Seguridad en el sistema

En este tema estudiaremos algunos aspectos relacionados con los sistemas que no han sido cubiertos en temas anteriores.

[Particiones y seguridad en el sector de arranque](#h.at2krvvr4yfy)

[Contraseña para el programa de configuración del BIOS y el orden de arranque de los dispositivos](#h.76qukvtxrymg)

[Seguridad en el gestor de arranque.](#h.dpqjcetintfc)

[Mecanismos de control de acceso.](#h.vh9jyh1i1ics)

[Saber algo: PINes y contraseñas](#h.kjl6q5tixzy3)

[Poseer algo: Tarjetas, llaveros...](#h.lawka9l159nt)

[Tarjetas magnéticas](#h.ymheqbklpgjk)

[Tarjetas con marcas ópticas.](#h.nwyo7cng50ho)

[Dispositivos RFID (IDentificación por Radio Frecuencia)](#h.gn4cfh2h3vue)

[Smartcard RFID](#h.j4b428247l2h)

[Exhibir una característica física: Biometría](#h.5ux65hf4uut)

[Huella Dactilar](#h.r6q3ssnosdtl)

[Iris](#h.8y2kfo4fbdue)

[Retina](#h.mgvketp843eb)

[Venografía](#h.x6jbmbramza7)

[Rostro](#h.1n3w86lxautn)

[Firma](#h.1gpwozg3hdra)

[Voz](#h.1vu3nfm4bdoi)

[Listas de control de acceso (ACLs)](#h.3h21gg7lv2mk)

[Cuotas de disco.](#h.x9wlhlxvhs9r)

[Auditorías del sistema operativo.](#h.7crbn2kpse9i)

# Particiones y seguridad en el sector de arranque

El espacio de las unidades de disco duro (HDD) puede ser dividido en varias *particiones* por el sistema operativo.

Un disco duro es una gran tira de sectores de 512 bytes cada uno. El hecho de que ese espacio de almacenamiento se parta es cosa de los sistemas operativos. Las particiones tienen muy poco que ver con el hardware.

La historieta de la tabla de particiones viene del sistema operativo PC-DOS de IBM (el que luego sería MS-DOS) y particionar los discos duros fue una ocurrencia de cuando éstos tenían unos pocos “megas” de capacidad. El sistema ha sido poco revisado e 20 años... y permanece prácticamente igual... solo que ahora utilizamos discos con mil veces más capacidad que hace 20 años.

En cierta medida, el sistema actual de tabla de particiones está bastante desfasado y va siendo sustituido por otro llamado GPT (Global Partition Table), más sofisticado, extensible... implementado por los principales sistemas operativos...

Pero mientras tanto, la tabla de particiones nos ha dejado una importante vulnerabilidad de los sistemas.

La fórmula de la tabla de particiones se utiliza también en otros dispositivos que son *vistos* por el sistema de manera similar a un HDD:

* Pendrives y tarjetas de memoria flash
* Discos de estado sólido (SSD)

No se encuentra en disquetes ni en dispositivos ópticos.

El sector 0 de un HDD se denomina MBR (Master Boot Record), y contiene en su interior:

* Un pequeño programa de arranque que empieza en el byte 0 del sector, al principio.
* La *Tabla de Particiones*, al final del sector. Una tabla que indica dónde comieza y la longitud de cada partición.

La tabla sólo tiene espacio para almacenar 4 particiones. Así que en sólo 4 partes como máximo puede dividirse un disco (Es lo que se llaman **particiones primarias...** sólo hay cuatro como máximo). Más tarde en la historia, a Microsoft se le ocurrió una forma de *partir* de nuevo una de estas particiones primarias, para obtener, a su vez, más partes (una partición primaria dividida pasa a llamase ***partición extendida*,** y sus partes se denominan ***particiones lógicas***)

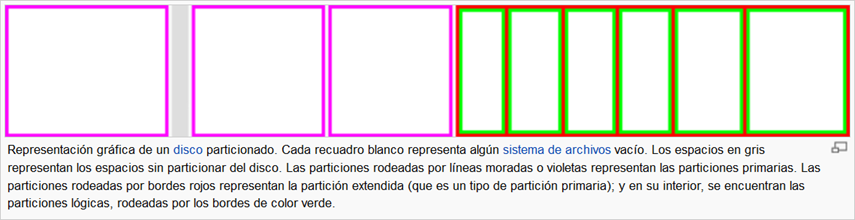
Las particiones primarias **no extendidas** pueden contener un sistema operativo, o un gestor de arranque... en la terminología se dice que son **particiones activas o arrancables**.

