CONTENIDO

[CRIPTOGRAFIA 2](#_Toc456178291)

[Los Principios de la Criptografía 2](#_Toc456178292)

[TIPOS DE ALGORITMO CIFRADO 4](#_Toc456178293)

[CRIPTOGRAFIA SIMETRICA 4](#_Toc456178294)

[Seguridad 4](#_Toc456178295)

[Cifrados simétricos en informática 4](#_Toc456178296)

[CRIPTOGRAFIA DE CLAVE ASIMENTRICA 5](#_Toc456178297)

[Esquemas para la propagación de la confianza 5](#_Toc456178298)

[Establecimiento de una web de confianza. 6](#_Toc456178299)

[Seguridad 7](#_Toc456178300)

[Ventajas y desventajas del cifrado asimétrico 7](#_Toc456178301)

[CRIPTOGRAFIA HIBRIDA 8](#_Toc456178302)

[Ejemplo 8](#_Toc456178303)

[CERTIFICADO DIGITAL 8](#_Toc456178304)

[TERCERAS PARTES DE CONFIANZA 8](#_Toc456178305)

[Cómo funciona un tercero de confianza 9](#_Toc456178306)

[Características del DNI electrónico 10](#_Toc456178307)

[Características del microchip 10](#_Toc456178308)

[Características de la tarjeta electrónica 10](#_Toc456178309)

[Procedimientos de autenticación y firma electrónica 11](#_Toc456178310)

[Procedimiento de autenticación y firma electrónica con la aplicación PKI 11](#_Toc456178311)

[HACKER 12](#_Toc456178312)

[Historia 12](#_Toc456178313)

[ARPANET 12](#_Toc456178314)

[UNIX 12](#_Toc456178315)

[GNU 13](#_Toc456178316)

[LINUX 13](#_Toc456178317)

[Ética hacker 13](#_Toc456178318)

[Controversia 14](#_Toc456178319)

[Activismo 15](#_Toc456178320)

[Clasificación de los hackers 16](#_Toc456178321)

[Sombreros 16](#_Toc456178322)

[Hacker de sombrero blanco 17](#_Toc456178323)

[Hacker de sombrero negro 17](#_Toc456178324)

[Hacker de sombrero gris 17](#_Toc456178325)

[Otros usos 17](#_Toc456178326)

[Phreaker 17](#_Toc456178327)

[Lamer o script-kiddie 18](#_Toc456178328)

[Newbie 18](#_Toc456178329)

# CRIPTOGRAFIA

## Los Principios de la Criptografía

Las personas quieren decir cosas diferentes cuando ellos hablan sobre la criptografía. Los niños juegan con códigos del juguete y los idiomas confidenciales. Sin embargo, éstos tienen poco para ver con la seguridad real y la criptografía fuerte. La criptografía fuerte es el tipo de criptografía que puede usarse para proteger información de valor real contra los delincuentes organizados, corporaciones multinacionales, y los gobiernos mayores. Las criptografías fuertes eran negocio sólo militar; sin embargo, en la sociedad de información se ha vuelto uno de las herramientas centrales por mantener secreto y confidencialidad.

Cuando nosotros pasamos a una sociedad de información, los medios tecnológicos para la vigilancia global de millones de personas individuales están poniéndose disponibles para especializarse a los gobiernos. La criptografía se ha vuelto uno de las herramientas principales para el secreto, confíe, mando de acceso, pagos electrónicos, seguridad corporativa, y los otros campos innumerables.

La criptografía es más una cosa militar con que no se debe jugar. Es tiempo para dé mistificar el misterio de criptografía y usar sus ventajas que necesita la sociedad moderna.

En lo siguiente, se presenta la básica terminología y los principales métodos de la criptografía. Cualquier opinión y evaluaciones presentadas aquí son especulativas, y el autor no puedo sostenerse responsable para su exactitud - aunque cada esfuerzo se hace por asegurarse que esta información es tan correcta y moderna como posible.

Terminología básica

Suponga que alguien quiere enviar un mensaje a un receptor, y quiere estar seguro que ningún otro puede leer el mensaje. Hay la posibilidad, sin embargo, que alguien abre la carta o intercepta la comunicación electrónica.

