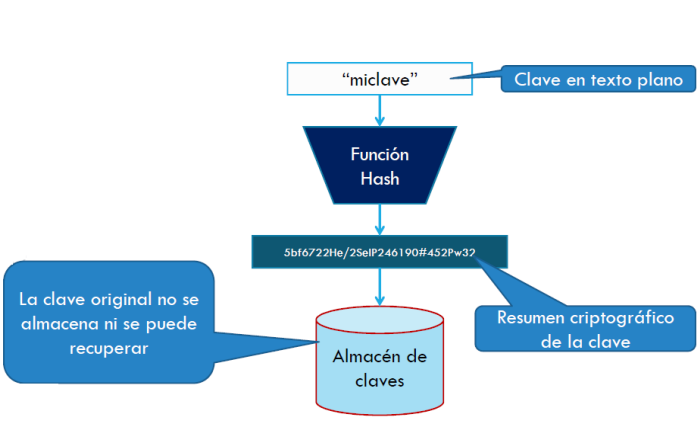
Cuando se quiere estar seguro de que el mensaje que le llega al receptor es el mismo que se está emitiendo, se proporciona un valor resumen del contenido de forma que ese valor tiene que obtenerse al aplicar la función resumen sobre el contenido distribuido asegurando así la integridad.

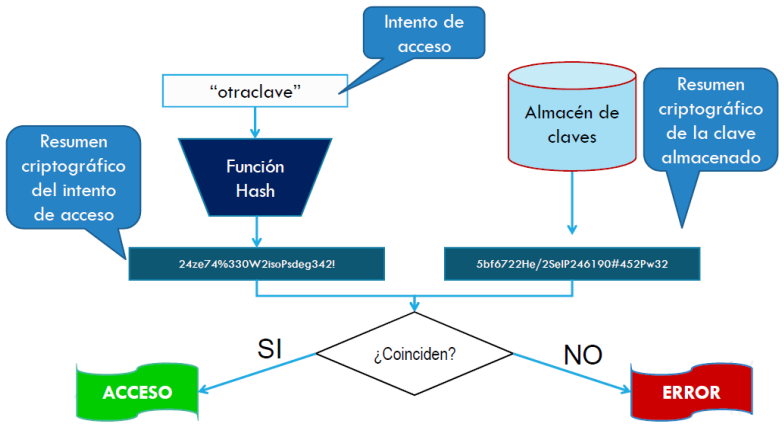
A esto se le suele llamar checksum criptográfico debido a que es un checksum que requiere el uso
de funciones resumen criptográfico para que sea difícil generar otros ficheros falsos que tengan el mismo valor resumen.

Registro e identificación seguros

Se pueden usar funciones hash para proporcionar una identificación de objetos o situaciones

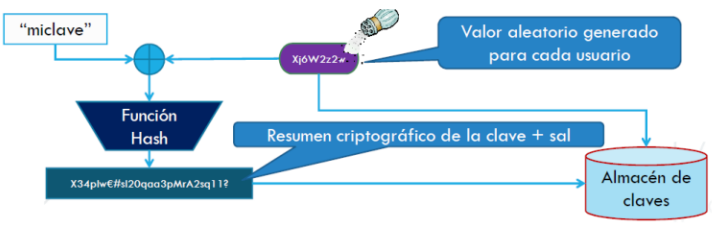
- La evaluación de la función hash debería ser poco costosa para facilitar la rápida comparación de elementos candidatos a ser iguales y de esta forma poder implementar algoritmos de búsqueda rápidos.
- Es labor del diseño de la función hash capturar la esencia del criterio de igualdad. Una buena función hash debe asegurarse de que dos objetos o situaciones que se considerar iguales den lugar al mismo valor hash. No obstante dos objetos pueden ser considerados iguales sin ser idénticos.

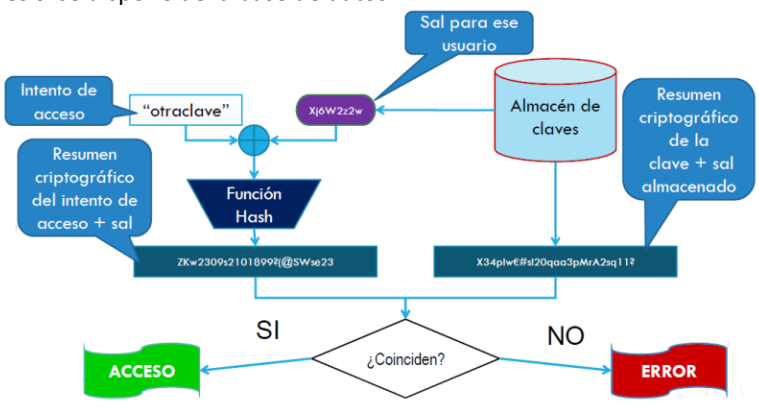




Problemas

- Todo el mundo con la misma clave tiene el mismo hash
- Se pueden precalcular los hash de todo el espacio de claves si se dispone de la base de datos





Ventajas del uso de sal

- La misma clave tiene una codificación distinta cada vez
- Dificulta los ataques por fuerza bruta
- Tener disponible la base de datos las claves y la sal no aporta nada dado que no puedes saber a cual pertenece cada uno

AUTOR: Cuesta Alario David

Identificar cadenas o subcadenas de archivos

Las funciones hash obtienen valores que permiten detectar características intrínsecas del contenido multimedia, de forma que se pueda identificar si dos archivos diferentes se corresponden con el mismo contenido multimedia independientemente de su nombre o ubicación de una forma sencilla y rápida.

Se utiliza como herramienta para la identificación y la rápida comparación de datos

- Detección de virus
- Autenticación con datos biométricos
- Detección de copias
- búsqueda de subcadenas dentro de otra cadena para la detección de copias

La firma digital

Un certificado digital consiste en que una entidad de confianza que firma mediante su clave privada la clave pública de un usuario

- Sirve para certificar que el usuario es quien dice ser
- Depende de la confianza en la entidad que lo certifica

Las funciones hash permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje (autenticación de origen y no repudio) y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originado dado que las firmas digitales permiten que:

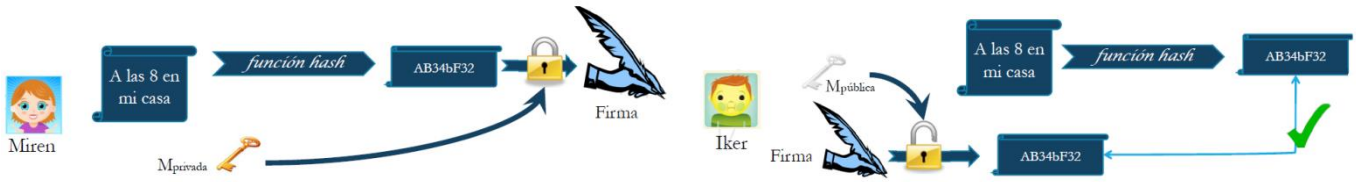
- Sólo el usuario legítimo puede firmar su documento
- Nadie podrá falsificar una firma
- Cualquiera puede verificar una firma digital
- Una copia de una firma digital es igual a la original
- No se puede reutilizar una firma
- No se puede modificar una firma
- No se puede negar haber firmado un documento
- No se puede alterar un documento después de haberlo firmado

Para firmar un mensaje:

- Se realiza el resumen criptográfico del mensaje
- Se cifra el resumen criptográfico con la clave privada del emisor
- Se cifra el mensaje y la firma con la clave pública del destinatario

Para verificar la autenticidad de la firma

- Se descripta la firma mediante la clave pública del emisor
- Se comprueba que el resumen criptográfico firmado coincide con el del mensaje



Con la firma digital se puede comprobar si el mensaje original ha sido modificado dado que nadie más que el emisor podría volver a firmar el resumen criptográfico de un documento modificado sin conocer la clave privada del emisor original

Confianza de firmas

El tercero de confianza es un organismo que se encarga de certificar la realización y el contenido de las operaciones y de avalar la identidad de los intervinientes, dotando a éstas de una mayor seguridad jurídica

Un usuario certifica (firmando con su clave privada) que la clave pública de otro usuario es de confianza

- **Validez**: cumple los requisitos de una firma (caducidad, etc.)
- **Confianza**: nos podemos fiar de esa firma

La confianza se propaga según la confianza que demos a los usuarios que firmen las claves:

- **Desconocido**: no nos fiamos de nada que firme ese usuario (por desconocimiento)
- **Ninguno**: no nos fiamos de nada que firme ese usuario (porque sabemos que lo hace mal)
- **Marginal**: nos fiamos de las claves firmadas por dos usuarios con confianza marginal
- **Absoluto**: nos fiamos de todo lo firmado por ese usuario

Una autoridad de certificación

- certifica la validez de una firma
- Debe mantener una base de datos de nombres distinguidos y de Autoridades de certificación subordinadas
- Debe permitir la revocación de certificados cuando estos se ven comprometidos o dejan de ser validos

El protocolo OCSP

- permite validar el estado de un certificado digital de manera online
- Es más eficiente que la verificación mediante Listas de Revocación de Certificados debido a su actualización constante

AUTOR: Cuesta Alario David

Software Maligno (Malware)

Se trata de un programa informático que tiene como objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático sin el permiso o el conocimiento del usuario con la finalidad de:

- Causar algún problema en el equipo en el que se encuentra instalado
  - Cambiar configuraciones
  - Eliminar archivos
  - Producir errores
- Acceder a cualquier información almacenada
  - Robar información
  - Espiar el comportamiento del usuario
  - Abrir la computadora a nuevos ataques

Clasificación

Para clasificar los distintos tipos de Malware suelen usar palabras genéricas que describen su comportamiento principal sin prestar atención a sus características. Esto se debe a que un mismo Malware puede tener más de un comportamiento agrupando características de varias clases. Como consecuencia los distintos tipos de malware no siempre están perfectamente diferenciados

Virus

Su principal característica es su capacidad para duplicarse y diseminarse haciendo copias de sí mismo tanto en el equipo infectado como en otros equipos

No obstante, la mayoría de los virus suelen llevar asociadas acciones dañinas a las que se le denominan payload. Estas pueden estar comprendidas desde una simple broma que produce molestias hasta destruir información mediante la modificación o eliminación de ficheros o bloquear las redes informáticas generando tráfico inútil

El funcionamiento de un virus informático es conceptualmente simple.

- Tras la ejecución de un programa que estuviera infectado el código del virus queda alojado en la memoria RAM de la computadora, incluso cuando el programa que lo contenía haya terminado de ejecutar.
- A continuación, el virus toma el control de los servicios básicos del sistema operativo con la finalidad se añadir su propio código en los archivos ejecutables que sean llamados para su ejecución con lo cual se completa el proceso de replicación.

Gusanos

Su principal característica es su capacidad para duplicarse y diseminarse haciendo copias de sí mismo tanto en el equipo infectado como en otros equipos

Los gusanos utilizan las partes automáticas de un sistema operativo para aprovechar las vulnerabilidades de una red de computadoras con la finalidad de realizar las mismas acciones que los virus pero sin la necesidad de la intervención del usuario:

- Se transmite a sí mismo con la finalidad de propagarse
- Puede contener instrucciones dañinas

Troyano

Su principal característica es que se presentan a sí mismos con una apariencia inofensiva pero que realmente tiene una funcionalidad oculta que puede ser de un ámbito muy diverso

Habitualmente se encuentran ocultos entre el código de una aplicación real que realiza su función correctamente con la finalidad de no levantar sospechas mientras el Troyano realiza sus funciones en segundo plano.

No tienen la capacidad para infectar otros ficheros u equipos por lo que para infectarse es necesario utilizar la aplicación en la cual se ocultan.

Bombas lógicas

Su principal característica es su capacidad para permanecer oculto en estado latente en el ordenador infectado hasta que se produce la circunstancia con la que estaba programado para activarse y entonces realizar su función que puede ser de un ámbito muy diverso.

Puertas traseras (BackDoors)

Su principal característica es su capacidad para permitir el acceso al sistema infectado a un usuario no autorizado eludiendo los procedimientos habituales de autenticación mediante una secuencia especial dentro del código de programación

Su principal finalidad es el espionaje y el robo de datos

Exploit

Se trata de un conjunto de instrucciones que permiten aprovechar una vulnerabilidad de seguridad de un sistema de información con la finalidad de conseguir un comportamiento no deseado del mismo, que puede ser de un ámbito muy diverso.

Spyware

Su principal característica es su capacidad para recopilar información de forma automática acerca del sistema infectado y transmitirla a una entidad externa sin el conocimiento o el consentimiento del propietario.

La información robada puede ser relativa al funcionamiento de algún programa informático concreto o al sistema operativo en general con la finalidad de obtener retroalimentación acerca de su funcionamiento. O bien puede ser de ámbito personal como por ejemplo contraseñas o archivos confidenciales, de forma que el autor pueda obtener un beneficio económico o de otro tipo a través de su uso o distribución.