Cada partición arrancable tiene [un bit activado que lo indica](http://es.wikipedia.org/wiki/Tabla_de_particiones).

Cuando un ordenador arranca, hay una utilidad grabada en el *firmware* de la placa base encargada de poner todo el sistema en marcha: se trata del BIOS (Basic Input-Output Services). El BIOS pondrá en marcha el hardware comprobando su integridad básica, y luego, cargará el MBR del primer dispositivo que tenga programado en la memoria principal.

Luego, pasará el control de la CPU a ese programa.

Ese programa de arranque del MBR revisará la tabla de particiones, y buscará la primera partición marcada como arrancable.... Localiza entonces el primer sector de dicha partición (el sector de arranque de la partición) y lo carga en memoria y le pasa el control de la CPU, poniéndose en marcha el sistema operativo o gestor de arranque que haya en esa partición.



# Contraseña para el programa de configuración del BIOS y el orden de arranque de los dispositivos

El BIOS (Basic Input/Output Services es software grabado en ROM en la placa base, y encargado de inicializar el ordenador, los componentes hardware y un sistema operativo). Ya sabemos que el BIOS cuenta con una utilidad de configuración, que se puede activar durante el arranque.

Ese programa de configuración del BIOS puede ser protegido por una contraseña, para que no pueda alterarse por cualquiera.

Con esto se logra proteger, entre otras cosas, **el orden de búsqueda de una partición arrancable** entre varios dispositivos.

El BIOS buscará un sector de arranque entre los dispositivos de memoria secundaria, en el orden en que se especifique en el programa de configuración.

**En ordenadores servidores o con información delicada, es necesario establecer como primer dispositivo de arranque el del disco duro que contenga el sistema operativo.**

**Un usuario que arranque con un sistema operativo desde una unidad extraíble puede.**

* **Acceder a datos de los volúmenes**
* **Realizar cambios en la información o el sistema (tales como introducir spyware o rootkits)**

**Un dispositivo extraíble que contenga malware en su MBR puede**

* **traspasarlo al sector de arranque del disco de arranque.**

Pasos 1:

|  |  |
| --- | --- |
|  | 1.- Establecer el orden de los dispositivos de arranque |
|  | 2.- Establecer una contraseña, para evitar que alguien pueda cambiarlo. |
|  | 3.- Aunque parezca una tontería, colocar un candado para evitar el acceso físico al interior del ordenador, para evitar que alguien haga un reset de la configuración del BIOS, mediante un jumper o pulsador en la placa. |

# Seguridad en el gestor de arranque.

Un gestor de arranque es un programa que se aloja en una partición primaria, y su cometido es arrancar otros sistemas operativos en otras particiones.

Los gestores de arranque son sofisticados, y *conocen* las interioridades y el funcionamiento de los sistemas operativos.

Uno de los más conocidos es GRUB ([*GNU GRand Unified Bootloader*](http://es.wikipedia.org/wiki/GNU_GRUB)*)* , ya que se utiliza habitualmente para el arranque de sistemas operativos Linux.

Los gestores de arranque permiten algunas configuraciones en los sistemas operativos que arrancan, y eso puede suponer vulnerabilidades de seguridad una vez arrancado el sistema.

Un posible atacante que manipule la forma en que GRUB u otro gestor arranca un sistema podría facilitarle una posible intrusión o manipulación en el equipo.

Por ejemplo, es conocido que los sistemas Linux pueden arrancar en el llamado ***modo monousuario*,** también conocido como  ***modo rescate***, en el cual, podría ser posible utilizar un usuario *root* sin contraseña.