En la terminología de la criptografía, el mensaje se llama plaintext o cleartext (texto abierto). Poniendo en código el mensaje de semejante manera que esconde su sentido se llama encriptan. El mensaje encriptado se llama el ciphertext (texto encifrado). El proceso de recuperar el plaintext del ciphertext se llamadecription. Encripcion y decription normalmente hacen uso de una llave, y el método codificando es tal que los decription sólo pueden ser realizados sabiendo la llave apropiada.

La criptografía es el arte, o ciencia, de guardar el secreto de mensajes o documentos. El criptoanálisis es el arte de recuperar el plaintext sin saber la llave apropiada. Las personas que hacen criptografía son criptógrafos, y los practicantes de criptoanálisis son criptoanálistas.

La criptografía se trata de todos los aspectos de mensajes seguros, autenticación, firmas digitales, dinero electrónico, y otras aplicaciones. Cristología es la rama de matemática que estudia las fundaciones matemáticas de métodos de la criptografía.

Básicos algoritmos de criptografía

Un método de encription y decription se llama un cifre. Algunos métodos de la criptografía confían en el secreto de los algoritmos; los tales algoritmos sólo son de interés histórico y no son adecuado para necesidades del mundo real. Todos los algoritmos modernos usan una llave para controlar encription y decription; un mensaje sólo puede ser decriptado si la llave de decription empareja la llave del encription.

Hay dos clases de algoritmos del encription usando llaves, los algoritmos simétricos (o llave-secreto) y asimétricos (o llave-público). La diferencia es que los algoritmos simétricos usan la misma llave para encription y decription (o la llave del decription se deriva fácilmente de la llave del encription), considerando que los algoritmos asimétricos usan una llave diferente para encription y decription, y la llave del decription no puede derivarse de la llave de encription.

Los algoritmos simétricos pueden ser divididos en los cifres del arroyo y cifres del bloque. Los cifres del arroyo pueden encriptar un solo bit de plaintext en un momento, considerando que los cifres del bloque toman varios bits (típicamente 64 bits en cifres modernos), y encriptar ellos como una sola unidad.

Cifres asimétricos (también llamados algoritmos de llave-pública o la criptografía de llave-pública) permiten las llaves para encription de ser pública (incluso puede publicarse en un periódico), permitiendo cualquiera al encriptar con la llave, considerando que sólo el destinatario apropiado (quién sabe la llave de decription) puede decriptar el mensaje. La llave de encription también se llama la llave pública y de decription la llave privada o confidencial.

Los algoritmos modernos de la criptografía ya no son cifres de lápiz-y-papel. Se diseñan algoritmos de la criptografía fuertes para ser ejecutados por las computadoras o dispositivos del hardware especializados. En la mayoría de las aplicaciones, la criptografía se hace con el software de la computadora.

Generalmente, los algoritmos simétricos son más rápidos a ejecutar en una computadora que el asimétrico. En práctica ellos se usan a menudo juntos, para que un algoritmo de llave-público sea usado al encriptar una llave de encription generada al azar, y esa llave del azar es usada al encriptar el mensaje real que usa un algoritmo simétrico. Esto a veces se llama

Las descripciones de muchos buenos algoritmos de la criptografía son ampliamente y públicamente disponibles de cualquier librería, biblioteca científica, oficina de patentes, o en el Internet. El cifre simétrico mas estudió y probablemente ampliamente extendido es DES; los próximos AES podrían reemplazarlo como el algoritmo del encription ampliamente usado. RSA probablemente es el algoritmo del encription asimétrico bien conocido. A bajo se encuentra la lista de varios buenos libros en la criptografía y los temas relacionados.

## TIPOS DE ALGORITMO CIFRADO

### CRIPTOGRAFIA SIMETRICA

La criptografía simétrica (en inglés symmetric key cryptography), también llamada criptografía de clave secreta (en inglés secret key cryptography) o criptografía de una clave (en inglés single-key cryptography), es 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. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

#### Seguridad

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Los algoritmos de cifrado ampliamente utilizados tienen estas propiedades (por ejemplo: AES).

Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio. Richard Feynman fue famoso en Los Álamos por su habilidad para abrir cajas de seguridad; para alimentar la leyenda que había en torno a él, llevaba encima un juego de herramientas que incluían un estetoscopio. En realidad, utilizaba una gran variedad de trucos para reducir a un pequeño número la cantidad de combinaciones que debía probar, y a partir de ahí simplemente probaba hasta que adivinaba la combinación correcta. En otras palabras, reducía el tamaño de posibilidades de claves.

Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 256 claves posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como 3DES, Blowfish e IDEA usan claves de 128 bits, lo que significa que existen 2128 claves posibles. Esto equivale a muchísimas más claves, y aun en el caso de que todas las máquinas del planeta estuvieran cooperando, tardarían más tiempo en encontrar la clave que la edad del universo.

#### Cifrados simétricos en informática

Cifrados de flujo: cifran el mensaje con correspondencias bit a bit sobre el flujo (stream). Algunos cifrados de flujo son RC4 o RC6.

Cifrados de Bloque: cifran el mensaje dividiendo el flujo en bloques de k bits. Cada bloque se corresponde con otro diferente. Por ejemplo, un bloque con k=3 "010" se podría corresponder con "110". Un ejemplo de cifrado de bloque es el algoritmo AES.

### CRIPTOGRAFIA DE CLAVE ASIMENTRICA

La criptografía asimétrica (en inglés asymmetric key cryptography), también llamada criptografía de clave pública (en inglés public key cryptography) o criptografía de dos claves1 (en inglés two-key cryptography), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y autentificación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de lossistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

#### Esquemas para la propagación de la confianza

Observar que la criptografía de clave pública necesita establecer una confianza en que la clave pública de un usuario (al cual se identifica por una cadena identificativa a la que se llama identidad) es correcta, es decir el único que posee la clave privada correspondiente es el usuario auténtico al que pertenece. Cuanto más fiable sea el método más seguridad tendrá el sistema.

Lo ideal sería que cada usuario comunicara (e idealmente probara) de forma directa al resto de usuarios cuál es su clave pública. Sin embargo, esto no es posible en la realidad y se desarrollan distintos esquemas para aportar confianza. Estos esquemas se pueden agrupar en dos tipos: Esquema centralizados y esquemas descentralizados. En los esquemas descentralizado hay varios nodos y cada uno tiene unas capacidades y derechos. En los esquemas centralizados hay una arquitectura cliente-servidor donde los servidores juegan un papel central y proveen servicios a los clientes. Cada esquema tiene sus ventajas e inconvenientes, por ejemplo, los sistemas centralizados suelen ser más vulnerables a ataques de denegación de servicio debido a que basta con que falle el servidor central para que el sistema de confianza caiga por completo. Los sistemas descentralizados se suelen considerar menos seguros contra ataques encaminados a publicar claves públicas falsas debido a que al haber varios nodos posibles a atacar es más difícil asegurar su seguridad. Los modelos más usados son:

Uso de una infraestructura de clave pública o PKI. En este modelo hay una o varias entidades emisoras de certificados (Autoridades de certificación o CA del inglés Certification Authority) que aseguran la autenticidad de la clave pública y de ciertos atributos del usuario. Para ello firman con su clave privada ciertos atributos del usuario incluyendo su clave pública generando lo que se llama certificado del usuario.

#### Establecimiento de una web de confianza.

No hay nodos aparte de los usuarios. Los usuarios recogen claves públicas de otros usuarios y aseguran su autenticidad si están seguros de que la clave privada correspondiente pertenece en exclusiva a ese usuario. Un usuario además puede directamente confiar en el conjunto de claves públicas en las que otro confía ya sea directamente o a través de otras relaciones de confianza. En cada caso es el propio usuario el que decide el conjunto de claves públicas en las que confía y su grado de fiabilidad. Dos usuarios que no se conocen pueden confiar en sus claves públicas si existe una cadena de confianza que enlace ambas partes. Este tipo de implementación de la confianza es el que usa por ejemplo PGP.

Uso de criptografía basada en identidad. En este modelo existe un generador de claves privadas o PKG (acrónimo de Private Key Generator) que a partir de una cadena de identificación del usuario genera una clave privada y otra pública para ese usuario. La pública la difunde para que el resto de usuarios la sepan y la privada es comunicada en exclusiva al usuario a quien pertenece.

Uso de criptografía basada en certificados. En este modelo el usuario posee una clave privada y otra pública. La clave pública la envía a una Autoridad de certificación que basándose en criptografía basada en identidad genera un certificado que asegura la validez de los datos.