Keylogger

Tiene la capacidad de monitorizar y capturar las teclas pulsadas por el usuario y las almacenan para un posterior envío al creador. Su principal finalidad es recopilar contraseñas de acceso pero también pueden ser usados para espiar conversaciones de chat

Stealers

Tiene la capacidad de robar información privada que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados en el equipo y si tienen contraseñas recordadas descifran esa información y la envían al creador.

Adware

Su principal característica es su capacidad para mostrar al usuario publicidad no solicitada de forma intrusiva bien mediante ventanas emergentes o redirigiendo solicitudes de páginas web.

Algunos programas shareware permiten usar el programa de forma gratuita a cambio de mostrar publicidad. En este caso el usuario consiente la publicidad al instalar el programa por lo que no debería ser considerado malware. No obstante, en muchas ocasiones los términos de uso no son completamente transparentes y ocultan lo que el programa realmente hace.

Hijackers

Tienen la capacidad de realizar cambios en la configuración del navegador web con la finalidad de conseguir, por ejemplo, cambiar la página de inicio del navegador por páginas web de publicidad.

Pharming

Es una técnica que suplanta el DNS modificando el archivo hosts para redirigir el dominio de una o varias páginas web a otra página web de otra máquina distinta. Estas páginas pueden ser de publicidad o bien una web falsa que imita a la verdadera

Como consecuencia, esta técnica puede ser utilizada con el objetivo de obtener las credenciales y datos personales mediante el secuestro de una sesión. Debido a que el usuario no sospecha que la página web no es la real, este introduce sus credenciales que son reenviadas a una entidad externa sin el conocimiento o el consentimiento del propietario

Scareware

Su finalidad es asustar al usuario infectado causando la percepción de una amenaza para hacerlo vulnerable a un ataque de ingeniería social de forma que se le pueda estafar para obtener información sensible o alguna retribución económica

Esta técnica esta generalmente dirigida a usuarios confiados y nada suspicaces.

Es muy frecuente combinarlos con Spyware y Adware

Rogue software

Implica convencer a los usuarios que un virus ha infectado su computador y después sugerir que paguen y descarguen un software antivirus para quitarlo. Usualmente el virus es enteramente ficticio y el software es o bien totalmente inútil o un malware funcional.

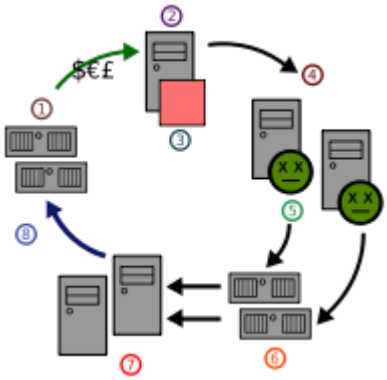
Dialers

Son programas malignos que toman el control del módem para realizar llamadas a un número de teléfono de tarificación especial y dejan la línea abierta cargando el coste de dicha llamada al usuario infectado.

Hoy en día los Dialers ya no son tan populares debido a que sus efectos sólo se muestran en usuarios con acceso a la Red Telefónica Básica y actualmente la mayoría de las conexiones a Internet son mediante ADSL y no mediante módem

AUTOR: Cuesta Alario David

Botnets



Se trata de un conjunto de redes de computadoras infectadas (habitualmente denominadas Zombis) que pueden ser controladas a la vez por el artífice del malware con la finalidad de realizar distintas tareas entre las que se pueden encontrar:

- El envío masivo de spam
- Lanzar ataques contra organizaciones
  - Como forma de extorsión
  - Para impedir su correcto funcionamiento.
- **Coinminer**: Usa la potencia del equipo para minar criptomonedas sin conocimiento del usuario

La principal ventaja que ofrece el uso de ordenadores infectados es el anonimato

En una Botnet cada computadora infectada por el malware se loguea en un canal de chat desde donde el atacante puede dar instrucciones a todos los sistemas infectados simultáneamente.

También permite mantener actualizado el malware en los sistemas infectados para hacerlos resistentes ante los antivirus

Ransomware

También llamados criptovirus o secuestradores son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un rescate para poder recibir la contraseña que permite recuperar los archivos.

rootkits

Fases de un virus

Llegada al sistema desde el exterior

- Intencionadamente
- Involuntariamente

Instalación: Se produce al ejecutar el código del virus por primera vez

- **Añadidura**: el código del virus se añade al final del archivo a infectar.
  - El tamaño del archivo infectado crece
- **Inserción**: el código del virus se reparte en huecos "libres" dentro del código del archivo infectado.
  - El tamaño del archivo infectado no varía.
  - Su creación no es trivial
- **Reorientación**: Una pequeña parte del código del virus se instala en el archivo a infectar mientras que el resto está distribuido por el sistema. Al ejecutarse el virus se recompone y cumple su función.
- **Sustitución**: El virus sustituye directamente el código del archivo a infectar

Activación y control del sistema

- **Acción directa**: Se ejecuta el virus cada vez que se ejecute el fichero infectado
- **Acción indirecta**: el virus está residente en memoria y se ejecuta de manera regular

Ocultamiento ante los ojos del usuario y del antivirus con la finalidad de pasar inadvertido

- **Dispersión**: el virus se divide y oculta sus partes
  - Marca los ficheros como ocultos
  - Se almacena en sectores libres del disco y los marca como defectuosos
  - Se almacena en formatos que el sistema operativo no es capaz de leer
- **Compresión**: el virus comprime el programa infectado y se instala en el sitio que queda libre para no modificar su tamaño
- **Camuflaje**: El virus engaña al sistema operativo y al antivirus cuando comprueban los atributos de los ficheros modificando las propiedades como el tamaño o la fecha de modificación entre otros
- **Sobrepasamiento**: El virus actúa directamente sobre las rutinas de los servicios del sistema, engañando al antivirus que comprueba los servicios del sistema
- **Autocifrado**: El virus se encripta y desencripta según lo necesite usando una clave distinta en cada ocasión. De este modo, el antivirus no puede acceder al contenido del virus y detectarlo
- **Polimorfismo**: El virus cambia de forma e incluso de comportamiento cada vez que se propaga
- **Blindaje**: Evita que el virus pueda ser desensamblado para que no se pueda acceder a su código y programar un antivirus para detectarlo

Reproducción consiste en crear copias del virus en otros ficheros

- Búsqueda de huéspedes
- Comprobación de que los huéspedes no han sido previamente infectados
- Recomposición del virus
- Copia en el programa huésped

Manifestación El virus lleva a cabo las acciones para las que ha sido diseñado

Nomenclatura

Prefijo / **Nombre** . **Variante** @ **Sufijo**

El **prefijo** identifica el sub-sistema objetivo al que afecta detecta el malware.

No es una parte obligatoria y puede no estar presente.

W32 ⟶ Windows 32bit

W95 ⟶ Windows 9X/Me

WM ⟶ Virus de macro de Word

XM ⟶ Virus de macro de Excel

El **nombre** es la denominación oficial que se le da al malware detectado y que se extiende a toda su familia

La **variante** indica la versión del malware detectado. Puede estar indicada por un número o una letra empezando por a hasta z y siguiendo por aa hasta zz y así sucesivamente

El **sufijo** indica el tipo de Malware del que se trata

Worm ⟶ Gusano

MM ⟶ Gusano de propagación por correo electrónico

Troj ⟶ Troyano

Bck ⟶ BackDoor

VBS ⟶ Programado en Visual Basic Script

JS ⟶ Programado en Java Script

Joke ⟶ Broma

Estadísticas

Observando la frecuencia y el tipo de malware utilizado en los ataques informáticos de años anteriores podemos observar cierto patrón con el que establecemos los siguientes criterios:

- Las plataformas más utilizadas sufren más ataques informáticos debido a que existe una mayor cantidad de objetivos, lo que aumenta la probabilidad de infectar a nuevos usuarios
- Las aplicaciones de código abierto son más fáciles de atacar dado que no es necesario llevar a cabo un proceso de ingeniería inversa para buscar fallos
- Los sistemas operativos que permiten que las compañías distribuidoras cambien partes del código para obtener una mayor diferenciación con respecto a otras distribuidoras son más fáciles de atacar debido a existe una alta probabilidad de generar nuevas vulnerabilidades al realizar dichas modificaciones
- Los sistemas operativos poco restrictivos con respecto al origen y autor de las aplicaciones permitidas son más propensos a recibir ataques. (Google Play, cualquiera puede subir una aplicación)

Virus Vs Gusanos

Teniendo en cuenta esta distinción, las infecciones transmitidas por correo electrónico o documentos de Microsoft Word deberían ser clasificadas más como virus que como gusanos debido a que dependen de su apertura por parte del destinatario para infectar su sistema.

AUTOR: Cuesta Alario David

Técnicas anti Malware

Origen de las infecciones

Las principales formas en las que se puede infectar un equipo informático mediante la entrada del malware son:

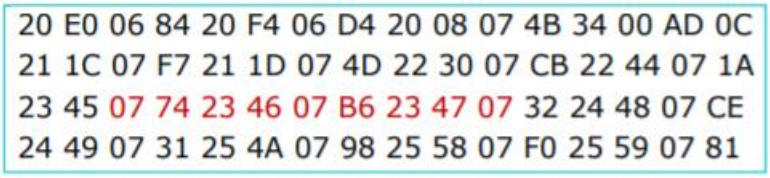
- Mediante Agujeros de seguridad del sistema operativo o los programas instalados
- Mediante la ejecución de correos electrónicos, ficheros o ejecutables infectados con virus
- Mediante la instalación de software poco confiable que pueda portar troyanos o BackDoors
- Una configuración débil de nuestro sistema operativo o las aplicaciones de internet

Las aplicaciones más sensibles al Malware son

- Aplicaciones de cliente de correo electrónico
- Aplicaciones de escritorio
- Aplicaciones de mensajería instantánea
- Navegadores web
- Aplicaciones P2P como eMule o Torrent

Técnicas de detección

Detección por cadena o firma



Se analiza el código binario del virus buscando una cadena representativa que lo diferencie de cualquier otro programa. Cuando el antivirus detecta esa cadena determina que hay infección.

- Es la técnica más extendida entre los antivirus debido a que:
  - Permite identificar cualquier él malware de forma concreta e univoca
  - Su coste computacional es muy reducido
- Esta técnica puede no ser eficaz ante malware que utilice determinadas técnicas de ocultación como la encriptación o la compresión
- Es una técnica reactiva:
  - No detecta nuevos virus ni modificaciones del mismo por lo que requiere actualización continua

Detección por localización y nombre de archivo

Se analizan aquellos directorios en los que el malware reconocido suele generar archivos concretos. Cuando el antivirus detecta uno de esos ficheros determina que hay infección.

- Es una técnica reactiva:
  - No detecta nuevos virus ni modificaciones del mismo por lo que requiere actualización continua
- No todos los malware generan ficheros, y los que lo hacen no siempre utilizan la misma ubicación o la misma nomenclatura

Detección heurística

Se analiza el código de todos los archivos que se ejecutan con la finalidad de buscar conjuntos de instrucciones y comportamientos habituales del malware

- Tiene una mayor capacidad para detectar malware nuevo por lo que no necesita de actualizaciones tan constantes. No obstante, no podrá detectar malware con características nuevas
- Tiene un alto coste computacional que penalizara el rendimiento durante los análisis
- Es muy propenso a falsos positivos
  - **Por ejemplo** detectar como malware un programa legítimo que tiene una funcionalidad de borrar los archivos con más de un año de antigüedad.

Detección por comportamiento

Se comprueban todas las acciones que intentan llevar a cabo las aplicaciones y se identifican aquellas que puedan ser potencialmente peligrosas debido a que son comportamientos habituales del malware

- Tiene una mayor capacidad para detectar malware nuevo por lo que no necesita de actualizaciones tan constantes. No obstante, no podrá detectar malware con características nuevas
- Tiene un alto coste computacional que penalizara el rendimiento durante la ejecución de las aplicaciones
- Es muy propenso a falsos positivos
  - **Por ejemplo** detectar como malware un programa legítimo que intenta eliminar un fichero

Detección por emulación

Con la finalidad de evaluar el grado de peligrosidad de una aplicación, estas se ejecutan en un entorno informático simulado (SandBox) antes de instalarlas en el sistema real

- Tiene una mayor capacidad para detectar malware nuevo por lo que no necesita de actualizaciones tan constantes. No obstante, no podrá detectar malware con características nuevas
- Tiene un coste computacional muy alto que penalizara el rendimiento durante los análisis
- Es muy propenso a falsos positivos

Chequeo de integridad

Se comprueba contra una base de datos (checksums, hash) la integridad de aquellos archivos del sistema operativo que no se suelen modificar. Si se detecta que alguno de estos archivos ha sido modificado sin autorización se determina que hay infección

- Debe partir de un archivo limpio
- Esta técnica puede no ser eficaz ante malware que utilice determinadas técnicas de ocultación como el Sobrepasamiento (spoofing)

Control de acceso

Sólo permite que se ejecuten aquellas aplicaciones que tengan permiso explicito del administrador, con determinados privilegios y según el perfil.