Manipulando el gestor de arranque puede lograrse arrancar un sistema linux en este modo.

Así pues, en sistemas con información sensible y que tengan un gestor de arranque, es conveniente **poner una contraseña para poder manipular la configuración del gestor de arranque.**

[Ejemplo: [poner una contraseña en GRUB, de la Guía Ubuntu](http://www.guia-ubuntu.org/index.php?title=GRUB#Proteger_con_contrase.C3.B1a)]

# Mecanismos de control de acceso.

Ya hemos comentado que los mecanismos de seguridad para control de acceso de una persona frente a un sistema caen generalmente en tres grandes grupos:

* Saber algo
* Poseer algo
* Exhibir alguna característica física intransferible.

Estos mecanismos pueden combinarse de muchas maneras, y pueden ayudar a realizar estas propiedades seguras:

* **Identificación**
* **Autenticación**

Haremos un breve repaso de algunas de las tecnologías que existen.

Se utilizan tanto para el control de acceso físico (el acceso de las personas a un **lugar**), como para el acceso lógico (ej: iniciar sesión en el sistema operativo, dejar constancia de la presencia en un sistema, firmar digitalmente una información, etc, etc).

## Saber algo: PINes y contraseñas

**PIN** significa Personal Identification Number... es una forma sencilla de contraseña: sólo números. Simplifican los teclados en los accesos. Suelen tener entre 4 y 6 dígitos (está demostrado que nos cuesta mucho recordar números de 8 o más cifras). Casi siempre se combinan con otros sistemas.

Las contraseñas que combinan también letras y signos requieren un teclado de ordenador.

Suelen tener una longitud mucho más grande, y ya sabes que es conveniente elegir contraseñas que

* Combinen mayúsculas y minúsculas
* Incluyan algún dígito y signos de puntación
* Tengan un mínimo de 10 carácteres
* Eviten incluir datos que puedan ser deducibles por ingeniería social (ej: nombre de mascotas/hijos/lugares... fechas de nacimiento/matrimonio/etc.)

|  |  |
| --- | --- |
| Ventajas:   * Económico * Sencillo * Fáciles de entender | Inconvenientes:   * Se puede olvidar * Se puede “prestar” |

## Poseer algo: Tarjetas, llaveros...

Hay una larga lista de distintivos que se pueden llevar encima. Algunos simplemente sirven para identificar, otros, más seguros, permiten autenticar.

Suelen combinarse con algún pin o contraseña.

### Tarjetas magnéticas



Siguen un estándar ISO[[1]](#footnote-1) Tienen una banda magnética, que en realidad está dividida en tres areas, en la que se graban los datos a distinta densidad magnética[[2]](#footnote-2). En total apenas caben unos 80 carácteres y unos pocos números.

La Pista magnética puede estar integrada en el plástico o pegada. Debe poder soportar abrasión (roce) Son, simplemente memoria (y no mucha, como puedes ver): se graban y leen con un lector magnético estándar. La polarización de las moléculas de un área determinan un bit a 1 o a 0. En la tarjeta no cabe mucho más que algunos datos de identificación y algunos códigos de redundancia para evitar errores de lectura.

|  |  |
| --- | --- |
| Ventajas:   * Sencillas de leer y escribir * Baratas | Inconvenientes   * Se pueden perder, robar… * Se duplican con facilidad * Son sensibles a campos electromagnéticos, que las van degradando * Se puede “prestar” |

**Tarjetas inteligentes SmartCard**



Tienen un circuito integrado, responden a varios estándares ISO. Su utilización es muy variada. Con respecto a la seguridad, incluye identificación, autenticación, control de acceso, criptografía y firma electrónica. También se utiliza en banca, transacciones electrónicas, compra/venta...