Uso de criptografía sin certificados. Este modelo es similar al modelo que usa criptografía basada en identidad pero con la diferencia de que lo que se genera en el centro generador de claves o KGC (acrónimo de Key Generator Center) es una clave parcial. La clave privada completa se genera a partir de la clave privada parcial y un valor generado aleatoriamente por el usuario. La clave pública es generada también por el usuario a partir de parámetros públicos del KGC y el valor secreto escogido.

Girault distingue tres niveles de confianza que dan los distintos modelos a la autoridad que interviene en el proceso (PKG, KGC o CA según cada caso):

Nivel 1: La autoridad puede calcular claves secretas de usuarios y por tanto pueden hacerse pasar como cualquier usuario sin ser detectado. Las firmas basadas en identidad pertenecen a este nivel de confianza

Nivel 2: La autoridad no puede calcular claves secretas de usuarios, pero puede todavía hacerse pasar como cualquier usuario sin ser detectado. Firmas sin certificados pertenecen a este nivel

Nivel 3: La autoridad no puede calcular claves secretas de usuarios, y tampoco puede hacerse pasar como un usuario sin ser detectado. Es el nivel más alto de fiabilidad. Las firmas tradicionales PKI y la firma basada en certificados pertenecen a este nivel

#### Seguridad

Según el segundo principio de Kerckhoffs toda la seguridad debe descansar en la clave y no en el algoritmo (en contraposición con la seguridad por la oscuridad). Por lo tanto, el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño de la clave del cifrado simétrico con el del cifrado de clave pública para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave del tamaño de 80 bits, el atacante debe probar hasta 280-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con una clave del tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

#### Ventajas y desventajas del cifrado asimétrico

La mayor ventaja de la criptografía asimétrica es que la distribución de claves es más fácil y segura ya que la clave que se distribuye es la pública manteniéndose la privada para el uso exclusivo del propietario, pero este sistema tiene bastantes desventajas:

Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.

Las claves deben ser de mayor tamaño que las simétricas. (Generalmente son cinco o más veces de mayor tamaño que las claves simétricas)

El mensaje cifrado ocupa más espacio que el original.

Los nuevos sistemas de clave asimétrica basado en curvas elípticas tienen características menos costosas.

Herramientas como PGP, SSH o la capa de seguridad SSL para la jerarquía de protocolos TCP/IP utilizan un híbrido formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica, y la criptografía simétrica para la transmisión de la información.

### CRIPTOGRAFIA HIBRIDA

La criptografía híbrida es un método criptográfico que usa tanto un cifrado simétrico como un asimétrico. 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.

#### Ejemplo

Tanto PGP como GnuPG usan sistemas de cifrados híbridos. La clave de sesión (clave simétrica) es cifrada con la clave pública del destinatario, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave de sesión (clave simétrica) y acto seguido usa ésta para descifrar el mensaje.

Un sistema de cifrado híbrido no es más fuerte que el de cifrado asimétrico o el de cifrado simétrico de los que hace uso, independientemente de cuál sea más débil. En PGP y GnuPG el sistema de clave simétrica es probablemente la parte más débil de la combinación. Sin embargo, si un atacante pudiera descifrar una clave de sesión, sólo sería útil para poder leer un mensaje, el cifrado con esa clave de sesión. El atacante tendría que volver a empezar y descifrar otra clave de sesión para poder leer cualquier otro mensaje.

## CERTIFICADO DIGITAL

Un certificado digital o certificado electrónico es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. El certificado digital es válido principalmente para autenticar a un usuario o sitio web en internet por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación. El nombre asociado a esta entidad de confianza es Autoridad Certificadora pudiendo ser un organismo público o empresa reconocida en Internet.

El certificado digital tiene como función principal autenticar al poseedor pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información delicada entre las partes.

### TERCERAS PARTES DE CONFIANZA

Una vez definido el concepto de certificado digital se plantea una duda: ¿cómo confiar si un determinado certificado es válido o si está falsificado?. La validez de un certificado es la confianza en que la clave pública contenida en el certificado pertenece al usuario indicado en el certificado. La validez del certificado en un entorno de clave pública es esencial ya que se debe conocer si se puede confiar o no en que el destinatario de un mensaje será o no realmente el que esperamos.