- Esta técnica
  - Es poco practica para usuarios particulares
  - Resulta difícil de administrar en ambientes heterogéneos

Limitaciones de las técnicas antimalware

Las principales ventajas del malware frente a las técnicas antivirus son:

- Facilidad de burlar los métodos de detección mediante las técnicas de ocultación
- Falsa sensación de seguridad de los usuarios
- Protocolos que no pueden ser analizados (https)
- Limitaciones de análisis en el perímetro (correo electrónico, web, etc.)
- Formatos de empaquetado y compresión
- Evolución y diversificación del malware

Debido a que todo el malware solo es detectable a posteriori surge la **Ventana vulnerable** que es el tiempo que pasa desde que se crea un nuevo tipo de malware hasta que se actualiza nuestro sistema y nos volvemos inmunes

Durante todo este esquema el usuario final no tiene ningún control, a excepción de la última etapa

El factor humano

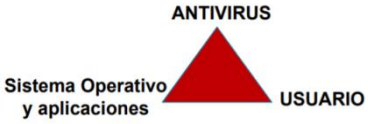
Podemos observar que:

- La mayor parte del malware requiere interacción por parte del usuario para que se pueda infectar la máquina.
- Los antivirus siguen un esquema reactivo por lo que solo serán eficaces cuando ya se haya producido el daño

Como consecuencia, podemos concluir que el componente humano es muy importante en la seguridad informática.

Por lo que, para evitar infecciones no deseadas es recomendable que los usuarios sigan las siguientes recomendaciones

- No abrir correo o ficheros que sean sospechosos
- Instalar aplicaciones conocidas y evitar utilizar links de descarga que no sean de la tienda oficial
- Mantener el Sistema Operativo actualizado siempre que sea posible mediante actualizaciones automáticas
- Configurar correctamente aquellas aplicaciones que tengan acceso a internet como el correo electrónico o los navegadores
  - Desactivar todos los servicios no necesarios
  - Revisar los permisos y denegar los que no les corresponden
  - Asignar las políticas de privilegios según usuario, aplicaciones y recursos compartidos



- Seguir una política adecuada para el uso de contraseñas
- Tener un plan de respaldo mediante copias de seguridad
- Utilizar un antivirus de confianza que utilice técnicas antivirus distintas y complementarias así como un Firewall perimetral basado en hosts

En caso de empresas también se aconseja disponer de

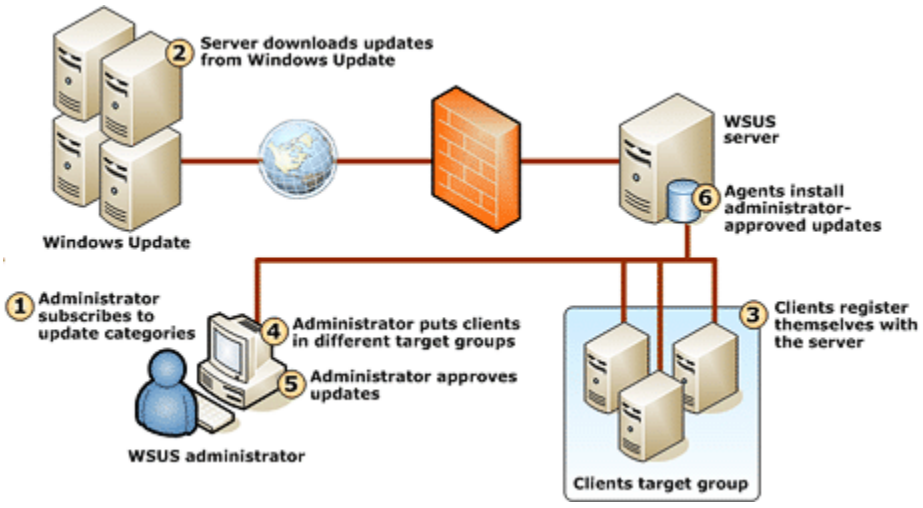
- Una política de filtrado por contenidos
- Una política de acceso a la red interna y externa
- Una gestión centralizada seguridad
- Auditorías y planes de contingencia y continuidad

Gestión centralizada

Windows Update: ofrece la posibilidad de obtener las últimas actualizaciones para mantener el dispositivo en funcionamiento sin problemas y de forma segura. Lo cual ayuda a que tu dispositivo funcione de forma eficaz y se mantenga protegido. Para los usuarios independientes y las organizaciones pequeñas es suficiente con tener correctamente configurado el gestor de actualizaciones automático de Windows

Tipo de usuario	Escenario	Solución
Usuario independiente	Todos los escenarios	Windows Update
Organización pequeña	Sin servidores de Windows	Windows Update
	Al menos un servidor Windows 2000 o una versión más reciente y un administrador de IT	WSUS
Empresa de tamaño mediano a grande	Desea una solución de administración de actualizaciones con un control básico que actualice Windows 2000 y las versiones más recientes de Windows	WSUS
	Desea una solución de administración de actualizaciones flexible con un mayor control para actualizar y distribuir todo el software	SCCM

Windows Server Update Services WSUS: Herramienta que permite al administrador de una red controlar las actualizaciones de todas las máquinas que pertenezcan a la misma red. Este sistema es suficiente para empresas pequeñas y medianas



Windows Server Update Services SCCM Herramienta que permite al administrador de una red controlar la instalación de software así como las actualizaciones y configuraciones de todas las máquinas de la misma red

- Existen extensiones para poder gestionar máquinas con sistemas operativos distintos a Windows

AUTOR: Cuesta Alario David

Diseño de sistemas de seguridad

La seguridad debe ser considerada un objetivo estratégico

Un sistema de seguridad debe

- Ser coherente con el valor de la información a proteger
- Equilibrar correctamente las medidas de seguridad
  - En el ámbito físico y lógico
  - Considerar los servicios un bien a proteger

Estándares de seguridad

Conjunto de normas de aplicación voluntaria impuestas con la finalidad de proporcionar a cualquier empresa un conjunto de buenas prácticas que permitan simplificar y unificar los criterios de la gestión de seguridad de la información con la finalidad de reducir costes y aumentar la efectividad.

Además también permite aumentar la confianza de una empresa entre sus clientes y proveedores

Los organismos de certificación son las empresas encargadas de:

- Unificar las diferentes normativas de productos y servicios
- Ofrecen orientación y ayuda durante la implantación de los estándares y normativas
- Certifican que se ha realizado un plan de gestión de seguridad adecuado
- Comprueban periódicamente que el plan de gestión de seguridad se está ejecutando de forma adecuada

Podemos encontrar las siguientes entidades de certificación:

- **BSI** British Standards Institution
- **IEC** International Electrotechnical Commission
- **ISO** International Organization for Standardization
  - **ISO 27000** Define términos y vocabulario
  - **ISO 27001** Especifica los requisitos de un SGSI
  - **ISO 27002** Define las medidas para gestionar la seguridad de los sistemas de información
    - **Capítulo 9** Control de accesos de los usuarios a los recursos servicios de la empresa
    - **Capítulo 11** Seguridad física y ambiental de los recursos de la empresa
  - **ISO 27003** Describe los pasos a seguir para diseñar un SGSI
    Como resultado de su aplicación se obtiene un plan de implementación del SGSI
  - **ISO 27004** Define cómo medir la efectividad de un SGSI que ya esté implementado
  - **ISO 27005** Define cómo elaborar un plan de riesgos
- **AENOR** Asociación Española de Normalización y Certificación

Sistema de gestión de seguridad

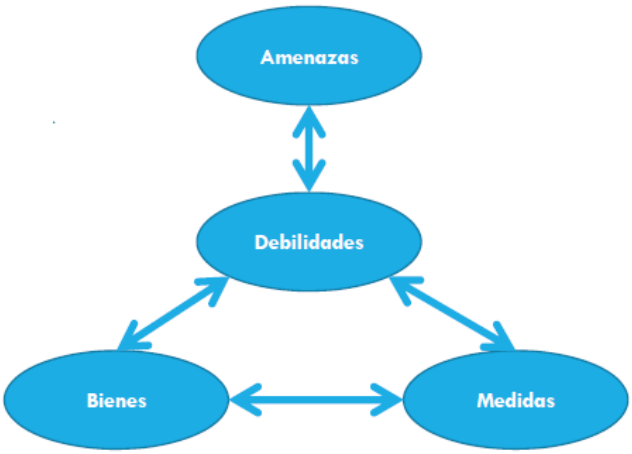
El procedimiento de análisis de riesgos incluye las siguientes etapas

Planificación: consiste en realizar un análisis de las diferentes áreas de una organización con la finalidad de establecer una política de recuperación ante un desastre

- Identificar los bienes a proteger
- Estimar el valor de esos bienes
- Identificar las amenazas que sufren dichos bienes
- Estimar la probabilidad de que esas amenazas se produzcan
- Analizar las medidas necesarias para eliminar esas amenazas
- Estimar el coste de implantar esas medidas

$$C_{oste} < P_{rovavilidad} * V_{alor}$$

El coste de implantar una medida debe ser inferior que la probabilidad de perder el activo que protege



Un plan de contingencia debe incorpora medidas de tres tipos

- **Técnicas**
  - Extintores contra incendios
  - Detectores de humo
  - Salidas de emergencia
  - Equipos informáticos de respaldo
  - Control de accesos
- **Organizativas**
  - Seguro de incendios
  - Precontrato de alquiler de equipos informáticos y ubicación alternativa
  - Procedimiento de Backups
  - Procedimiento de actuación en caso de incendio
  - Contratación de un servicio de auditoría de riesgos laborales
- **Humanas**
  - Formación para actuar en caso de incendio
  - Designación de un responsable de sala
  - Asignación de roles y responsabilidades para la copia de seguridad

Ejecución: Llevar a cabo las medidas de seguridad propuestas durante la fase de planificación

Un plan de contingencia está compuesto por tres sub planes

- **Plan de respaldo:** Establece las medidas de prevención que se van aplicar antes de que se produzca alguna de las amenazas previstas durante la planificación con la finalidad de evitar que se produzcan dichas amenazas
- **Plan de emergencia:** Establece como se debe actúan durante la materialización de una amenaza con la finalidad de reducir sus efectos adversos
- **Plan de recuperación:** Establece como se deben restaurar los sistemas para recuperar su funcionamiento normal
  - Qué recursos materiales son necesarios
  - Qué personas están implicadas en el cumplimiento del plan
  - Cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan
  - Qué protocolos de actuación deben seguir y cómo son

Comprobación: llevar a cabo revisiones periódicas con la finalidad de garantizar que

- El sistema de gestión de seguridad implementado sigue siendo efectivo
  - Esta actualizado frente a nuevas amenazas
  - Se están ejecutando correctamente los planes de respaldo
- El personal recuerda cómo debe actuar ante una emergencia

Actuación: Ante la materialización de una amenaza:

- Si la amenaza estaba prevista:
  - Y las contramedidas fueron eficaces: Se revisan aspectos menores para tratar de mejorar la eficiencia
  - Y las contramedidas no fueron eficaces: Se analiza la causa del fallo y se proponen nuevas contramedidas
- Si la amenaza no estaba prevista: se realiza un nuevo análisis de riesgos

Personal Involucrado en un sistema de gestión de seguridad

Elementos que intervienen en un sistema de seguridad informático:

- La administración de seguridad es la responsable de:
  - Determinar los bienes que se deben proteger
  - Identificar los riesgos que se pueden producir
  - Realiza e implementar el plan de seguridad
- Los usuarios son todos aquellos que vayan a participar en el sistema. Para el correcto funcionamiento todos deben:
  - Conocer la política de seguridad de la empresa
  - Involucrarse en la seguridad
  - Conocer la legislación

AUTOR: Cuesta Alario David

Tipos de seguridad

Las amenazas para un sistema informático pueden proceder desde dos fuentes.

De este modo, para garantizar su seguridad es necesario que esté protegido desde ambos de vista por igual

¿De qué sirve tener el software protegido contra hackers si cualquiera puede llevarse el ordenador?

Seguridad Lógica

Son todas aquellas técnicas de prevención y recuperación que se implementan con la finalidad de evitar aquellas amenazas que se producen como consecuencia de la acción de un software dañino que llega por vía remota y se instala en la computadora del usuario.

Seguridad Física

Consiste en proteger físicamente los recursos del sistema con la finalidad de que la información crítica o sensible no sea accedida físicamente por personal no autorizado.

- Establecer áreas seguras mediante la aplicación de barreras físicas
  - Muros y vallas
  - Personal de seguridad
  - Tarjetas de acceso
  - Sistemas biométricos
- Procedimientos de control contra las amenazas a los recursos
  - Los accesos deben ser auditados de manera periódica
  - La información de los accesos también debe ser protegida
  - Es recomendable llevar una identificación visible de manera continua
  - Alentar a los empleados a sospechar de personas no identificadas
  - Revisar los permisos de manera periódica
  - No todos los empleados tienen porqué saber qué se hace en el área protegida
  - Las áreas protegidas desocupadas deben quedar bloqueadas
- Controlar a los usuarios ajenos a la organización
  - Los visitantes de áreas protegidas deben ser supervisados o inspeccionados
  - La fecha y hora de sus entradas y salidas debe quedar registrada
  - El acceso debe permitirse con propósitos específicos y autorizados
  - El visitante debe ser instruido en las medidas de seguridad del área

Amenazas a los sistemas de gestión de información

El 90% de empresas que experimentan pérdidas significativas de datos, quiebran en un plazo de 3 años.