Básicamente existen de tres tipos

* Las más sencillas, **son simplemente un dispositivo de memoria secundaria**: tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. Éstas se usan generalmente en aplicaciones de identificación y control de acceso sin altos requisitos de seguridad, también para prepago de servicios.
* **Microprocesadas**: tarjetas con una estructura análoga a la de un ordenador (procesador, memoria principal (rom), memoria secundaria(ram) ). Éstas albergan ficheros y aplicaciones y suelen usarse para identificación y pago en banca.
* **Criptográficas**: tarjetas microprocesadas avanzadas en las que hay módulos hardware para la ejecución de algoritmos usados en cifrados y firmas digitales. En estas tarjetas se puede almacenar de forma segura un certificado digital (y su clave privada) y firmar documentos o autenticarse con la tarjeta sin que el certificado salga de la tarjeta (sin que se instale en el almacén de certificados de un navegador web, por ejemplo) ya que es el procesador de la propia tarjeta el que realiza la firma. Un ejemplo de estas tarjetas es el **DNIe.**

Las tarjetas criptográficas y microprocesadas se entregan a los clientes (La Policía Nacional, los bancos, las empresas) ya programadas, en el estado denominado ***prepersonalización***. En su chip se instala un sistema operativo, un pequeño sistema de ficheros y una aplicación que es capaz de aceptar sólo las órdenes para las que fue programada. Una vez *personalizada* la tarjeta -cosa que se realiza a través de la propia aplicación instalada en la tarjeta-, éstas no suelen admitir cambios en el titular de la tarjeta, con lo cual, la aplicación no puede personalizarse para otra persona.

Tienen una serie de tamaños normalizados, pero los más conocidos son los del tamaño de una tarjeta de crédito y los del tamaño de una tarjeta SIM de telefonía Móvil.



Con respecto a la seguridad tienen mucha más utilidad que las tarjetas magnéticas.

[más: [Tarjetas inteligentes en wikipedia](http://es.wikipedia.org/wiki/Tarjeta_inteligente)]

### Tarjetas con marcas ópticas.



Los códigos ópticos **de una dimensión** se utilizan en la industria para identificar mercancía desde los años 80. Estamos muy acostumbrados a ellos, ya que los vemos habitualmente en productos comunes.

Hay varios estándares, pero todos ellos fueron ideados para su lectura con un dispositivo laser. La luz láser se refleja de manera distinta en la tinta negra que en el papel blanco. El lector de códigos de barra lanza un haz de luz láser, y observa y analiza el reflejo de la luz para “leer” los números que el código representa.

Los códigos opticos **de dos dimensiones** se empezaron a diseñar en los años 90, pero en la década del 2000 es cuando tuvieron aplicación real. Son códigos pensados para ser captados por una cámara normal (incluso “barata”, como las de los móviles), que toma una imagen en formato digital. Luego, un software de análisis de imagen puede extraer los datos de la foto.

La ventaja es que dispositivos móviles, como teléfonos, smartphones y PDAs pueden leer estos códigos, sin necesidad de recurrir a lectores láser.   
Además, **pueden almacenar mucha más información, incuso alfanumérica.**

Quizá, los más populares de los bidimensionales sean los códigos QR, como el que ves en la imagen, capaz de almacenar más de 4000 carácteres alfanuméricos, y ser leído con una aplicación de teléfono móvil. (Ej: [Barcode Scanner](https://play.google.com/store/apps/details?id=com.google.zxing.client.android) para Android)



Con respecto a las tarjetas magnéticas, son mucho más baratas, y se pueden duplicar todavía más fácilmente. Así pues, sólo valen para identificación.

[más: [códigos de barras en wikipedia](http://es.wikipedia.org/wiki/Codigo_de_barras)]

|  |  |
| --- | --- |
| Ventajas:   * Barato. Se puede incluso construir de manera casera * En el caso de los bidimensionales, cabe mucha información * El hardware es relativamente barato. En los unidimensionales también es barato, aunque no es tan *trasnportable* | Inconvenientes:   * Se puede “prestar”, robar, etc. * Muy fácil de duplicar * En los unidimensionales, cabe poca información |

### Dispositivos RFID (IDentificación por Radio Frecuencia)

Son dispositivos que permiten almacenar y recuperar pequeñas cantidades de datos de manera inalámbrica. Se basan en un pequeño chip que almacena esos datos y que, ante la presencia de una determinada señal procedente de un lector los emite, mediante señales de radio para que puedan ser leídos en su entorno inmediato.

