**2.1.1.- Seguridad lógica.**

La seguridad lógica agrupa los procedimientos existentes para controlar el acceso lógico no autorizado a la información, tanto si se intenta realizar mientras se encuentra almacenada como durante su transmisión.

* Restringir el acceso a los programas y archivos.
* Garantizar que todo usuario puede acceder a los datos o aplicaciones que necesita
* Asegurar que con cada información o dato con el que se trabaje se emplea el procedimiento adecuado y no alternativas no autorizadas.
* Que la información enviada solo sea recibida por el destinatario deseado y no por otro.
* Que la información recibida sea la misma que ha sido enviada.
* Que existan sistemas alternativos de almacenamiento y de transmisión.

**2.1.2.- Control lógico de acceso.**

* Cuál será el procedimiento por el que un usuario puede solicitar un permiso para el acceso a un activo de software.
* Como se decidirá si se le concede o no el acceso solicitado.

Los requisitos mínimos de seguridad de cualquier sistema son:

* **Identificación y autentificación:** todo usuario debe ser identificado antes de concederle el acceso mediante el proceso de autentificación.
* **Roles:** en función de su rol el usuario tendrá derecho o no a determinados servicios.
* **Transacciones:** para realizar operaciones delicadas es necesario utilizar un procedimiento de seguridad añadido.
* **Ubicación y horario:** restricciones de acceso en función de un horario, calendario o ciertas ubicaciones.
* **Control de acceso interno:** contraseñas, métodos cifrados, listas de control de acceso, etc.
* **Control de acceso externo:** mediante cortafuegos, pasarelas de comunicaciones, túneles, etc.

**2.1.3.- Listas de control de acceso.**

Conocidas como ACL, son un conjunto de reglas que utilizan los sistemas operativos o las aplicaciones para gestionar los permisos de acceso de los usuarios. Mediante las ACL se registra que usuarios tienen acceso a cada recurso del sistema.

* Leer un archivo.
* Escribir un archivo.
* Ejecutar un archivo.

**2.1.3.1.- ACL en Ubuntu.**

Las ACL extienden el esquema de permisos en Unix-Ubuntu POSIX.1.

Los archivos y directorios tienen conjuntos de permisos configurados para el propietario del archivo, el grupo al que pertenece el propietario y el resto de usuarios del sistema. Estos permisos básicos tienen limitaciones.

Ubuntu soporta, además de la máscara de permisos asignadas por umask, dos tipos básicos de ACL:

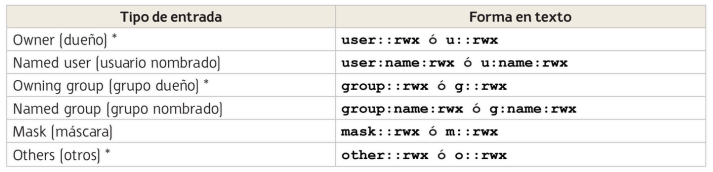
* **ACL estándar o mínima:** ACL de control de directorios y archivos. Contiene únicamente las entradas para los tipos propietario, grupo propietario y otros, que corresponden a los bits de permisos convencionales (POSIX) para archivos y directorios.
* **ACL extendida:** incluye además, una entrada de máscara, que puede contener al mismo tiempo distintas entradas de los tipos de usuario nombrado y grupo nombrado.

Además, las ACL se pueden configurar por usuario, por grupo y a través de la máscara de permisos.

En esencia, el permiso resultante surge de realizar la operación AND entre la negación de la máscara del usuario y los valores 666 para archivos y 777 para directorios.

Para trabajar con ACL debemos comprobar que:

* El núcleo del sistema operativo está compilado para soportar atributos extendidos y ACL.
* El sistema de archivos se monta con atributos extendidos y ACL.
* Se dispone de las utilidades para establecer el ACL: paquete ACL.



Las ACL que equivalen a los permisos POSIX se indican mediante \*.

**2.2.- Establecimiento de políticas de contraseña.**

Dentro de las políticas de seguridad de la organización se deben establecer cuantas normas sean necesarias para garantizar que las contraseñas sean seguras y robustas.

También se deben proveer políticas para el almacenamiento seguro de las contraseñas, sus períodos de caducidad y la concienciación a los usuarios para salvaguardar sus contraseñas.