Ocasionadas por el hombre

Los usuarios son parte del sistema (tienen acceso a información y servicios) por lo que también pueden generar problemas de seguridad (voluntarios o involuntarios). Como consecuencia, hay que tenerlos en cuenta en las políticas de seguridad

- Evaluar los riesgos y su exposición a los mismos
  - Robo
  - Fraude
  - Sabotaje
- Preparar una respuesta por si se producen
- Limitar el acceso a los datos
  - Permisos de impresión o extracción de datos sólo a los usuarios que realmente lo necesitan
  - Revisión de los empleados al abandonar el área de seguridad

"Un sistema de seguridad es tan efectivo como lo es su eslabón más débil. En el caso de la seguridad online, el eslabón más débil es siempre el factor humano"

Alteraciones del entorno

Temperaturas extremas: Sistemas de refrigeración

Polvo o Insectos: Filtros en los conductos y Limpieza

Ocasionadas por desastres naturales

Terremotos

- Emplazamientos adecuados
- Protecciones del edificio

Fuego

- Detector humo y calor
- Materiales ignífugos
- Extintores revisados

Tormentas eléctricas:

- Limitadores de tensión
- Estabilizadores de corriente
- Sistemas de Alimentación Ininterrumpida

Inundaciones y derrame de líquidos

- Sistemas de drenaje o cámaras estancas
- Prohibido comer y beber en el puesto de trabajo
- Localización del equipamiento a nivel general y en salas adecuadas
- Revisar conductos del agua

AUTOR: Cuesta Alario David

Ingeniería Social

Como ya hemos visto la mayor parte de los virus necesita la intervención del usuario para infectar un equipo

Detrás del éxito de una gran parte de los ataques informáticos se encuentra un usuario inocente

"Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es una llamada a un empleado desprevenido y acceden al sistema sin más."

"Si pides información confidencial la gente sospecha de inmediato. No obstante, Si finges que ya tienes esa información y dices algo que está mal, la gente suele corregirte con la información que estabas buscando."

Consiste en aprovechar el factor humano para obtener información confidencial

- Principios de la Ingeniería Social según Kevin Mitnick
  - Todos queremos ayudar
  - El primer movimiento es siempre de confianza hacia el otro
  - No nos gusta decir NO
  - A todos nos gusta que nos alaben
- Debilidades humanas típicamente explotadas
  - Desconocimiento / Ignorancia
  - Dejadez / Pereza
  - Curiosidad
  - Comunicación
  - Miedo
  - Vergüenza / Desprestigio

Técnicas

Pasivas: consiste en obtener información de un usuario sin interactuar con él, realizando un seguimiento de su actividad online y esperando a que cometa un error que se pueda aprovechar.

Se puede utilizar la información publicada en las redes sociales para obtener información que será utilizada más adelante como base de una técnica activa

- Obtener posibles contraseñas
- Descubrir aficiones o actividades habituales que realiza el usuario

Activas: Se engaña al usuario para que proporcione información

- **Scam** Estafa a través de correo electrónico o páginas web fraudulentas en las que se pretende convencer al usuario para que facilite información sensible o acceda a realizar un pago por medio del engaño

  Técnicas que se pueden considerar:
  - **Hoax :** Es una falsedad articulada de manera deliberada para que sea percibida como verdad.
    - Presentar una supuesta donación o un premio de lotería a recibir al que se accede previo envío de dinero
    - Juegan con los miedos o buena intención de los usuarios
    - Cuando algo sea real, el usuario no se lo creerá

    Para no verse afectado por estas amenazas:
    - Evitar acceder a información cuya fuente no sea confiable y eliminar el correo no solicitado
    - No utilizar dinero en el pago de servicios o productos de los cuales no se posean referencias ni se pueda realizar el seguimiento de la transacción.
  - **Spam :** Se trata de una técnica de envió masivo de mensajes no solicitados, generalmente de tipo publicitario, que perjudican de alguna o varias maneras al receptor
    - No suelen tener consecuencias económicas
    - Generan tráfico inútil y sobrecargan servidores
  - **Cross Site Scripting** Inyectar código malicioso en la página real

- **Phishing :** Consiste conseguir la credibilidad del usuario mediante una suplantación de identidad
  - Cambiar el contenido de un mensaje para que parezca que proviene de una fuente que no es la real con la finalidad de hacerse pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica. Generalmente se manipula:
    - El diseño HTML del correo electrónico para lograr que un enlace parezca una ruta legítima pero redirija a la misma página web clonada
    - El dominio del que procede el mensaje de modo que parezca que proceden de tu dominio

  Los ataques de phishing suelen ser masivos pero pueden ser dirigidos
  Para no verse afectado por estas amenazas:
  - Nunca dar información confidencial por e-mail
  - Teclear directamente la dirección en vez de pinchar un enlace
  - Comprobar que la conexión esté cifrada
  - Comprobar los certificados de las páginas Web a las que se acede
  - Usar versiones actualizadas de los navegadores
  - Usar un antivirus que analice las webs que se visitan
  - Usar un servicio de análisis de URLs
  - Añadir un registro del marco de políticas del remitente (SPF) al host de tu dominio permitirá a los destinatarios saber qué servidores tienen permiso para enviar correos desde tu dominio. De este modo podemos garantizar que esos correos no están falsificados.

- **Pharming** Consiste en manipular el tráfico legítimo de un sitio web para que dirija a los usuarios a sitios web falsos con una apariencia muy similar que instalarán software malicioso o registrarán datos personales del usuario
  - Manipulando el fichero de hosts en local
  - **DNS Spoofing** Manipulación del servidor de nombres de dominio mediante la introducción de datos corruptos en la cache del sistema con la finalidad de que re direccionar todo el tráfico dirigido a la IP asignada a un dominio a otra IP distinta que se corresponde con una réplica de la original

  Esta técnica es especialmente peligrosa porque, si afecta a un servidor DNS, incluso los usuarios con equipos protegidos y libres de malware pueden convertirse en víctimas aunque se introduzca correctamente la URL debido a que el redireccionamiento es invisible para el usuario.

  Para no verse afectado por estas amenazas:
  - sospechar si el aspecto de la web es diferente
  - Comprobar los certificados antes de registrarse

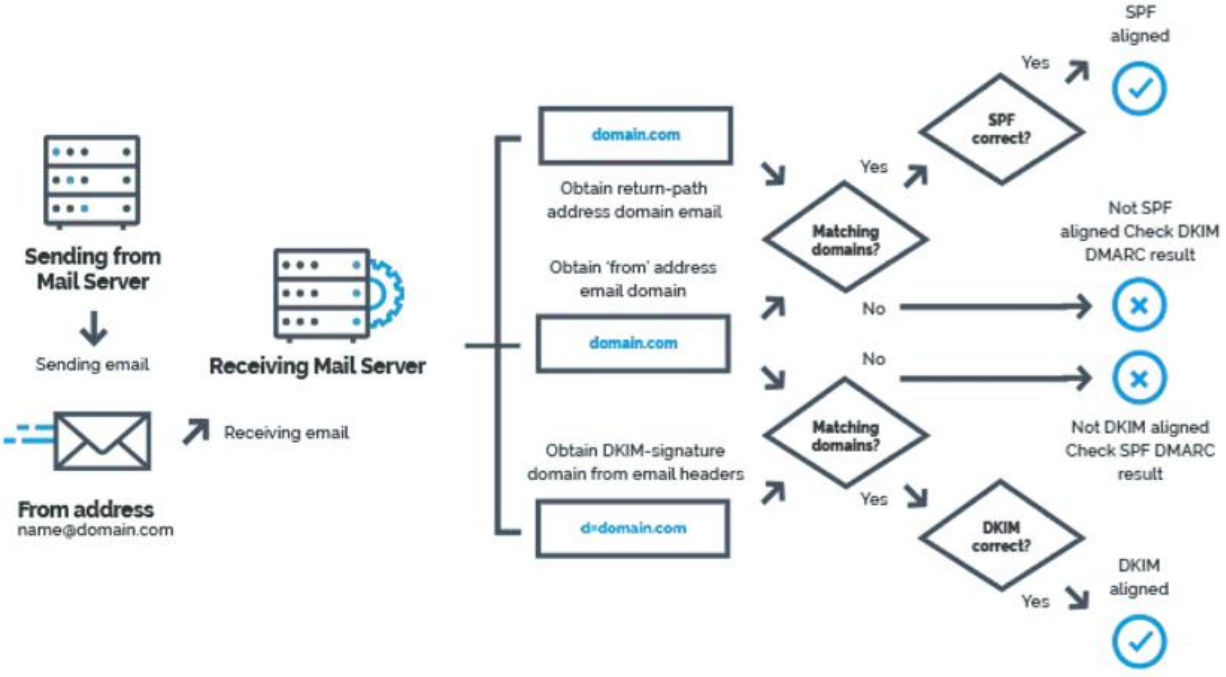
Prevención

La única forma de luchar contra la Ingeniería Social

- Educación de los usuarios
- Implantación de políticas de seguridad que realmente se sigan

Técnicas para detectar fraudes en los correos electrónicos

- **SMTP** (Simple Mail Transfer Protocol) Es el protocolo de red utilizado para el intercambio de mensajes de correo electrónico. Este protocolo se suele utilizar conjuntamente con otros debido a que posee algunas limitaciones en cuanto
  - La recepción de mensajes en el servidor de destino
  - El acuerdo de autentificación entre todos los servidores de correo
- **DMARC** Es un estándar pretende unificar los métodos utilizados en la autenticación del dominio del remitente de correos electrónicos para que tanto los remitentes como los destinatarios puedan verificar los mensajes entrantes
  Para ello se definen las medidas que deben aplicarse a los mensajes recibidos:
  - Deben estar autenticados al menos mediante una de las siguientes técnicas de validación
    - **SPF** (Sender Policy Framework) Es una extensión del protocolo SMTP que permite establecer una protección contra la falsificación de direcciones en el envío de correo electrónico. Permite que el responsable del dominio compruebe las máquinas que están autorizadas para enviar correo a un dominio concreto utilizando la identificación IP a través del Servidor de nombres de dominio.
      - **RMX** Consiste en utilizar el registro MX para comprobar si la dirección IP de la máquina que realiza él envió coincide con la dirección IP de la maquina a la que está especificado que se dirija la respuesta. Pero esta suposición no siempre es cierta, especialmente en grandes proveedores de soluciones de correo
      - **DMP** (Designated Mailer Protocol) consiste en que los proveedores de servicios de internet identifiquen las máquinas responsables del envío del correo. Esta solución es válida, pero para que sea efectiva requiere que todos los proveedores la adopten e implementen.
    - **DKIM** (DomainKeys Identified Mail) es un mecanismo de autenticación de correo electrónico que permite a una organización responsabilizarse del envío de un mensaje de manera que éste pueda ser validado por un destinatario. DKIM utiliza criptografía de clave pública insertando una firma en las cabeceras del mensaje para garantizar Autentificación e integridad al firmar electrónicamente correos electrónicos legítimos de manera que puedan ser verificados por los destinatarios validando la firma obteniendo la clave pública del firmante a través del DNS.
  - El dominio autenticado debe concordar con el que figura en la dirección del encabezado del mensaje.