Los chips son relativamente pequeños, lo cual hace que puedan ser insertados en dispositivos tales como relojes, llaveros, etiquetas… además de tarjetas de plástico.

Es también la tecnología que se utiliza para identificar animales mediante una cápsula subcutánea. Al conjunto del chip RFID con su antena se le suele llamar **etiqueta RFID (tag RFID)** o Transpondedor RFID.



En la imagen de arriba: diversos ejemplos de etiquetas RFID: las dos primeras tienen realmente forma de etiqueta, y puede observarse fácilmente la antena, que sirve tanto para recibir energía que pone en marcha el chip como para “responder” con el identificador numérico grabado en el chip. Sirven para identificación de mercancía, pero el mismo tipo de antena y chip incuido en una tarjeta plástica del tamaño de una tarjeta de crédito puede servir para identificación de personas.

Los relojes del ejemplo son para identificación de personas. Tienen la antera en la correa.

El cuarto ejemplo es una etiqueta con forma de pequeño botón en un encapsulado cerámico, que puede insertarse en abalorios, como llaveros, colgantes, pulseras...  
El quinto ejemplo es una cápsula subcutánea para identificación de mascotas.

Este tipo de etiquetas no necesita energía (batería). La toman prestada del lector, que la emite en forma de pulso electromagnético. Se denominan **tags pasivos**. Necesitan estar en un rango relativamente cercano al lector... o bien que el lector sea muy grande, y pueda proporcionar energía a bastantes centímetros de distancia.

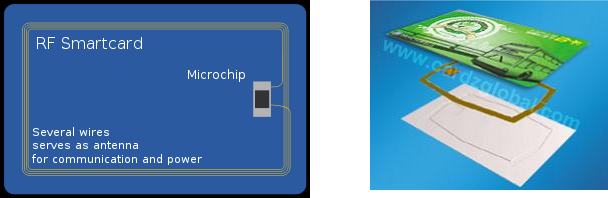
Existen también los tag RFID activos, que son menos comunes y más caros y voluminosos: llevan una pequeña batería para ayudarlos. Son más fiables –hay menos errores de lectura con ellos- y alcanzan rangos de lectura de varios metros.



|  |  |
| --- | --- |
| Ventajas:   * Comodidad: no es necesario sacar nada. Basta entrar en el ámbito del lector para que pueda detectar el chip y leer su información. | Inconvenientes:   * Se puede “prestar”, robar, etc. * No es fácil de duplicar, pero tampoco muy difícil. * Los tags pasivos suelen tener una tasa incómoda de errores de lectura * Hay varios estándares en competencia * No cabe mucha información en el chip: unos pocos bytes, lo justo para emitir un número o una cadena identificadora. |

### Smartcard RFID

Por último, comentar que existe una tecnología que combina en una tarjeta de tamaño normalizado un chip SmartCard con una antena RFID. De esta manera, una tarjeta SmartCard -mucho más segura- puede interactuar con un lector sin necesidad de *insertarla* físicamente en ningún sitio.



No llevan un chip sencillo RFID, sino que utilizan una antena como la de RFID para captar energía, que activa el microprocesador de la SmartCard. Se basan en un estándar internacional ISO/IEC 14443 En aplicaciones de autenticación suelen utilizarse junto con una clave privada asimétrica o una clave secreta simétrica compartida que se mantiene en el interior de la tarjeta, y protegida por un PIN. La identidad se verifica mediante desafío/respuesta.

[más: [en la wikipedia, sólo en inglés](http://en.wikipedia.org/wiki/Contactless_smart_card)]

## Exhibir una característica física: Biometría

La biometría es el estudio de los métodos que permiten reconocer a un ser humano.

En las TI, utilizamos rasgos físicos o de comportamiento para identificar a las personas.