*En general, las políticas de gestión de contraseñas indican:*

* Deben tener un tamaño mínimo de 8 caracteres.
* Deben tener caducidad, máximo 2 meses.
* Se debe tener en cuenta el número de intentos.
* Debe impedir que se repita la contraseña al cambiarla.
* Deben ser robustas: incluir, mayúsculas, minúsculas, números y caracteres no alfanuméricos.
* No deben ser fechas, nombres propios ni tener relación con el usuario.
* No deben encontrarse en ningún diccionario de lenguaje.

Con respecto a su almacenamiento, lo ideal es que el usuario tenga sus contraseñas en su memoria. En las grandes organizaciones, se suele utilizar una contraseña para realizar todas las tareas, a este técnica se le llama Single Sign-on (SSO).

Ahora se utiliza la autenticación multifactor, es decir, completar el uso de contraseña con algún otro factor de autenticación. **Por ejemplo:** *contraseña y confirmación al móvil*.

En Ubuntu, las contraseñas encriptadas se almacenan en /etc/shadow.

En Windows, las contraseñas están accesibles desde el Panel de Control → Administración de credenciales.

**2.2.1.- Ataque por diccionario.**

Mecanismo utilizado para intentar conocer una contraseña probando una lista contenida en un diccionario.

Los diccionarios suelen completarse con listas de contraseñas ya utilizadas que se han obtenido de alguna filtración o compra/venta.

Este tipo de ataque casi siempre es más eficiente que un ataque de fuerza bruta, pues muchos usuarios siguen usando contraseñas repetidas año tras año.

* Utilizar siempre contraseñas inventadas con mayúsculas, minúsculas, números y símbolos.
* Establecer un número máximo de intentos de acceso.

**2.2.- Ataque por fuerza bruta.**

Se prueban combinaciones de letras, números y caracteres especiales hasta encontrar la contraseña de acceso.

Para protegernos de ellos, es muy conveniente:

* Utilizar siempre contraseñas inventadas con mayúsculas, minúsculas, números y símbolos.
* Establecer un número máximo de intentos de acceso.
* Utilizar por costumbre contraseñas largas, mínimo 12 caracteres.

**2.3.- Criptografía: simétrica y asimétrica.**

La criptografía es la disciplina que engloba técnicas capaces de transformar datos legibles en datos no legibles y viceversa, mediante algoritmos matemáticos.

Los algoritmos transforman, mediante una clave, texto plano en texto cifrado (o al contrario) utilizado para transmitir o almacenar datos.

Es útil cuando una persona no autorizada consigue acceder a los datos, evitando que pueda llegar a entenderlos.

1. El precio de reventar la encriptación es más caro que el valor de la información.
2. El tiempo para reventar la encriptación es más largo que el tiempo de vida de la información.

Los procesos criptográficos pretenden dar solución a las siguientes necesidades:

1. **La privacidad:** la información solo puede ser leída por destinatarios autorizados.
2. **La integridad:** la información no puede ser alterada sin que el destinatario lo advierta.
3. **La autenticidad:** garantía de que la información procede de quien afirma haberla mandado.
4. **El no repudio:** si un emisor envió información, no puede negar ser autor del mismo.

**2.3.1.- Tipos de criptosistemas.**

Tenemos dos sistemas de encriptación: la simétrica o clave privada y la asimétrica o clave pública. Garantizan principalmente la privacidad, la autenticidad y el no repudio.

Los dos sistemas presentan algoritmos para codificar los mensajes. Tanto para codificar como para decodificar utilizan claves que solo deben ser conocidas por los usuarios involucrados en la comunicación.

Debido a que los algoritmos son de dominio público, es esencial garantizar la complejidad y privacidad de las claves, tanto a nivel de emisor como del receptor.

Una medida que se utiliza muy frecuentemente para indicar el nivel de seguridad de la clave es el número de bits utilizados para generarla. A mayor número de bits, mayor seguridad pero menor velocidad de cifrado.

En la práctica se suele utilizar los dos tipos combinados. Los mensajes se codifican mediante algoritmos simétricos, que suelen ser muy eficientes, y las claves simétricas se codifican mediante criptografía asimétrica, que es mucho más costosa computacionalmente.

Es importante también tener en cuenta las funciones hash garantizan esencialmente la integridad de los mensajes.

**2.3.1.1.- Criptografía simétrica.**

Se basa en el siguiente criterio: un mensaje lo ciframos con un algoritmo empleando una clave y podemos descifrarlo utilizando la misma clave. La clave debe comunicarse al receptor para que pueda descifrar el mensaje.