- **Listas negras** Es una lista de personas, instituciones u objetos que deben ser discriminados en alguna forma con respecto a los que no están en la lista. En una lista negra anti Spam se pueden encontrar direcciones IP individuales o rangos completos de las que se han recibido spam o correo electrónico masivo no solicitado:
  - **SORBS** (Spam and Open Relay Blocking System) Lista negra antispam.
  - **UCEPROTECTL2** (Unsolicited Commercial email) Listas negras de mala reputación

AUTOR: Cuesta Alario David

Seguridad en Redes

Una **red telemática** es el conjunto de equipos conectados mediante un medio de transmisión de datos con la finalidad de compartir información, recursos o servicios en base a un conjunto estricto de reglas que define la sintaxis y la semántica de la comunicación:

- **Protocolo de transferencia de hipertexto HTTP** se trata de un protocolo de comunicación estandarizado para la transferencia de recursos de hipertexto que utilizan los elementos de software de la arquitectura web entre un cliente y un servidor para comunicarse
  Se caracteriza porque:
  - No guarda información sobre conexiones anteriores.
    - Las cookies permiten almacenar información en el sistema cliente por un tiempo indeterminado
    -
  - Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor:
    - El cliente realiza una petición enviando al servidor un mensaje con cierto formato.
    - El servidor le envía un mensaje de respuesta.
  - Da soporte directo a aplicaciones para el envío y recepción de datos a través de la World Wide Web **WWW**
  - Referencia un recurso mediante un identificador único denominado Universal Resource Identifier **URI**

- **El modelo TCP/IP** es un estándar abierto donde se especifican el conjunto de reglas generales para que un equipo pueda comunicarse en una red.
  Un proceso de comunicación completo incluye estos pasos:
  - Creación de datos en la capa de aplicación del host origen
  - Segmentación y encapsulación de datos a medida que pasan por el pila de protocolos host origen
  - Generación de datos para transporte por los medios en la capa de acceso a la red del sistema
  - Transporte de los datos a través de red (compuesta por medios y por cualquier dispositivo intermediario)
  - Recepción de los datos en la capa de acceso a la red del host de destino
  - Des-encapsulación y re-ensamblaje de los datos a medida que pasan por la pila en el dispositivo de destino
  - Transmisión de estos datos a la aplicación de destino en la capa de aplicación del dispositivo final de destino

- El **sistema de nombres de dominio DNS** (Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.
  Entre sus funciones se encuentra:
  - Asocia información variada con el nombre de dominio asignado a cada uno de los participantes de la red
  - Permite localizar y direccionar equipos conectados a la red mediante un identificador único y universal
    - La dirección IP de Google es 216.58.210.163 pero es más común llegar a través de www.google.es

Los mecanismos de seguridad de una red son el conjunto de técnicas que permiten minimizar sus vulnerabilidades con la finalidad de conseguir que el coste de obtener una información protegida sea superior al valor de la misma

Los servicios más importantes a proteger son:

- **Confidencialidad:** Se garantiza que la información transmitida o almacenada en un sistema informático sólo podrá ser leída por su legítimo destinatario, por lo que si dicha información cae en manos de terceras personas no podrán acceder al contenido original.
- **Integridad:** Se garantiza desde su creación la información almacenada, procesada o transmitida no ha sido modificada, o en su defecto permite detectar si se ha dañado, añadido o eliminado parte de la información.
- **Disponibilidad:** Mediante un diseño suficientemente robusto frente a ataques e interferencias se garantiza el correcto funcionamiento del sistema informático con la finalidad de que la información esté disponible en todo momento para sus legítimos usuarios y propietarios
- **Autenticidad:** Se puede comprobar la identidad delos usuarios que participan en la comunicación
- **No repudio:** Se demuestra la autoría de la información mediante un mecanismo que impida que el usuario que la ha creado y enviado pueda negar dicha circunstancia. Se aplica la misma situación al destinatario de la información
  - **Reclamación de origen** (Prueba de origen)**:** Permite probar quién ha sido el creador de determinada información
  - **Referencia temporal** (Prueba de envió)**:** Permite constatar la realización de una operación o comunicación en un determinado instante
  - **Confirmación** (Prueba de entrega)**:** Permite confirmar la realización de una operación reflejando los usuarios que han intervenido
- **Anonimato:** Garantiza que la identidad de los usuarios que acceden a determinados recursos o servicios queda oculta

Tipos de ataques

Sobre la autenticación

- Interceptación
  - **Sniffing** Interceptación de la información que viaja por la red
  - **Man In The Middle** Además de interceptar la información también se puede insertar y modificar a voluntad
  - **Hijacking** Robo de conexiones a un usuario autentificado en el sistema
- Suplantación
  - **Spoofing:** Suplantación de identidad

Sobre la información

- Revelación
- Reenvío
- Manipulación
- Repudio

Sobre los servicios

- Denegación: Satura el software o el Hardware con peticiones hasta que deja de responder
  - **Ataque Distribuido de Denegación de Servicio DDoS** Se realiza desde varias máquinas donde una de ellas ejerce de master y coordina a las demás
- Apropiación

Tipos de protección

Seguridad Perimetral

Usar una arquitectura y elementos de red que provean de seguridad al perímetro de una red frente a otra • Normalmente se estará hablando de una red interna e Internet

Gestión Unificada de Amenazas UTM

Dispositivo que aúna múltiples aspectos relacionados con la seguridad de las comunicaciones

Cortafuegos

Dispositivo software o hardware que permite definir la política de acceso a la red permitiendo o denegando el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas

Es la primera defensa de una red, su finalidad es evitar que usuarios no autorizados tengan acceso a redes privadas conectadas a Internet para ello examina cada mensaje entrante o saliente y bloquea aquellos que no cumplen los criterios de seguridad especificados

Existen dos estrategias de configuración:

- **Política restrictiva** (lista blanca): se deniega todo el tráfico externo a excepción de un conjunto de direcciones especificadas explícitamente.
  Es más segura ya que es más difícil permitir por error tráfico potencialmente peligroso
- **Política permisiva** (lista negra): se acepta todo el tráfico externo a excepción de un conjunto de direcciones especificadas explícitamente
  Es menos segura debido a que es posible que no se haya contemplado algún caso de tráfico peligroso

Un cortafuego correctamente configurado añade las siguientes protecciones a la red:

- Bloquea accesos no autenticados de equipos, aplicaciones y usuarios
- Permite controlar y restringir las comunicaciones entre las partes.
  - Bloquea el tráfico no autorizado
  - Permite el trafico autorizado
- Proporciona un único punto de acceso a la red

Un cortafuego por sí mismo no constituye una defensa suficiente debido a que solo es capaz de analizar y filtrar el tráfico que pase a través de él. Como consecuencia resulta una protección ineficiente ante:

- Ataques procedentes desde el interior de la red
- Ataques cuyo tráfico no pase a través de él o se filtre debido a una mala configuración del trafico permitido
- Ataques de ingeniería social o usuarios negligentes
- Software informático infectado por virus o troyanos
- No es capaz de analizar el correo electrónico ni filtrar el SPAM
- No puede analizar los medios físicos de información (USBs o CDs)

Tipos de cortafuegos

- **De nivel de pasarela:** Aplica mecanismos de seguridad para aplicaciones específicas como FTP o Telnet
  - Es muy eficaz pero puede provocar una degradación del rendimiento
- **De capa de red:** Permite aplicar filtros en función de la IP de origen/destino y del puerto origen/destino
- **De capa de aplicación:** Permite aplicar filtros en función de las características propias del protocolo de comunicación.
  Por ejemplo si se trata de trafico HTTP se puede:
  - Realizar filtrados según la URL
  - Aplicar reglas en función de los valores de los parámetros de un formulario
- **Personal:** se instala como software en un ordenador perteneciente a una red, filtrando las comunicaciones entre dicho ordenador y el resto de la red

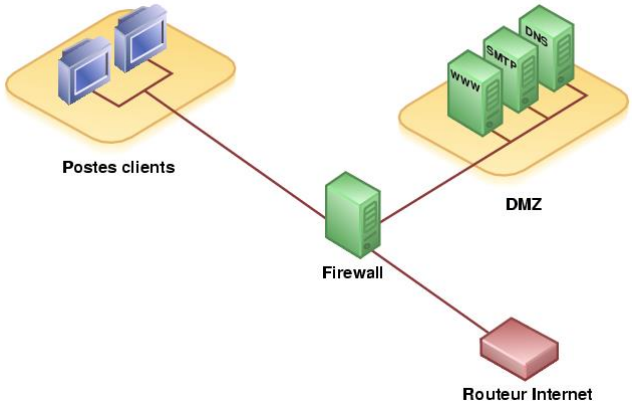
Honeypots

Se trata de una red interna que no contiene ninguna información sensible o servicio real configurado intencionadamente para parecerse lo máximo posible a los sistemas reales pero con algunas vulnerabilidades. Su finalidad es atraer los ataques de los Hackers desviándolos del sistema real y aprovechándolos para estudiar nuevas técnicas y recoger muestras de virus y spam.

Estos sistemas deben estar especialmente controlados y ajenos a cualquier red interna

Zona desmilitarizada DMZ

Es una red local que se ubica entre la red interna de una organización y una red externa (generalmente internet) con el objetivo de separar los datos importantes de la red interna de los servicios públicos que deben poder ser accedidos desde la red externa (correo electrónico, web y DNS) y como consecuencia son más vulnerables ante un posible ataque.



Se crea mediante el uso de uno o dos cortafuegos que limita el acceso entre las distintas redes

- Permitiendo las conexiones desde la red interna y la externa a la zona desmilitarizada
- Bloqueando las conexiones desde la zona desmilitarizada a la red interna de modo que solo se le permita acceder a la red externa

De este modo se permite que los equipos de la zona desmilitarizada puedan dar servicios a la red externa a la vez que protegen la red interna. En el caso de que unos intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada descubrirán que se hallan en un callejón sin salida.

Servicios de Detección y Prevención de Intrusos IDPS

Se trata de un dispositivo de seguridad de red basado en el funcionamiento de los cortafuegos, que monitoriza el contenido y las actividades del tráfico generado en una red con la finalidad de detectar firmas de ataques conocidos, o comportamientos sospechosos con la finalidad de:

- **Sistema de prevención de intrusos IPS** Bloquear la actividad maliciosa
- **Sistema de detección de intrusos IDS** Avisar al administrador de la actividad maliciosa

En función del ámbito de protección podemos diferenciar entre:

- **Host HIDPS**: se instala en la máquina y detecta cambios en el sistema operativo y en las aplicaciones
- **Network NIDPS**: monitoriza el tráfico de la red local
- **Wi-Fi WIDPS**: monitoriza el tráfico inalámbrico
- **Network Behaviour Analysis NBA**: Examina el comportamiento del tráfico de la red

En función del tipo de comportamiento podemos diferenciar entre:

- **Detección heurística:** analiza comportamientos extraños
- **Detección de firmas:** detecta patrones de ataques conocidos

Pasarelas antivirus y antispam

Se trata de un servicio que analiza y filtra el tráfico hacia la red interna permitiendo detectar contenidos

Redes Virtuales Privadas VPN

Es una tecnología de red que permite acceder de manera segura a una red interna desde una infraestructura no segura creando una extensión de la red de área local (LAN) sobre una red pública o no controlada como Internet.

Se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas y cifrado

Mediante este sistema se consigue que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

De este modo conseguimos Autenticación y autorización, Integridad, Confidencialidad y no repudio aunque no se trabaje en la red interna.

Proxys

Dispositivo Software o Hardware que hace de intermediario entre la red interna y externa gestionando las peticiones de recursos que realiza cada cliente a otro servidor

El uso de un proxy proporciona mayor seguridad durante la navegación porque el servidor que recibe la petición desconoce quién se ha conectado realmente. De este modo conseguimos control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, anonimato de la comunicación

Redes Wi-Fi

Las distintas versiones del estándar IEEE 802.11 hacen referencia a su frecuencia y velocidad

Protocolos de seguridad en redes Wi-Fi

WEP

- Utiliza RC4 (algoritmo roto)
- Opción desaconsejada

WPA

- Utiliza RC4 con mejoras
- Opción desaconsejada

WPA2

- Utiliza AES
- Opción recomendada para redes personales o pequeñas empresas
- Alguien conectado a la red puede desencriptar el tráfico de otro usuario si no se esta utilizando una VPN

WPA2 Enterprise

- Utiliza AES
- Opción recomendada para grandes empresas o redes corporativas
- Incluye contraseñas aleatorias usando un servidor RADIUS
- Incluye múltiples protocolos de EAP: Certificados, usuario y contraseña, tarjetas inteligentes

WPA3

- Utiliza claves de 192 bits
- Incluye mecanismos de protección incluso para contraseñas poco seguras
- Incorpora un método Wi-Fi Easy Connect para incorporar dispositivos a través de códigos QR

Servidor RADIUS

Es un protocolo de autenticación que gestionan quién se puede conectar a la red inalámbrica en base a una jerarquía de servidores de manera que si uno no tiene la información, la pide a su superior

Sistema WPS

Es un protocolo de autenticación que incorpora algunas simplificaciones para simplificar el proceso de autentificación a la red inalámbrica que pueden implicar una disminución de la seguridad tales como:

- No incluir un número máximo de intentos en códigos PIN
- Informar si existe un error en los 4 primeros dígitos

AUTOR: Cuesta Alario David

Seguridad Web

La **Open Web Application Security Project** **OWASP** analiza las vulnerabilidades más comunes de las aplicaciones WEB y publica periódicamente un informe

Informe 2017: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Inyección de código

Consiste en engañar al intérprete que analiza los datos introducidos por el usuario enviando datos inesperados como parte de una consulta de modo que el intérprete confunda los parámetros con comandos del sistema
Mediante inyección de código es posible

- Acceder a información restringida de una base de datos
- Aumentar los privilegios de un usuario
- Instalar malware en un servidor

Se encuentran frecuentemente en

- Consultas SQL, LDAP
- Comandos de sistema operativo
- Analizadores sintácticos de XML
- Cabeceras SMTP
- Parámetros de funciones

Estos defectos son fáciles de encontrar cuando se examina el código, sin embargo son difíciles de descubrir mediante pruebas funcionales. Existen utilidades de escaneo que pueden ayudar a encontrar estos defectos

Las técnicas para evitar la inyección son muy sencillas de aplicar:

- Validación de las entradas filtrando los caracteres "peligrosos"
- No usar cuentas con privilegios de administrador
- No proporcionar mayor información de la necesaria (evitar la información de los errores hacia el usuario)
- No construir las sentencias SQL directamente con los valores recogidos, usar sentencias parametrizadas

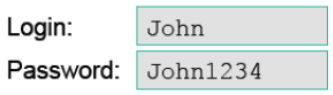
Inyección SQL

Se aprovecha de la sintaxis en este lenguaje para introducir comandos de manera ilícita que permitan leer o modificar la base de datos, comprometiendo el contenido de la consulta original.