La manera en que se puede confiar en el certificado de un usuario con el que nunca hemos tenido ninguna relación previa es mediante la confianza en terceras partes.

La idea consiste en que **dos usuarios puedan confiar directamente entre sí, si ambos tienen relación con una*tercera parte* ya que ésta puede dar fé de la fiabilidad de los dos**.

La necesidad de una Tercera Parte Confiable (TPC ó TTP, Trusted Third Party) es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es impensable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada. Además, la mejor forma de permitir la distribución de los claves públicos (o certificados digitales) de los distintos usuarios es que algún agente en quien todos los usuarios confíen se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

En conclusión, se podrá tener confianza en el certificado digital de un usuario al que previamente no conocemos si dicho certificado está avalado por una tercera parte en la que sí confiamos. La forma en que esa tercera parte avalará que el certificado es de fiar es mediante su firma digital sobre el certificado. Por tanto, podremos confiar en cualquier certificado digital firmado por una tercera parte en la que confiamos. La TPC que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave púbica se conoce con el nombre de Autoridad de Certificación (AC).

### Cómo funciona un tercero de confianza

El tercero de confianza archiva las declaraciones de voluntad que integran los contratos electrónicos, e interviene cuando las partes pactan esta forma de acreditación de la celebración de los contratos electrónicos.

Aunque la LSSI exige una duración mínima de la custodia 5 años, en realidad el mínimo práctico es de 6 años, por exigencia del Código de Comercio y de la normativa de blanqueo de capitales, respecto a los sujetos obligados.

En el marco de los servicios de confianza regulados por el reglamento europeo de 2014, los Terceros de Confianza pasan a denominarse Prestadores de Servicios de Confianza Digital y aplican mecanismos de seguridad como la Firma Electrónica, el Sello de Tiempo, la Custodia Electrónica o los servicios de Entrega Electrónica fehaciente de mensajes.

Documento Nacional de Identidad Electronico

El Documento Nacional de Identidad en el Perú es un tipo de DNI electrónico (DNIe) que se expide a partir del 15 de julio de 20131 y reemplazará gradualmente al  DNI actual. Está destinado principalmente a jóvenes de 18 y 19 años que lo soliciten por primera vez, funcionarios públicos, personal del sistema electoral, e instituciones privadas que realicen convenios con el RENIEC.2 Su validez es de ocho años.

El DNI electrónico o DNI-e peruano, está fabricado en policarbonato y tiene el formato de una tarjeta de crédito, siguiendo la norma ISO 7816. Posee un chip basado en las tecnologías de firma electrónica, tarjeta inteligente y biométrica, e incorpora inicialmente cuatro aplicativos de software: El primero de identidad eMRTD ICAO, el segundo de firma digital PKI, el tercero de autenticación biométrica por huella dactilar Match-on-Card y un cuarto de tipo genérico que incluya el almacenamiento de datos y dispositivos contadores.

En junio de 2015, el DNI electrónico fue reconocido como el mejor documento de identidad de América Latina, durante la «Conferencia Latinoamericana de Imprenta de Alta Seguridad» efectuada en Lima, la cual estuvo organizada por la firma británica Reconnaissance International, dedicada a holografía, moneda, autenticación y seguridad documentaria.

### Características del DNI electrónico

[](https://commons.wikimedia.org/wiki/File:Dniecaracteristicas.jpg)

#### Características del microchip

* Sistema operativo Java Card, que posibilita la incorporación de futuras aplicaciones y contenidos.
* Capacidad criptográfica para gestión de claves RSA y firma digital con certificados.
* Memoria EEPROM de 144 Kb.
* Seguridad conforme a los estándares internacionales Common Criteria nivel EAL4+ ó FIPS 140-2.
* Basic Access Control (BAC), que previene el acceso no autorizado al contenido del chip.
* Active Authentication (AA), clave RSA de 1024 bits que garantiza la autenticidad del chip e impide su clonación.
* Aplicaciones: PKI, ICAO eMRTD, Match On Card (MOC).
* Software complementario: Middleware, SDK para aplicaciones cliente, Java Card SDK