Dado que la clave debe ser conocida tanto por el emisor como por el receptor, se le llama *clave simétrica*. Al utilizarse una sola clave, también es conocida como *clave única* o *clave privada*.

**Ventajas:**

* Es simple, rápida y eficiente.
* Las claves deben tener más de 40 bits.

**Desventajas:**

* Distribución de las claves.
* Dificultad de almacenar y proteger muchas claves diferentes, pues cada par de usuarios debe tener su propia clave secreta particular.

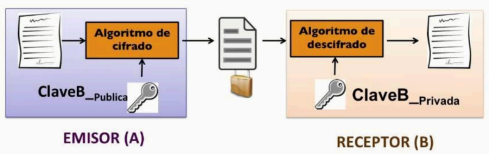
*La criptografía simétrica puede ser:*

* De bloques (block cipher). El texto plano se cifra en bloques de tamaño fijo.
* De flujo (stream cipher).

**2.3.1.2.- Criptografía asimétrica**.

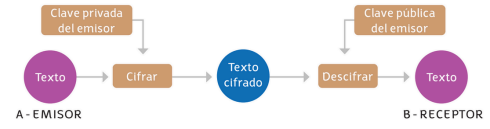
* **Pública:** es conocida por el emisor y el receptor del mensaje.
* **Privada:** cada emisor y receptor de mensajes tiene su propia clave privada, conocida sólo por ellos mismos.

El funcionamiento básico, que garantiza la *privacidad* del mensaje, de un EMISOR A a un RECEPTOR B es el siguiente:



* El EMISOR (A) cifra el mensaje en base a la clave pública del RECEPTOR (B).
* Se transmite el mensaje.
* El RECEPTOR (B) descifra el mensaje utilizando su clave privada.

Si queremos garantizar la *autenticidad* y el *no repudio*, perdiendo seguridad en la privacidad, el proceso sería el siguiente:



* El A-EMISOR cifra el mensaje en base a su clave privada.
* Se transmite el mensaje.
* El B-RECEPTOR descifra el mensaje utilizando la clave pública del A-EMISOR

Si deseamos guardar la *privacidad, la autenticidad* y el *no repudio*, se combinan los dos casos anteriores:

* A envía a B un mensaje codificado dos veces, primero con la clave pública de B y después con la clave privada de A.
* B decodifica el primer mensaje con la clave privada de B (privacidad) y el segundo con la clave pública de A (autenticidad y no repudio).

Mediante la criptografía asimétrica se evita la administración del gran número de claves secretas de la simétrica, pero presenta la desventaja de requerir un proceso para asegurar que las claves públicas son auténticas y pertenecen al usuario correspondiente.

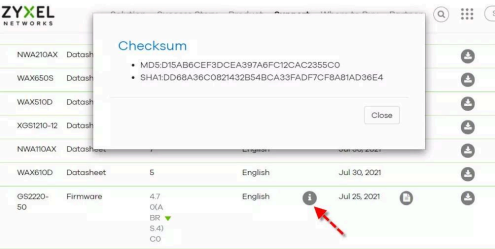
Las CA se encargan de certificar que una clave pública pertenece al usuario u organización válida y de la distribución de estas, emitiendo los certificados digitales de las claves públicas.

Además de la desventaja anterior, el cifrado de un mensaje es mil veces más lento que con el algoritmo de clave simétrica, agravando el problema cuando utilizamos grandes cantidades de información en los mensajes.

**2.3.1.3.- Funciones hash.**

Llamadas también funciones resumen o unidireccionales, pues son prácticamente imposibles de invertir.

No utilizan clave, utilizan la llamada huella digital, fingerprint, resumen o hash. Actualmente se está utilizando el término checksum para indicarnos un hash que podemos comprobar.



Utilizan un algoritmo matemático para obtener un código alfanumérico (hash) de longitud fija a partir de un conjunto de datos: mensaje, fichero, documento, imagen, etc.

Si aplicamos el algoritmo sobre unos datos en varias ocasiones, siempre vamos a obtener el mismo hash. **Una modificación generaría un hash distinto al obtenido por el documento original.**

Por norma general, los hash son representados en hexadecimal.

El código alfanumérico no se puede considerar texto cifrado, pues no existe ningún proceso inverso que aplicado sobre el devuelvan los datos originales.

* El emisor obtiene el hash de los datos que desea enviar a un receptor.
* El emisor envía al receptor los datos y el hash obtenido.
* El receptor genera el hash de los datos que ha recibido.
* El receptor compara ese hash con el enviado por el emisor.
* Si los dos hash son iguales, los datos no han sido modificados durante la transmisión.
* Si los hash son distintos, existe la plena seguridad que se han modificado los datos durante la transmisión.