Considérese una página web que tiene dos campos para permitir a los usuarios introducir su nombre y contraseña.

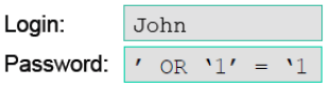
El código detrás generará una consulta SQL para verificar dichas credenciales contra la lista guardada en la base de datos:

SELECT ListaUsuarios. NombreUsuario **FROM** ListaUsuarios
WHERE ListaUsuarios. NombreUsuario $= 'NombreUsuario'$
AND ListaUsuarios. Contraseña $= 'Contraseña'$



Sin embargo, si un usuario introduce un '$NombreUsuario$' valido puede pontear la contraseña con un TRUE

SELECT ListaUsuarios. NombreUsuario **FROM** ListaUsuarios
WHERE ListaUsuarios. NombreUsuario $= 'NombreUsuario'$
AND ListaUsuarios. Contraseña $= '' \boldsymbol{OR} '1' = '1'$



- Si esta consulta devuelve alguna fila entonces se permite el acceso mediante inyección SQL

De esta misma manera se puede introducir cualquier comando comentando la última comilla para que no produzca error

SELECT $*$ **FROM** ListaUsuarios
WHERE ListaUsuarios. NombreUsuario $= '' \boldsymbol{OR} '1' = '1'$
AND ListaUsuarios. Contraseña $= ''; \boldsymbol{DROP\ TABLE}$ ListaUsuarios ; $--'$

- Para que la inyección SQL funcione hay que saber cuántas columnas hay en la consulta o bien hay que conseguir que la sentencia original devuelva vacío

Pérdida de autentificación

Consiste en aprovecharse de las debilidades de una aplicación relacionadas con la autenticación y la gestión de sesiones con la finalidad de comprometer una sesión establecida por un usuario legítimo asumiendo su identidad

- Es posible copiar el identificador de una sesión y utilizarlo para registrarse como el usuario legítimo cuando este haya abandonado su máquina sin cerrar la sesión.
  - Accediendo a los datos de la sesión almacenados en Tokens visibles o a las cookies establecidas permanente
  - A través de un ataque XSS o escuchas en la red mientras se navega por el sitio web
  - Si los datos de sesión se envían sin cifrar cualquiera puede escucharlos por la red
- Es posible registrarse como el propio usuario si se accede a la contraseña debido a una gestión incorrecta
  - Cuando se utilizan contraseñas o preguntas de seguridad sencillas
  - Cuando las contraseñas no se encriptan con un algoritmo seguro
  - Cuando se muestran las contraseñas en la URL

Las técnicas para evitar la pérdida de autentificación son:

- Asegurarse de cerrar la sesión
  - Cuando el usuario se desloguea

```
session_destroy();

Setcookie (“galletita” , “”,time() -3600)
```

  - Cuando el usuario pasa cierto tiempo sin hacer nada
    - Se declara una variable de tiempo en el inicio de sesión
    - En todas las páginas de la aplicación se comprueba periódicamente si dicha variable se ha desbordado

```
$_SESSION['tiempo']= time();
```

```
If (time() > $_SESSION['tiempo'] +300)
{
        session_destroy();
        echo 'Sesión cerrada por inactividad';
        //direccionar a la identificación
}
$_SESSION['tiempo']=time();
```

- Encriptar correctamente los identificadores de sesión cuando se envíen al servidor
- Utilizar los siguientes atributos durante la declaración de las cookies
  - **Httponly** permite evitar el acceso mediante lenguajes de Script
  - **Secure** Los datos solo se envía a través de canales para evitar las escuchas en la re

```
Setcookie ($name , $value , $expire , $path, $domain ,  True , True)
```

Se pueden modificar los valores por defecto en el fichero **PHP. ini**

```
session.cookie_httponly = 1      session.cookie_secure = 1
```

Exposición de datos sensibles

Consiste en no tomar medidas de protección adecuadas para aquellos datos que se consideren sensibles en la aplicación de modo que los atacantes los pueden robar o modificar.

- Almacenamiento de datos sensibles sin cifrar
- Transmisión de datos sensibles sin cifrar
- Uso de algoritmos de cifrado débiles

Los datos sensibles requieren métodos de protección adicionales

- Almacenando cifrada la información sensible
- Asegurando que la información sensible se envíe a través de protocolos seguros
- Usando algoritmos de cifrado robustos

Entidades XML externas

Consiste en aprovecharse de las vulnerabilidades de los procesadores XML para revelar archivos internos a través de las entidades externas referencias en los documentos XML

- Subiendo ficheros XML con código embebido
- Haciendo uso de las dependencias de los ficheros XML

Para evitarlo es recomendable

- Evitar el uso del formato XML y sustituirlo por las estructuras JSON
- Validar todos los fichero XML antes de procesarlos
- Actualizar los procesadores de XML para evitar vulnerabilidades conocidas
- Limitar los orígenes desde los que se pueden enviar ficheros XML

AUTOR: Cuesta Alario David

Rotura de control de acceso

Consiste en no aplicar correctamente las restricciones sobre los permisos que tienen los usuarios autenticados permitiendo acceder sin autentificación o con una autentificación no adecuada a determinados objetos o funcionalidades

- Ver archivos sensibles
- Modificar datos, derechos de acceso o permisos

Si una página no está protegida ante este tipo de ataques se suele poder acceder a todas las funcionalidades escribiendo directamente la URL de la funcionalidad a la que se quiere acceder

Para evitar la rotura de control de acceso se deben emplear datos de sesión o cookies que identifiquen unívocamente a cada usuario y sus permisos a lo largo de todas las ventanas de la aplicación

- Creando una jerarquía de usuarios y almacenando a que clase pertenece cada usuario
- Comprobando en cada ventana si el tipo de usuario es el adecuado o si los permisos son insuficientes.

Para implementarlo:

- Establecemos la sesión cuando el usuario se loguea
  - Mediante datos de sesión

```
$_SESSION['usuario'] = usuario que se ha logueado
```

  - Mediante cookies

```
setcookie('entrada', $DNI, time() + 365 * 24 * 60 * 60);
```

- En cada página de la aplicación comprobamos si el usuario tiene acceso
  - Mediante datos de sesión

```
If ( isset($_SESSION['usuario'] ) AND $_SESSION['usuario'] == $DNI)
{
        echo 'Acceso permitido';
        //redireccionar a la página normal
}
else
{
        echo 'Acceso no permitido';
        //redireccionar a la identificación o inicio
}
```

  - Mediante cookies

```
If ( isset($_COOKIE['entrada'] ) AND $_COOKIE['entrada'] == $DNI)
{
        echo 'Acceso permitido';
        //redireccionar a la página normal
}
else
{
        echo 'Acceso no permitido';
        //redireccionar a la identificación o inicio
}
```

Falsificación de peticiones

Se trata de un método de rotura de control de acceso que consiste en suplantar la forma que tiene una petición de la aplicación con la finalidad de conseguir que un usuario que está correctamente autorizado la ejecute sin darse cuenta

Para evitar la falsificación de peticiones se utiliza un "token" único y aleatorio que forme parte del formulario que realice cualquier petición. Para implementarlo:

- Establecemos el toquen cuando el usuario se loguea

```
$_SESSION['token'] = md5(time());
```

- Lo introducimos en el formulario en un campo de tipo hidden

```
<form>
        ......
        <input type="hidden" value="<?php echo $_SESSION['token']; ?>">
</form>
```

- En cada página de la aplicación se comprueba si el Token coincide con el generado en el inicio de la sesión

```
If ( isset($_POST['token'] ) AND $_POST['token'] == $_SESSION['token'])
{
        //redireccionar a la página normal
}
else
{
        //La llamada no procede de donde debería
}
```

Configuración de seguridad incorrecta

Se trata de un problema muy común que consiste en no tener una buena configuración de la aplicación por desconocimiento, despiste o dejadez. Cometiendo errores como:

- Cabeceras HTTP mal configuradas
- Mensajes de error con contenido sensible
- Falta de parches y actualizaciones
- Dependencias y componentes desactualizados
- Trabajar con usuarios con permisos de administrador
- Mantener las cuentas que se crean por defecto
- Permitir el uso de contraseñas poco seguras

Para evitar una configuración de seguridad incorrecta:

- Eliminar aquellas cuentas de servicios que no se usen
- Modificar las contraseñas que traen por defecto muchos programas
- Deshabilitar puertos/servicios que no se usen
- Actualizar las aplicaciones
- Obligar a los usuarios a usar contraseñas “seguras”
- Definir usuarios específicos para cada aplicación con los permisos que correspondan

Secuencia de comandos en sitios cruzados

Consiste en ejecutar código en lenguaje Script que se introduce como un campo de un formulario y se almacena en una base de datos del navegador de la víctima permitiendo

- Tomar datos no confiables y enviarlos al navegador web sin una validación y codificación apropiada
- Actualizar una página web existente con datos suministrados por el usuario
- Redireccionar a los usuarios hacia un sitio malicioso
- Se ejecuta cada vez que se muestra el valor de ese campo

Se puede probar la vulnerabilidad introduciendo un alert en cualquier campo de un formulario o añadiéndolo a la URL

```
< script > alert(“es vulnerable”); </script >
www. sitio. com/ver. php? id =< script > alert(“es vulnerable”) </script >
```

Para evitar la secuencia de comandos en sitios cruzados se recomienda:

- Limpiar el texto que introduzca el usuario eliminando los caracteres “peligrosos”
- Limpiar los valores que obtengamos de la URL eliminando los caracteres “peligrosos”
  Existen funciones que realizan el trabajo de escapado devolviendo un texto “limpio”

Deserialización insegura

Cuando una aplicación recibe datos en formatos serializados para construir objetos a partir de ellos se puede introducir información que generen objetos no deseados aprovechando el proceso de desempaquetado para

- Realizar ataques de repetición
- Realizar inyecciones
- Modificar los privilegios de ejecución.
- Conducir a la ejecución remota de código en el servidor.

Para evitar la deserialización insegura se recomienda:

- Restringir los formatos en los que se admiten los datos por ejemplo a los tipos primitivos
- Desempaquetar únicamente los datos que vengan firmados
- Desempaquetar únicamente los datos que vengan de orígenes fiables
- Ejecutar el proceso de deserialización en un entorno controlado, de manera externa al resto de la aplicación

Componentes con vulnerabilidades conocidas

Consiste en usar software que utilizan componentes con vulnerabilidades conocidas y por lo tanto puedan ser explotadas para debilitar las defensas de las aplicaciones y permitir ataques

Para evitar el uso de componentes con vulnerabilidades conocidas se recomienda:

- Estar al día de la publicación de vulnerabilidades
- Aplicar los parches correspondientes en cuanto salgan
- Buscando alternativas que no presenten vulnerabilidades

Logueo y monitorización insuficientes

Consiste en no registrar los intentos de acceso o las acciones no autorizadas independientemente de si tienen éxito o no.
La información de los intentos de acceso puede ser muy valiosa

- para detectar
  - **Conductas sospechosas:** empleados accediendo al sistema cuando no deben
  - **Nuevos tipos de amenazas:** El tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos
  - **El objetivo de los ataques:** múltiples intentos fallidos con el mismo usuario
- Para impedir
  - Que los nuevos ataques se mantengan en el tiempo
  - Los ataques de repetición

En algunos casos es obligatorio almacenar esta información debido a la LOPD con la finalidad de detectar a los responsables de los incidentes

Para evitar el logueo y monitorización insuficientes se recomienda:

- Almacenar toda la información referente a las conexiones exitosas y fallidas
- Analizar la información sobre las conexiones
- Bloquear al usuario cuando alcanza un determinado número de intentos fallidos consecutivos

Aspectos legales

Las leyes son una serie de normas generales que están abiertas a la interpretación que se les quiera dar.

Existen distintos niveles de legislación, cada uno de los cuales es más específico porque debe recoger las obligaciones establecidas por el nivel anterior

Nivel europeo

A nivel Europeo se ha intentado crear la definición de cibercrimen (convención de Budapest de 2001) para que los países miembros puedan adoptar en sus legislaciones los delitos informáticos si lo desean.