#### Características de la tarjeta electrónica

* Fondo con patrón Guilloché
* Impresión de textos o motivos visibles con luz ultravioleta
* Micro línea offset
* Zona de foto con micro texto ondulado
* Dispositivo Ópticamente Variable (DOVID)
* Grabado Láser
* Tinta ópticamente variable (Optical Variable Ink - OVI)
* Elemento de seguridad microscópico (JDSU charms)
* Imagen Láser Variable (CLI)

#### Procedimientos de autenticación y firma electrónica

El chip de la tarjeta posee un sistema de autenticación a través de la tecnología biométrica, que almacena información de las impresiones digitales de los dedos índices de cada mano. Para validar la identidad del titular, se deben seguir los siguientes pasos:

En primer lugar, el centro de atención requiere contar con un lector de tarjetas y un lector de huellas.

El ciudadano presentará su DNI electrónico y colocará el dedo índice en el lector de huellas.

La aplicación MOC comparará la imagen archivada con la huella dactilar.

Si ambas imágenes coinciden, la tarjeta responderá afirmativamente, procediendo a la validación de la identidad.

#### Procedimiento de autenticación y firma electrónica con la aplicación PKI

El DNI electrónico ofrece la posibilidad de firmar digitalmente documentos electrónicos y autenticar la identidad mediante la aplicación PKI. Para hacer uso de esta herramienta, el usuario debe disponer de una lectora de tarjetas conectada a su computadora, y opcionalmente, de un dispositivo de lectura de huellas dactilares o lector biométrico.

Para autenticar la identidad: El ciudadano ingresa al sitio web de la institución pública. Si es requerida la identificación, deberá introducir el DNI-e en la lectora de tarjetas. La verificación se produce introduciendo el PIN de autenticación (Número de Identificación Personal) o si dispone de un lector biométrico, la huella dactilar.

Para firmar electrónicamente: Para que el ciudadano pueda firmar digitalmente un formato o documento electrónico, deberá primero introducir su DNI-e en la lectora de tarjetas, el sistema solicitará el PIN de firma, la tarjeta efectuará la verificación, de resultar satisfactoria se obtendrá un archivo firmado digitalmente.

# HACKER

## Historia

En 1961 el MIT, el Massachusetts Institute of Technology, adquirió la microcomputadora PDP-1, lo que atrajo la curiosidad de un grupo de estudiantes que formaban parte delTech Model Railroad Club, TMRC, ya que podrían interactuar directamente con ella mediante códigos de programación. Debido a que la microcomputadora tardaba mucho en encender, se quedaba prendida toda la noche haciendo que los miembros del TMRC tuvieran acceso a ella y pudieran empezar a experimentar, uno de los logros más famosos de estos experimentos fue la creación del videojuego Spacewar. Tiempo después algunos miembros del TMRC se volvieron miembros del Laboratorio de Inteligencia Artificialdel MIT y se llevaron con ellos la tradición de jugarse bromas inocentes entre ellos, a las cuales llamaban hacks. Fueron los miembros de este laboratorio los primeros en autonombrarse hackers.3 Esta comunidad se caracteriza por el lanzamiento del movimiento de software libre. La World Wide Web e Internet en sí misma son creaciones de hackers.6

## ARPANET

Después de 1969 el laboratorio de Inteligencia Artificial del MIT fue conectado a la ARPANET desde donde pudo tener contacto con otros departamentos de investigación informática de otras universidades como Stanford y Bolt Beranek & Newman. Con ésta nueva forma de comunicación los estudiantes empezaron a colaborar con otros a pesar de la distancia. A partir de este momento se empezó a formar una cultura y nació el Jargon file[1], documento que tenía una lista de términos que se usaban en su jerga coloquial y que se originó en Standford en 1987.[2].3 Los hackers de MIT crearon su propio sistema operativo, el ITS que usaba el lenguaje LISP.8

## UNIX

Al mismo tiempo que ARPANET nacía, también era creado el sistema operativo UNIX en los laboratorios Bell. UNIX, junto con el lenguaje C, era muy portable y compatible con las máquinas. Las máquinas con UNIX tenían su propia conexión con otras máquinas con UNIX, y esta interconexión recibió el nombre de Usenet. Para 1980 los primeros sitios en Usenet empezaban a transmitir noticias, formando una gran red de distribución que crecería más que ARPANET.8

Ambos grupos de hackers estaban divididos y era poco común que alguien que usara UNIX también usara ARPANET. En 1983 se canceló la distribución de la PDP-10, la cual fuera una de las microcomputadoras favoritas de los hackers y en la cual se construyó el ITS. Después de la cancelación de esta microcomputadora por parte de la Digital Equipment Corporation la variante de UNIX creada en Berkeley se convirtió en el sistema hacker por excelencia,8 y por esa época Richard M. Stallman, inventor del editor Emacs, creó la Free Software Foundation.