Como ejemplo de utilización real podemos destacar: *descarga de ficheros de servidores, documento firmado digitalmente, etc.*

**2.4.- Firma digital. Certificados digitales.**

Su objetivo es garantizar la identidad del firmante y la del mensaje respecto a la firma digital y, con las autoridades de certificación, tener la certeza de que la clave pública utilizada es de quien dice ser su propietario, mediante la emisión de certificados digitales.

**2.4.1.- Identidad digital.**

Conjunto de elementos que garantizan la identidad a través de medios electrónicos.

El anonimato en Internet y las posibilidades de fraude limitan las operaciones comerciales y el no repudio, que en los procesos judiciales supone un inconveniente importante.

La identidad digital se plasma a efectos prácticos mediante la firma electrónica.

1. **La firma electrónica simple:**

*Consiste en marcar una casilla o introducir un código PIN o contraseña.*

Su valor legal depende de pruebas complementarias, pues no permite identificar al usuario.

**Por ejemplo:** *firmar condiciones generales de una web, transacciones bancarias simples….*

1. **La firma electrónica avanzada:**

*Permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados.*

Asegura la identidad -no la autenticidad- y la integridad. Requiere el uso de certificados digitales de identificación del firmante. Tiene plena validez legal.

**Por ejemplo:** *firmar facturas digitales, consentimiento informado, emails, gestiones con la administración pública de carácter general, etc.*

1. **La firma electrónica cualificada:**

Basada en un certificado digital y en el uso de un dispositivo seguro de creación de firma cualificado, como por ejemplo el DNIe. El DNIe tiene que ser leído por el lector físico de DNIe o un dispositivo con NFC que cumpla el estándar ISO 14443.

Asegura la autenticidad, la integridad y el no repudio. Tiene el mismo valor legal que la firma manuscrita, por lo que su anulación por alguna de las partes involucradas es prácticamente

imposible.

**Por ejemplo:** contratos, pólizas de seguros, gestiones bancarias importantes.

**2.4.1.1.- Tarjetas.**

* Se autoriza a la tarjeta con independencia de quien la tenga.
* Se pueden falsificar.
* Para mayor seguridad, puede ir acompañada de un código o contraseña.

Podemos encontrarnos con los siguientes tipos de tarjetas:

* **Sin contacto:** usan la tecnología RFID o NFC que permiten transmitir la identidad mediante ondas de radio.
* **Con contacto:** llevan una serie de contactos metálicos dorados conectados a un chip de silicio. Para su lectura tienen que ser insertadas en un lector para lograr el contacto físico con él.

**Por ejemplo:** *el DNI electrónico hace uso de la firma electrónica cualificada, las smartcards o tarjetas inteligentes que almacenan un certificado digital de identificación posibilitan la firma electrónica avanzada, las tarjetas bancarias (débito o crédito) normalmente se basan en la firma electrónica simple.*

**2.4.1.2.- Firma digital.**

Conjunto de datos asociados a un mensaje que permiten asegurar la identidad del firmante -ojo, no la autenticidad- y la integridad del mensaje.

Para producir una firma digital necesitamos algo relacionado de forma única con el firmante.

Si deseamos garantizar además la privacidad durante la firma electrónica, tendremos que codificar todo el mensaje durante su emisión y no solo su hash.

1. Durante la emisión se genera el hash en base al mensaje a enviar.
2. El emisor encripta el hash con su clave privada, añadiendo el hash cifrado al mensaje original. A éste hash cifrado se le llama firma digital.
3. El receptor, al recibir el mensaje, calcula de nuevo el hash del mensaje recibido.
4. El receptor desencripta, mediante la clave pública del emisor, la firma digital
5. El receptor compara el hash enviado por el emisor con su propio hash obtenido. Si ambos hash coinciden, se garantiza la autenticidad del firmante y la integridad del mensaje recibido.

**2.4.2.- Certificados digitales.**

Es un documento digital mediante el cual un tercero confiable garantiza la correspondencia entre la identidad de un sujeto, entidad u organización y una clave pública.

La certificación de claves públicas requieren una conexión segura en el navegador (https-normalmente el dibujo de un candado cerrado).

Una **PKI** engloba el software y hardware junto con los usuarios, políticas y procedimientos que permiten la creación y gestión de certificados digitales basados en criptografía asimétrica.