Al unirse adaptan su legislación para contemplar los siguientes delitos

- Contra la confidencialidad, integridad y la disponibilidad de los datos y sistemas informáticos
  - Acceso ilícito a sistemas
  - Interceptación ilícita de datos
  - Interferencia en el funcionamiento de un sistema
  - Falsificación o fraude mediante la introducción, alteración, borrado de datos
  - Abuso de dispositivos que faciliten la comisión de los delitos anteriores
- Contra la producción, oferta, difusión, transmisión, adquisición o tenencia en sistemas de contenidos
  - De pornografía infantil
  - De material racista o xenófobo
  - De minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad
- Contra la propiedad intelectual y derechos afines

Definiciones

Datos personales

Toda información sobre una persona física identificada o identificable directa o indirectamente mediante un identificador

Tratamiento

Cualquier operación o conjunto de operaciones realizadas sobre datos personales mediante procedimientos automatizados o realizado por personas. Entre las que se incluyen

- Recogida y registro
- Organización, estructuración
- Conservación
- Adaptación o modificación
- extracción, consulta o utilización
- Cualquier forma de habilitación de acceso como comunicación, transmisión, difusión o cotejo
- Interconexión
- Limitación, supresión o destrucción.

Seudonimización

Tratamiento de datos personales de manera que no puedan atribuirse a un interesado sin utilizar información adicional que figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física

Fichero

Conjunto estructurado de datos personales accesibles con arreglo a determinados criterios

Responsable del tratamiento

Persona física o jurídica que se hace responsable del tratamiento de los datos y determina los fines y medios del tratamiento.

Encargado del tratamiento

Persona física o jurídica que trata los datos personales por cuenta del responsable del tratamiento

Destinatario

Persona física o jurídica al que se le comunican los datos personales conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

No se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación que cuente con la conformidad de la Unión o de los Estados miembros

Tercero

Persona física o jurídica distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Consentimiento del interesado

Toda manifestación de voluntad por la que el interesado acepta el tratamiento de datos personales mediante una declaración afirmativa:

- Libre
- Específica
- Informada
- Inequívoca

Protección de datos

En el reglamento 2016/679 se contemplan los derechos de protección de las personas físicas en lo que respecta al tratamiento de datos personales y su libre circulación

Los datos personales recogidos deben cumplir las siguientes restricciones

Integridad y confidencialidad

Teniendo en cuenta

- El estado de la técnica
- Los costes de aplicación
- La naturaleza, el alcance, el contexto y los fines del tratamiento
- Los riesgos de probabilidad y gravedad para los derechos y libertades de las personas físicas

Los datos personales serán tratados mediante la aplicación de medidas técnicas u organizativas apropiadas que permitan garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento

Incluyendo las siguientes medidas técnicas y organizativas:

- La seudonimización
- El cifrado
- La capacidad de restaurar la disponibilidad y el acceso
- Un proceso de verificación, evaluación y valoración

De tal manera que se garantice una seguridad adecuada contra

- El tratamiento no autorizado o ilícito
- La pérdida, destrucción o daño o alteración accidental o ilícita
- La comunicación o acceso no autorizado

Responsabilidad proactiva

El responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que las políticas de protección de datos:

- Son conformes con el presente Reglamento
- Garantizan la protección de los derechos del interesado
- Se aplican adecuadamente.
- Se revisan y actualizan periódicamente.

Cuando el responsable del tratamiento elija un encargado para tratar datos personales, este deberá ofrecer garantías suficientes de haberse comprometido a respetar la confidencialidad de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del

Comunicación

El responsable del tratamiento facilitará al interesado toda la información pertinente acerca del tratamiento de los datos así como cualquier actuación realizada:

- En el plazo de un mes a partir de la recepción de la solicitud.
  Dicho plazo podrá prorrogarse otros dos meses en función de la complejidad y el número de solicitudes
  - Informando al interesado en el plazo de un mes a partir de la recepción de la solicitud
  - Indicando los motivos de la dilación
- De forma gratuita

Cuando las solicitudes sean manifiestamente infundadas o excesivas (especialmente debido a su carácter repetitivo) el responsable del tratamiento podrá:

- Cobrar un canon razonable
- Negarse a actuar respecto de la solicitud.

Se facilitara al interesado la siguiente información:

- La identidad y los datos de contacto
  - Del responsable o de su representante
  - Del delegado de protección de datos
- Los fines del tratamiento y los intereses legítimos del responsable o de un tercero
- La base jurídica del tratamiento
- Los destinatarios o las categorías de destinatarios a los que se les comunican los datos personales.
  Así como los destinatarios a los que se tiene intención de comunicárselos
  En particular destinatarios en organizaciones internacionales
- Confirmación de si se están tratando o no datos personales que le conciernen así como las categorías de datos personales que están siendo tratados
- El plazo durante el cual se conservarán los datos personales o los criterios utilizados para determinar dicho plazo
- Cualquier información sobre el origen de los datos cuando estos no se hayan obtenido directamente del interesado
- La existencia del derecho a solicitar
  - El acceso a los datos personales relativos al interesado
  - La rectificación, supresión o limitación del tratamiento de los datos
  - La portabilidad de los datos
- Las consecuencias derivadas de no facilitar los datos que se consideran obligatorios para suscribir el contrato
- La existencia de decisiones automatizas incluyendo información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Transparencia

Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado

Finalidad

Los datos personales serán recogidos con fines determinados, explícitos y legítimos

Exactitud

Los datos personales se mantendrán actualizados

Limitación del plazo

Los datos personales se conservaran durante no más tiempo del necesario en relación con los fines para los que son tratados

Minimización

Se recogerán exclusivamente los datos personales necesarios, adecuados y pertinentes en relación con los fines para los que son tratados

Solo serán objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento

Por defecto, los datos personales no serán accesibles a un número indeterminado de personas físicas, sin la intervención del interesado

Revocación

El interesado tendrá derecho a retirar su consentimiento en cualquier momento.

- La retirada del consentimiento no afectará a la licitud del tratamiento previo a su retirada.
- Será tan fácil retirar el consentimiento como darlo.
- El responsable del tratamiento estará obligado a suprimir sin dilación los datos personales cuando:
    - Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos
    - El interesado retire el consentimiento en que se basa el tratamiento de conformidad
    - El interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento
    - Los datos personales hayan sido tratados ilícitamente
    - Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida
    - Los datos personales se hayan obtenido de servicios ofertados a menores de edad

Actualización

El interesado tendrá derecho a obtener del responsable del tratamiento
- La rectificación de los datos personales inexactos que le conciernan.
- Que se completen los datos personales que sean incompletos inclusive mediante una declaración adicional.

Limitación del tratamiento

El responsable del tratamiento estará obligado a dejar de utilizar los datos personales del interesado cuando:

- El interesado impugne la exactitud de los datos personales durante un plazo que permita al responsable verificar la exactitud de los mismos
- El interesado se oponga al tratamiento de los datos personales mientras se verifica si los motivos del interesado prevalecen sobre los del responsable
- El tratamiento sea ilícito pero el interesado se oponga a la supresión de los datos personales
- El responsable ya no necesite los datos personales para los fines del tratamiento pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones

Oposición

El interesado tendrá derecho a oponerse al tratamiento de los datos personales que le conciernan en cualquier momento

Especialmente cuando el tratamiento de datos personales tenga por objeto

- La mercadotecnia directa
- El tratamiento automatizado, incluida la elaboración de perfiles

El responsable del tratamiento dejará de tratar los datos personales, salvo:

- Que se acrediten motivos legítimos que prevalezcan sobre los intereses, los derechos y las libertades del interesado
    - Es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento
    - Está autorizada por el Derecho de la Unión o de los Estados miembros
    - Se basa en el consentimiento explícito del interesado
- Para la formulación, el ejercicio o la defensa de reclamaciones.

Portabilidad de los datos

El interesado tendrá derecho a

- Recibir los datos personales que le incumban en un formato
    - Estructurado
    - De uso común
    - De lectura mecánica
- Transmitir directamente los datos personales que le incumban a otro responsable del tratamiento sin oposición del anterior responsable siempre que sea técnicamente posible y
    - El tratamiento esté basado en el consentimiento
    - El tratamiento se efectúe por medios automatizados

Notificación de violación de la seguridad

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente en un plazo no superior a 72 horas después de que haya tenido constancia de ella.

Se permite exceder el plazo cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. En cuyo caso deberá ir acompañada de indicación de los motivos de la dilación.

La comunicación no será necesaria cuando el responsable del tratamiento ha adoptado medidas de protección que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos

Si la comunicación directa al interesado supone un esfuerzo desproporcionado se optará por una comunicación pública por la que se informe de manera igualmente efectiva a los interesados.

Excepciones

El Derecho de la Unión o de los Estados miembros podrá limitar el alcance de las obligaciones y los derechos siempre que:

- Se respete la esencia de los derechos y las libertades fundamentales
- Sea una medida necesaria y proporcionada para salvaguardar
    - La seguridad del Estado
    - La defensa de los derechos y libertades de otros
    - La seguridad pública
    - La independencia judicial y de los procedimientos judiciales
    - Otros objetivos importantes de interés público general

Protección de redes y servicios

Define qué servicios relativos a las telecomunicaciones deben ofrecerse a los ciudadanos

Neutralidad de la red

Incluye el acceso a Internet en los servicios universales

- Permite a los operadores priorizar el tráfico de las redes en función de las necesidades y para evitar congestiones
- Permite las conexiones gratuitas a servicios con los que hayan llegado previamente a un acuerdo
- No se puede perjudicar o cobrar por un tráfico específico

Confidencialidad

Los estados miembros garantizarán la confidencialidad de las comunicaciones prohibiendo la intervención, escucha, grabación y almacenamiento a excepción del el almacenamiento técnico necesario para la conducción de una comunicación

Comunicaciones no solicitadas:

Sólo se autoriza el uso de sistemas de llamada automática (sin intervención humana), fax o correo electrónico con fines de venta directa a aquellos abonados que hayan dado su consentimiento previo.

- Se debe ofrecer a los clientes la posibilidad de oponerse de manera sencilla y sin cargo alguno tanto
    - En el momento en que se recojan sus datos
    - Cada vez que reciban un mensaje
- Se prohíbe disimular u ocultar la identidad del remitente así como o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones.

Propiedad intelectual

Los Estados miembros dispondrán en su derecho nacional medidas judiciales destinadas a prevenir cualquier infracción de un derecho de propiedad intelectual.

Para considerar a alguien como el autor de una obra es suficiente con que su nombre figure en la obra de forma habitual.

La duración de los derechos de autor es de 70 años tras el fallecimiento del último autor o de su publicación si es anónima

- Obras literarias
- Obras cinematográficas o audiovisuales
- Composición musical con letra
- Fotografías:

Personas legitimadas para solicitar la aplicación de medidas, procedimientos y recursos:

- Los titulares de los derechos
- Las personas autorizadas a usar dichos derechos
- Los organismos de gestión de derechos colectivos reconocidos
- Los organismos profesionales de defensa reconocidos.

Nivel estatal

La legislación estatal tiene que cubrir lo indicado en las directivas europeas

Cuando se aprueba una nueva directiva los estados miembros tienen un plazo para adaptar sus leyes

En España

- **El código penal** recoge la legislación estatal
    - no reconoce los delitos informáticos como delitos específicos sino como un medio que se puede usar para cometer otros delitos tales como
        - Robo de dinero o información
        - Suplantación de identidad
        - Tráfico de armas, dinero, personas, etc…
        - Amenazas
        - Estafas
- **El Grupo de Delitos Telemáticos de la Guardia Civil** es el encargado de investigar las infracciones del Código Penal

Prostitución y corrupción de menores

Se considera delito relativo a la prostitución y la corrupción de menores a cualquier acción que

- Induzca, promueva, favorezca, facilite, explote o se lucre con prostitución infantil
- Capte, utilice, financie o se lucre con espectáculos exhibicionistas o pornográficos (tanto públicos como privados) con la finalidad de elaborar cualquier clase de material pornográfico infantil
- Produzca, venda, distribuya, exhiba, ofrezca o facilite la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil aunque el material tuviere su origen en el extranjero o fuera desconocido
- Adquiera o posea pornografía infantil para su propio uso
- Acceda por medio de las tecnologías de la información y la comunicación a contenido de pornografía infantil a sabiendas

En cuya elaboración hayan sido utilizadas personas

- Menores de edad
- Personas con discapacidad necesitadas de especial protección

Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de Internet que contengan o difundan pornografía infantil, o en su defecto, para bloquear su acceso a los usuarios que se encuentren en territorio español.

Abusos sexuales

Se considera delito relativo a los abusos sexuales a cualquier acción que

- Realice actos que atenten contra la libertad o indemnidad sexual de otra persona
    - Sin violencia o intimidación
    - Sin que medie consentimiento
    - Se ejecuten sobre personas que se hallen privadas de sentido debido a
        - Un trastorno mental
        - El uso de fármacos, drogas o cualquier otra sustancia natural o química
- Ejecute o haga ejecutar a otra persona actos de exhibición obscena ante
    - Menores de edad
    - Personas con discapacidad necesitadas de especial protección
- Venda, difunda o exhiba material pornográfico entre
    - Menores de edad
    - Personas con discapacidad necesitadas de especial protección

Delitos sobre daños

Se considera delito relativo a daños a cualquier acción que

- borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles por cualquier medio y sin autorización cualquier tipo de datos informáticos, programas informático o documentos electrónicos ajenos
- Obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:
  - Introduciendo o transmitiendo datos
  - Destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica
- Produzca, adquiera para su uso, importe o facilite a terceros sin estar autorizado
  - Un programa informático concebido o adaptado para cometer alguno de los delitos mencionados
  - Una contraseña o código de acceso que permitan acceder a la totalidad o a una parte de un sistema de información

Delitos sobre amenazas

Se considera delito relativo a amenazas a cualquier acción que

- Exija de otro una cantidad o recompensa bajo la amenaza de
  - Revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés

Delitos sobre calumnias e injurias

Se considera delito relativo a calumnias a cualquier acusación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad.