Los sistemas biométricos pueden contribuir principalmente a

* La **identificación** y **autenticación** de las personas

De manera colateral, y combinándolos con diversas técnicas, se pueden utilizar también para

* El **no repudio** de la información
* El **control del acceso**
* El mantenimiento de la **confidencialidad**.

Frente a los sistemas basados en saber algo o poseer algo, en biometría, se aprovecha el hecho de que existen una **característica personal**, que siempre se lleva encima y no es posible olvidarla o transferirla.

A esas características se les denomina **indicadores biométricos** (por ejemplo, la huella digital es uno), pero deben cumplir algunas propiedades…

Para que un control de acceso en biometría sea fiable, el indicador biométrico utilizado debe tener algunas características:

* **Universalidad**: Todo el mundo debe tener ese indicador
* **Unicidad:** El indicador es distinto en cada persona
* **Permanencia:** No cambia con el tiempo, ni a corto ni a largo plazo
* **Cuantificación:** debe poder ser representado mediante modelos numéricos, para que un sistema digital pueda utilizarlo.

Además de exigir características al propio indicador, el **sistema biométrico** también debe reunir algunas:

* **Efectividad:** Debe ser cómodo y rápido para los usuarios
* **Aceptabilidad:** No debe provocar rechazo en su uso ni ser peligroso para la salud.
* **Fiabilidad:** Los resultados han de ser fiables, con poca probabilidad de ser trucado o utilizado fraudulentamente.

Los sistemas biométricos funcionan en base a la recopilación de muestras estadísticas del indicador que utilicen para todas las personas que el sistema deba identificar. Por ejemplo un sistema basado en huellas dactilares (el indicador) debe recoger al menos una muestra del indicador de cada persona que el sistema tenga que identificar, y la guarda en una base de datos.   
La muestra se almacena como un modelo numérico que representa al indicador, junto con la identidad de la persona a la que pertenece (su nombre, o un identificador).

En un momento posterior, cuando es necesario identificar a una persona, se toma de nuevo una muestra, que es comparada con las muestras almacenadas, y el sistema determina la **probabilidad** de que la muestra recién tomada corresponda a cada una de las personas de las cuales se almacenan las muestras.

Los sistemas de calidad se pueden **calibrar.** Es decir, configurar para aceptar a una persona en determinadas condiciones o rechazarla en otras.

Un sistema biométrico no es infalible. Como ya hemos visto, en basa en mediciones, modelos numéricos y probabilidades.

Por ello, el sistema puede dar lugar a

* **Falsas aceptaciones**: Cuando se acepta a una persona que NO es.
* **Falsos rechazos**. Cuando se rechaza a una persona que SÍ es.

Así pues, es conveniente calibrar el sistema para intentar determinar el llamado **PUNTO DE EQUILIBRIO**

El punto de equilibro es aquel en el que se minimizan las falsas aceptaciones y el falso rechazo.



Cuanta mas exigencia se le pone al sistema (se exige alta probabilidad de concordancia entre la muestra recien tomada y la almacenada) mayores son los falsos rechazos.

Cuanta menos exigencia se le pone al sistema (se exige menos concordancia entre la muestra recien tomada y la almacenada) mayores son las falsas aceptaciones.

Una falsa aceptación es más peligrosa que un falso rechazo, porque podría dejar pasar a alguien no autorizado.

Los fabricantes de sistemas biométricos sólo dan por bueno y seguro el calibrado de un sistema si se cumple simultáneamente que

* La tasa de Falsas aceptaciones<0,1%  
  (menos de 1 entre 1000)
* La tasa de Falsos rechazos<2%  
  (menos de 1 entre 50)

Vamos a dar un pequeño repaso a los indicadores más conocidos, comentando sus características básicas.