La PKI consta de:

* **Autoridades de certificación (CA).** Emiten y revocan los certificados digitales.
* **Autoridades de registro (RA).** Verifican la identidad de los usuarios o entidades que solicitan un certificado digital.
* **Autoridades de repositorios (directorios).** Almacenan los certificados emitidos, caducados y revocados.
* **Titulares de certificados**. Usuarios o entidades que poseen certificados digitales.
* **Autoridades de validación (opcional).** Suministran información en tiempo real de forma online del estado de un certificado digital.

La distribución del certificado digital siguiendo el estándar X.509 es posible realizarla:

* *Con clave privada en formato \*.pfx o \*.p12.*
* *Con clave pública en formato \*.cer o \*.crt.*

**2.5.- Sistemas biométricos de identificación.**

La biometría se basa en el reconocimiento automático de los individuos en función de sus características biológicas y de comportamiento.

* **Biometría conductual.** Se basa en medidas de las acciones de una persona tales como hábitos de uso, conducta y comportamiento. Las más importantes son la forma de uso de un teclado y la forma de realizar la firma manuscrita de una persona.
* **Biometría fisiológica.** Se basa en medidas de partes del cuerpo humano, como por ejemplo, huellas dactilares, iris, el rostro, etc.

**2.5.1.- Sistemas biométricos actuales.**

1. Reconocimiento del rostro.
2. Termograma del rostro.
3. Huellas dactilares.
4. Geometría de la mano.
5. Venas de la mano.
6. Lectura del iris.
7. Patrones de la retina.
8. Reconocimiento de voz.
9. Reconocimiento de firma.

Las técnicas que se consideran más efectivas son, lectura del iris y patrones de la retina.

En muchas ocasiones se combinan varios de estos indicadores biométricos dando lugar a la biometría Multi-Modal.

El funcionamiento de los sistemas de autenticación biométrica es el siguiente: *captura, extracción de datos relevantes, comparación con la información almacenada, comprobación de la identidad.*

* Sistemas caros pero robustos
* Suelen utilizarse como control de acceso de alta seguridad.
* El temor a identificarse con partes del cuerpo influye todavía bastante.
* Mis acciones pueden ser cambiadas, aunque requieren un gran esfuerzo. Las partes del cuerpo no pueden ser cambiadas mediante métodos sencillos. Las claves pueden ser cambiadas fácilmente.
* Muy aceptada al principio de su implantación, actualmente está en completa revisión legal.

**2.6.- Análisis forense en sistemas informáticos.**

Su objetivo es realizar un análisis una vez se ha materializado una amenaza en el sistema informático. Por lo tanto, el análisis forense informático permite:

* Analizar las consecuencias que se han producido.
* Averiguar quien ha sido el autor.
* Conocer las causas y metodología empleada.
* Detectar las debilidades.

El resultado del análisis forense puede ser aceptado legalmente en un proceso judicial.

Por su complejidad, el análisis forense requiere formación interdisciplinar: *derecho, criminalista, psicología, seguridad informática.*

1. Identificación del incidente.
2. Captura de las evidencias.
3. Preservación de las evidencias.
4. Análisis de la información obtenida.
5. Elaboración de las conclusiones.

El análisis forense informático siempre está presente en:

* Delitos en los que se actúa contra el equipamiento informático.
* Delitos en los que los equipos informáticos contienen las evidencias.
* Delitos en los que los equipos informáticos son utilizados para cometer el crimen.

En España, las unidades de las fuerzas de seguridad dedicadas al análisis forense son:

* Brigada Central de Investigación Tecnológica del CNP.
* Grupo de Delitos Telemáticos de la Guardia Civil.

**2.6.1.- Incidente de seguridad informática. Evidencia digital.**

Un incidente de seguridad informática puede considerarse como una violación o intento de violación de la política de seguridad.

Se debe tener registro de todos los incidentes de seguridad sufridos por la organización, de manera que de su análisis se puedan extraer conclusiones que permitan deducir si han sido

provocados de forma voluntaria o no.

Con respecto a la evidencia digital, se define como el conjunto de datos en formato binario, como ficheros o su referencia a estos, que se encuentren en los soportes físicos o procesos lógicos del sistema atacado.

La evidencia digital es la base del análisis forense informático y por ello debe ser preservada en su estado original.

Actualmente, la referencia para el análisis digital forense es la norma ISO/IEC 27037:2016, que proporciona pautas para el manejo de la evidencia digital.