- El acusado por delito de calumnia quedará exento de toda pena probando el hecho criminal que hubiere imputado.

Se considera delito relativo a injurias a cualquier acción o expresión que se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad y lesione de forma grave la dignidad de otra persona

- Menoscabando su fama
- Atentando contra su propia estimación

Los delitos de calumnia e injuria se agravan si realizan con publicidad propagándolos mediante cualquier medio de difusión de masas tales como la imprenta, la radio o internet.

La diferencia entre injuria y calumnia es la imputación de un delito, pues si el hecho que se imputa tiene carácter delictivo nos encontraremos ante una calumnia y de no tenerlo nos enfrentaremos a una injuria.

Delitos sobre estafas

Se considera delito relativo a estafa a cualquier acción con ánimos de lucro que

- Utilicen el engaño para inducir a otra persona a realizar un acto de disposición en perjuicio propio o ajeno
- Consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
- Produzca, adquiera para su uso, importe o facilite a terceros sin estar autorizado
  - Un programa informático concebido o adaptado para cometer alguno de los delitos mencionados
  - Cualquier dato o instrumento que pueda utilizarse para cometer alguno de los delitos mencionados
    - Tarjetas de crédito o débito
    - Cheques de viaje
    - Firmas
    - Expedientes, protocolos o documentos públicos u oficiales de cualquier clase

Delitos sobre revelación de secretos

Se considera delito relativo a descubrir los secretos a cualquier acción que permita vulnerar la intimidad de otro sin su consentimiento

- Apoderándose, utilizando o modificando documentos o efectos de carácter personal o familiar (Papeles, cartas, mensajes de correo electrónico)
- Utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen

AUTOR: Cuesta Alario David

Delitos sobre la propiedad intelectual

La propiedad intelectual protege

- Las creaciones originales literarias, artísticas o científicas expresadas en cualquier medio
- Las interpretaciones artísticas, los fonogramas, las grabaciones audiovisuales y las emisiones de radiodifusión

La propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación.

Se considera delito relativo a la vulneración de la propiedad intelectual a cualquier acción que sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual y con ánimo de obtener un beneficio económico directo o indirecto o en perjuicio de tercero

- Reproduzca, plagie, distribuya, comunique públicamente o explote económicamente dicho objeto
- Almacenen intencionadamente ejemplares de obras cuando estuvieran destinadas a ser reproducidas, distribuidas o comunicadas públicamente

A quien en la prestación de un servicio de la sociedad de la información preste o facilite dichos servicios de modo activo y no neutral se le ordenará la interrupción de la prestación del mismo

Inclusión de la propiedad intelectual

Es lícita la inclusión en una obra propia de fragmentos de otras ajenas siempre que se trate de obras ya divulgadas y su inclusión se realice a título de cita o para su análisis, comentario o juicio crítico

Tal utilización sólo podrá realizarse con fines docentes o de investigación, en la medida justificada por el fin de esa incorporación e indicando la fuente y el nombre del autor de la obra utilizada.

La puesta a disposición del público (por parte de prestadores de servicios electrónicos de agregación de contenidos) de fragmentos no significativos de contenidos divulgados en publicaciones de actualización periódica y que tengan una finalidad informativa no requerirá autorización del editor ni derechos a percibir una compensación equitativa

Programa informático

Se entenderá por programa de ordenador toda secuencia de instrucciones destinadas a ser utilizadas en un sistema informático para realizar una tarea obtener un resultado determinado

Los programas de ordenador serán protegidos únicamente si fuesen una creación intelectual propia de su autor

No estarán protegidos las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador Incluidos los que sirven de fundamento a sus interfaces

También gozarán de la misma protección

- Su documentación técnica y preparatoria (Manuales de uso)
- Cualesquiera versiones sucesivas del programa así como los programas derivados
    - Salvo aquellas creadas con el fin de ocasionar efectos nocivos a un sistema informático.

Será considerado autor y titular de los derechos del programa informático la persona, grupo de personas o persona jurídica que lo hayan creado

- Los derechos de autor sobre un programa de ordenador que sea resultado unitario de la colaboración entre varios autores serán propiedad común y corresponderán a todos éstos en la proporción que determinen.
- Cuando un trabajador asalariado cree un programa en el ejercicio de las funciones que le han sido confiadas la titularidad de los derechos de explotación corresponden exclusivamente al contratante salvo pacto contrario

Delitos sobre la propiedad industrial

A través de las patentes se protege la propiedad Industrial que representa la creatividad, ingenio e invención del intelecto humano que puede ser aplicado en la industria. Pues son una de las posesiones más importantes para las personas y sociedades

Se considera delito relativo a la vulneración de la propiedad industrial a cualquier acción que sin la autorización de los titulares de los correspondientes derechos de propiedad industrial y con ánimo de obtener un beneficio económico directo o indirecto o en perjuicio de tercero

- fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio
    - Objetos amparados por tales derechos.
    - Obtenidos directamente por el procedimiento patentado.
    - Incorporen un signo distintivo idéntico o confundible
- Utilice u ofrezca la utilización de un procedimiento objeto de una patente
- Almacene intencionadamente servicios o actividades amparados por tales derechos

Protección de datos

La Agencia Española de Protección de Datos se encarga de

- Velar por el cumplimiento de la legislación sobre protección de datos
- Atender peticiones y reclamaciones
- Sancionar los incumplimientos
- Establece las siguientes obligaciones
    - Declarar los ficheros automatizados y no automatizados con datos de carácter personal
    - Legitimar los datos
        - Consentimiento del afectado
        - Información al afectado
        - Calidad de los datos
- Proteger los ficheros para preservar la confidencialidad, integridad y disponibilidad de los datos

Ley de Servicios de la Sociedad de la Información y de comercio electrónico

Las empresas deben

- Informar en su página web acerca de los siguientes datos
    - Razón social, NIF, domicilio y dirección de correo electrónico
    - Datos de inscripción registral
    - Códigos de conducta a los que estén adheridas
    - Precio de los productos o servicios con indicación de los impuestos y gastos de envío aplicables
    - Autorización administrativa para el ejercicio de la actividad
- Recabar el consentimiento del destinatario cuando empleen dispositivos de almacenamiento y recuperación de datos

Ley General de Telecomunicaciones

El acceso a internet es un servicio universal por lo que su prestación debe estar garantiza para todos los usuarios finales con

- Independencia de su localización geográfica
- Con una calidad determinada
- A un precio asequible.

Suministro de la conexión a la red pública de comunicaciones electrónicas desde una ubicación fija

Prestación del servicio telefónico disponible al público

En España la empresa obligada a suministralos es telefónica

Accesibilidad

Las siguientes páginas de internet y sus contenidos

- Las administraciones públicas
- Las entidades y empresas que se encarguen de gestionar servicios públicos
- Los centros públicos educativos
- Los centros privados sostenidos total o parcialmente con fondos públicos

Deberán cumplir ciertos criterios de accesibilidad para garantizar el acceso a

- Las personas mayores
- Las personas con discapacidad

Salvo cuando una funcionalidad o servicio no disponga de una solución tecnológica que lo permita

Además deberán contener de forma clara

- Información sobre el grado de accesibilidad que hayan aplicado
- La fecha en que se hizo la revisión del nivel de accesibilidad
- Un sistema de contacto para que los usuarios puedan transmitir las dificultades de acceso al contenido de las páginas

Nivel autonómico

Su ámbito de actuación se limita a los ficheros de titularidad pública

Los de titularidad privada hay que declararlos en la agencia estatal

Define sus propios formularios y procesos para el tratamiento de datos y la ejecución de los derechos asociados a los mismos

En Euskadi existen una serie de leyes que complementan y especifican (no pueden contradecirlas) la legislación a nivel estatal

- Definen sus propias normas de accesibilidad
- Definen Entidades Certificadoras
- Definen normas y formas de comunicación con la administración de manera electrónica

Informática Forense

Es una disciplina criminalística que Incluye un conjunto de técnicas que permiten investigar sistemas informáticos para obtener y procesar evidencias digitales con validez jurídica para la investigación privada

Algunas de las tareas que se llevan a cabo pueden consistir en

- Extraer información de un sistema
- Recuperar información cifrada / eliminada / dañada
- Monitorizar el comportamiento de un sistema
- Detectar incumplimientos de las políticas de la empresa

Es utilizada por

- Agentes de la ley
- Compañías de seguros
- Compañías privadas
- Personas particulares

Identificación

Consiste en identificar los sistemas (evidencias) que van a ser necesarios en la investigación

Para que todas las evidencias digitales obtenidas tengan validez jurídica es conveniente activar la cadena de custodia desde el primer momento garantizando que

- Se ha respetado la ley para obtenerlas
- La información es exactamente la que se recogió
- Durante su análisis no se ha modificado /creado / eliminado nada
- El análisis realizado es reproducible

De este modo se registra de manera exhaustiva toda la información con la mayor cantidad de detalles posible (anotaciones, grabaciones, fotografías) acerca de las acciones que se realizan sobre las evidencias

- Las fechas y horas en las que se realizaron
- Quien las manejaba
- Quien es el responsable de su custodia
- Donde se almacenaban

Es aconsejable

- La presencia de un notario que de fe de todo lo que se realiza
- Tomar fotografías que muestren su disposición configuración
- Usar programas sistema externos para realizar copias

En primer lugar, si el sistema informático sigue en marcha hay evitar que se sigan usando y recoger toda la información volátil

- Procesos en ejecución
- Archivos abiertos
- Claves del registro abiertas
- Versiones desencriptadas de datos
- Adjuntos de Email ,imágenes, fragmentos de chat
- Llaves criptográficas
- Contraseñas en texto plano
- usuarios conectados
- puertos abiertos

Identificación y análisis

Una vez recogida toda la información volátil se apaga el sistema y hace una copia bit a bit de toda la información no volátil que se va a analizar posteriormente

Deberemos tratar de obtener la mayor cantidad de información posible minimizando las alteraciones y su impacto, para ello es aconsejable

- Calcular y almacenar el resumen criptográfico del original y de la copia para asegurar que son idénticos
- Acceder a la información mediante el uso de **Write Blockers** que permiten la lectura pero evitan la escritura en disco
- Realizar un duplicado de la copia forense para evitar
  - Tener que trabajar con la copia original
  - Tener que volver a tocar el original

Principio de intercambio de Locard

"Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"

Principio de incertidumbre de Heisenberg

"El mero hecho de medir el estado de un sistema lo altera"

Analizar toda la información obtenida es una tarea tediosa

- Se usan muchos tipos de herramientas
- Hay que ser ordenado y meticuloso
- No se puede leer información confidencial que no esté relacionada con la investigación

Una técnica muy habitual es la búsqueda ciega en la que se realizan búsquedas por palabras clave solo se analiza la información donde figuran dichas palabras

- La intuición del analista es esencial

Conservación

Se deben evitar Pérdidas / Contaminación / Daño / Alteración / Manipulación

Para ello es conveniente

- Documentar exhaustivamente toda la información recogida
  - Etiquetar todos los dispositivos recogidos
  - Indicar marca, modelo, número de serie
  - Fecha, datos y firma de las personas que lo trasladen y manipulen
- Mantener las copias originales a buen recaudo Para ello se puede
  - Entregar una copia a todas las partes interesadas
  - Tener una copia de respaldo

Exposición

Se realiza un informe explicando todo el proceso y los resultados obtenidos

- Debe ser muy detallado reflejando todo el proceso
  - Situación que ha hecho necesaria la intervención
  - Las evidencias que se han recogido
  - Los procesos que se han seguido durante la recogida, duplicación, conservación
  - Las técnicas y herramientas usadas para analizar la información
  - Resultados obtenidos y conclusiones que pueden derivarse
- Deben estar explicados de forma que se pueda comprender por personas no técnicas
- Debe ser imparcial (sin reflejar opiniones ni suposiciones)

La validez jurídica de una evidencia digital la decide el juez

Un documento con una firma electrónica reconocida tiene validez jurídica

Todo un informe pericial puede ser desestimado si se ha violado alguna ley para realizarlo

En el caso de que haya un juicio el perito actuará en calidad de testigo y tendrá que explicar el informe que elaboró en su momento y responder a las preguntas de los abogados

- A veces se llama a declarar a un perito para que desmonte el informe de otro perito
  - Porque se rompió la cadena de custodia y las evidencias se pudieron alterar
  - Porque las conclusiones del informe no son directamente derivables de los resultados obtenidos
  - Porque aplicando técnicas distintas se obtienen resultados que contradicen los obtenidos en el informe