|  |  |
| --- | --- |
| Huella Dactilar Se basan en la suposición de que los surcos que conforman las huellas dactilares de cada individuo son únicas. A partir de ellas se pueden obtener mediciones que lleven a la identificación o verificación de una persona  Se utiliza un escáner de luz visible para obtener las huellas.  Es el indicador más conocido y tiene muchos años de estudio. Los sistemas buenos son relativamente fiables, pero los sistemas más eficaces se están combinando con venografía. |  |
| Iris El iris está formado por un músculo que abre y cierra la pupila del ojo. Tiene colores y formas características que son distintivas de cada individuo.  Se utiliza un sensor CCD similar al de las cámaras fotográficas, para obtener una especie de fotografía.  Es un buen sistema, pero algunos estudios revelan que el iris no es un indicador tan bueno como se pensaba hace algunos años. Cambia y existen similitudes entre personas. |  |
| Retina La retina es la parte interior del globo ocular. La estructura de pequeños vasos sanguíneos de su interior es única para cada individuo  Se utiliza un sensor CCD similar al de las cámaras fotográficas, con una tenue luz para obtener una especie de fotografía a través de la pupila.  Como inconveniente achacado a estos sistemas cabe citar una cierta incomodidad debido a que es necesario acercar los ojos al dispositivo. La tenue luz que emite también puede resultar molesta para algunas personas  La retina se ha revelado como un indicador muy eficaz. |  |
| Venografía El entramado de venas que recorren la superficie de la palma de la mano, o de un solo dedo parece ser un buen indicador biométrico.  Ésta es una de las técnicas que más están evolucionando en los últimos tiempos.  Se utiliza un CCD similar al de un escáner o cámara digital, pero capaz de captar infrarrojos. Debido a la diferencia de temperatura de los vasos sanguíneos con respecto a los músculos, éstos emiten un poco más de calor y puede ser captado por los CCD infrarrojos.  Se considera un buen indicador, y los sistemas biométricos que la utilizan son fiables y no muy caros |  |
| Rostro El reconocimiento automático de un rostro es el viejo sueño de la biometría, pero está lejos de alcanzarse con un alto grado de confianza.  El rostro es una de las partes del cuerpo más accesibles y por el que normalmente, los humanos nos reconocemos.  Aunque se pueden medir y cuantificar ciertos aspectos del rostro, su estudio es muy complejo, y además, cambia espectacularmente en periodos breves de tiempo (nos maquillamos, se nos hinchan los ojos cuando no dormimos bien, gesticulamos, nos dejamos barba o nos peinamos de manera distinta). El reconocimiento debe basarse en mediciones que sean constantes: las facciones fundamentales.  El rostro es un elemento tridimensional, que una cámara capta sólo en dos dimensiones.  Por el momento, no es un buen indicador biométrico para una máquina, aunque para los humanos sea el más común.  Se utiliza una cámara fotográfica normal, aunque hay sistemas que combinan varias para obtener mediciones en 3D. |  |
| Firma El reconocimiento de la firma (y de la escritura en general) se basa en los aspectos dinámicos del hecho: es decir, en los movimientos que realizamos al firmar, y no en la propia firma.  Las tabletas captadoras de la firma suelen llevar un lápiz activo, que detecta la presión. Combinada con la propia tableta (que es un sensor táctil resistivo, como el de las PDA) se puede obtener mediciones de la dinámica de la firma (velocidad de cada trazo, ángulos, presión, etc.) |  |
| Voz Al igual que pasa con el rostro, la voz es un indicador muy difícil de reconocer. Aunque hay ciertas características, es un indicador que cambia con el tiempo y el momento. (Ej: el tono varía cuando nos acabamos de levantar de dormir… la velocidad también cuando estamos cansados).  Se utiliza un simple micrófono y software de análisis muy complejo.  Aunque muy apreciado en las películas de espías, no tiene buenos resultados en la realidad comparado con otros sistemas. |  |

# Listas de control de acceso (ACLs)

Una lista de control de acceso o ACL (del inglés, access control list) es **un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.**

Encontramos ACLs en muchos sitios:

* En el acceso a un sistema operativo
* En el acceso a objetos de un sistema operativo, como carpetas, ficheros, o determinado hardware
* En elementos de red enrutadores, firewalls, proxys
* En dependencias físicas, como edificios, habitaciones, etc...