[](https://commons.wikimedia.org/wiki/File:Actual_DEC_UNIX_License_Plate_DSC_0317.jpg)

Placa que dice "vive libre o muere UNIX\* \*marca registrada de laboratorios Bell

## GNU

En 1983 Stallman buscaba crear un propio sistema operativo de tipo UNIX que estuviese disponible de forma libre, y fundó el proyecto GNU (acrónimo de GNU No es UNIX). Stallman sustituyó el copyright o todos los derechos reservados, por el copyleft o todos los derechos reversados, con lo que buscaba que cualquier programa publicado en la red por la FSF pudiera ser utilizado y modificado bajo una licencia de la Fundación y con la condición de difundir las modificaciones que se llegasen a hacer al programa también respetando las libertades del usuario. Otro de sus logros fue haber popularizado el término "software libre" en un intento de conseguir su objetivo y ponerle nombre al producto de toda cultura hacker.3

## LINUX

En 1991, un estudiante de la Universidad de Helsinki, Linus Torvalds diseñaba su propio UNIX sobre la base de la fundación y publicó la fuente de su código en la red pidiendo ayuda para perfeccionarlo. Con ayuda de cientos de programadores que se pusieron a la tarea de ayudar a Linux con el código, se desarrolla el Kernel Linux (erróneamente se lo denomina sistema operativo), que originalmente tenía el nombre de Freix. Hoy en día es promocionado por diferentes gobiernos, como el de Francia, y siempre está en código abierto y sin derechos de propiedad sobre él.9

## Ética hacker

En 1984, Steven Levy publica el libro Hackers: heroes of the computer revolution en el cual se ve por primera ocasión la idea de la éticahacker, donde se manifiesta una ética de libre acceso a la información y código fuente del software. Levy se basó en entrevistas para poder identificar seis principios básicos relacionados con las creencias y operaciones de hackers para hacer esta ética.

[](https://commons.wikimedia.org/wiki/File:Steven_Levy_(1).jpg)

Steven Levy, autor de Hackers: heroes of the computer revolution

De acuerdo a Levy los seis fundamentos del hacker son:

* El acceso a los computadores debe ser ilimitado y total.
* Toda información debería ser libre
* Es necesario promover la descentralización y desconfiar de las autoridades
* Los hackers deberían ser juzgados por su labor y no por cosas como su raza, edad o posición social
* Se puede crear arte y belleza en un computador
* Las computadoras pueden cambiar tu vida para mejor

Sin embargo, la ética hacker genera controversia y hay personas, como el estudiante de derecho Patrick S. Ryan que critican que la ética hacker y consideran que "hay muy poca ética" y la catalogan como "un grito de batalla -que- no pone límites a los hackers"12 Sin embargo, para otras personas, como Linus Torvalds, ésta ética va de acuerdo al trabajo del hacker que es "interesante, emocionante y algo que se goza", adjetivos que en ocasiones son usados por los mismos hackers para describir su trabajo, lo que también limita la restricción que tienen sobre la libertad de usar información.13

De acuerdo a Raymond, la ética social del hacker se basa en tres principios:

* La creencia de que compartir información es bueno
* Que los hackers tienen una responsabilidad ética de compartir la información con la que trabajan
* Que los hackers deberían facilitar el acceso a computadoras cuando sea posible

## Controversia

En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980.15 Según Helen Nissenbaum, que los hackers sean mal vistos ayuda al gobierno y a los poderes privados con dos cosas: 1) a definir lo que es normal en el mundo computacional haciendo creer que un buen ciudadano es todo lo que el hacker no es; 2) a justificar la seguridad, la vigilancia y el castigo.16

A los criminales se le pueden sumar los llamados "script kiddies", gente que invade computadoras, usando programas escritos por otros, y que tiene muy poco conocimiento sobre cómo funcionan. Este uso parcialmente incorrecto se ha vuelto tan predominante que, en general, un gran segmento de la población no es consciente de que existen diferentes significados.