# Cuotas de disco.

Una cuota de disco es un límite establecido por el administrador del sistema que restringe ciertos aspectos del uso del sistema de archivos en los sistemas operativos modernos. El objetivo de la utilización de las cuotas de disco es limitar la asignación de espacio en el disco duro de una manera razonable.

Suele haber dos límites

* Soft limit: Es un límite de aviso, pero se puede seguir trabajando
* Hard limit: Es un límite absoluto. Para crear nuevos ficheros hay que borrar otros.

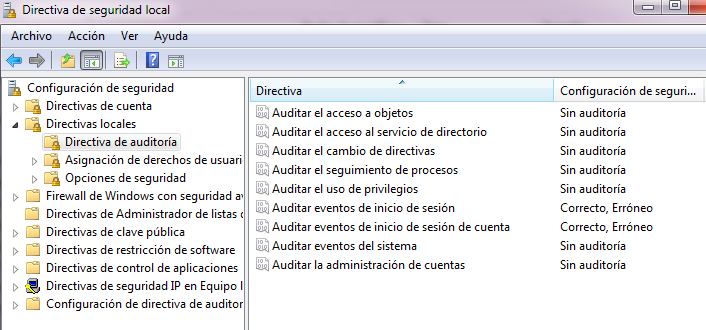
En servidores con servicios que producen información es conveniente poner cuotas de disco a los usuarios que administren el sistema, dado que existe una forma sencilla de lograr una denegación de servicio (**DoS**) si se logra acceso como uno de estos usuarios: **llenar completamente el disco y no dejar espacio para el normal funcionamiento de los servicios**. Esto puede lograrse tanto con una intrusión por red, como interactiva, como a través de malware.

# Auditorías del sistema operativo.

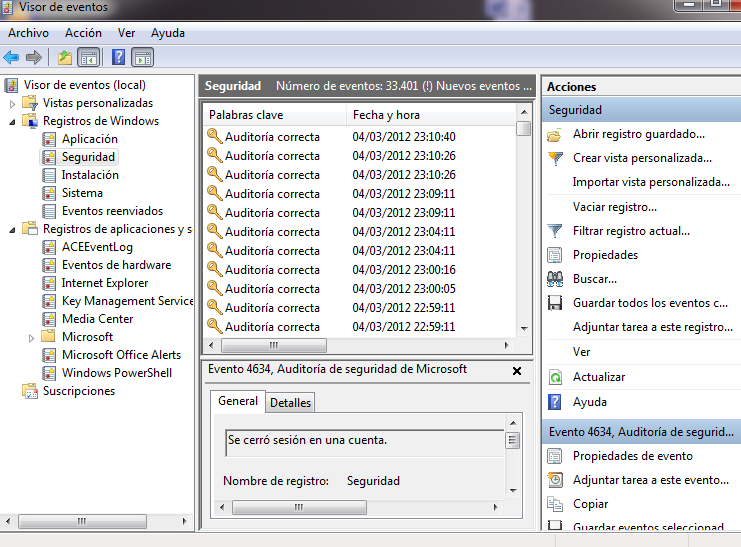
La auditoría del sistema operativo consiste en la monitorización y registro de diversos eventos que ocurran en el sistema, y que puedan tener interés de cara a una Auditoría de seguridad Informática.

Por defecto, los sistemas operativos registran la existencia de algunos hechos en el sistema, normalmente relacionados con el mal funcionamiento de aplicaciones, hardware o partes del propio sistema. No obstante, suele ser común poder activar la monitorización de otros eventos.

Por ejemplo, en Windows, pueden activarse auditorías de eventos que ocurren en el contexto de un equipo, o incuso en el contexto de un dominio de Windows. (Panel de Control/Herramientas administrativas/Directivas de seguridad)



Los eventos auditados pueden ser revisados con el **Visor de Eventos**



1. ISO 7881 [↑](#footnote-ref-1)
2. Superior: 79 caracteres alfanuméricos (210 bpi) Central: 40 caracteres numéricos (75 bpi) Inferior: 107 caracteres numéricos (210 bpi)

   (bpi: Bits Per Inch). [↑](#footnote-ref-2)