Mientras que los hackers aficionados reconocen los tres tipos de hackers y los hackers de la seguridad informática aceptan todos los usos del término, los hackers del software libre consideran la referencia a intrusión informática como un uso incorrecto de la palabra, y se refieren a los que rompen los sistemas de seguridad como "crackers" (analogía de "safecracker", que en español se traduce como "un ladrón de cajas fuertes").

Ambigüedad y debate

Los términos hacker y hack pueden tener connotaciones positivas y negativas. Los programadores informáticos suelen usar las palabras hacking y hacker para expresar admiración por el trabajo de un desarrollador cualificado de soporte lógico, pero también se puede utilizar en un sentido negativo (delincuentes informáticos) para describir una solución rápida pero poco elegante a un problema. Algunos[¿quién?] desaprueban el uso del hacking como un sinónimo de cracker, en marcado contraste con el resto del mundo,[¿dónde?] en el que la palabra hacker se utiliza normalmente para describir a alguien que se infiltra en un sistema informático con el fin de eludir o desactivar las medidas de seguridad.17

En un principio se utilizaba "hack" como verbo para expresar "perder el tiempo" (e.j. "Puedo hackear con el computador"), el significado del término ha cambiado a lo largo de décadas desde que empezó a utilizarse en un contexto informático. Como su uso se ha extendido más ampliamente, el significado primario de la palabra, por parte de los nuevos usuarios, ha pasado a uno que entra en conflicto con el énfasis original.

## Activismo

[](https://commons.wikimedia.org/wiki/File:HappyHackingBicicleta.png)

En sentido amplio el término hacker o hacking se puede asociar a movimientos sociales que promueven cambios en los modos de vida.

Desde el año 2002-2003, se ha ido configurando una perspectiva más amplia del hacker, pero con una orientación a su integración al hacktivismo en tanto movimiento. Aparecen espacios autónomos denominados hacklab o hackerspace y los hackmeeting como instancias de diálogo de hackers. Desde esta perspectiva, se entiende al hacker como una persona que es parte de una conciencia colectiva que promueve la libertad del conocimiento y la justicia social.

Se entiende, por tanto, el hacktivismo (fusión de hack y activismo) como el empleo de las destrezas técnicas más diversas, en pro de fines sociales, ecológicos, humanitarios o de cualquier otra índole con repercusión o tendente a la defensa de los derechos humanos.

Así, el hacktivismo debe ser entendido no desde un prisma reduccionista como equivalente siempre al desarrollo de actividades subversivas. Encontramos ramificaciones del hacktivismo en la liberación de conocimiento (como puede ser la misma Wikipedia, en la que los conocimientos informáticos y técnicos de sus creadores dieron lugar a toda una revolución en el modo de crear y compartirse el conocimiento humano más allá de barreras académicas o comerciales); O en la liberación de información clasificada que se considera debe estar, por definición, a disposición de la sociedad (casos de WikiLeaks o las filtraciones de Snowden sobre las actividades militares y casos de espionaje gubernamentales).

Por tanto, el fenómeno hacker tiene un importante componente de aperturismo y liberación de conocimientos e información que, a través del activismo de estos especialistas, benefician a la sociedad en general.

En este caso, los roles de un hacker pueden entenderse en cuatro aspectos:

* Apoyar procesos de apropiación social o comunitaria de las tecnologías.
* Poner a disposición del dominio público el manejo técnico y destrezas alcanzadas personal o grupalmente.
* Crear nuevos sistemas, herramientas y aplicaciones técnicas y tecnológicas para ponerlas a disposición del dominio público.
* Realizar acciones de hacktivismo tecnológico con el fin de liberar espacios y defender el conocimiento común y abierto.

## Clasificación de los hackers

### Sombreros

Un término acuñado a mediados del año 2014 por un hacker de la comunidad Underground[¿quién?] quien definió como "sobre el sombrero" a todos los profesionales vinculados con las artes Hacking. En un corto escrito, explica como a través del tiempo deben comprender y aprender todas las formas existentes de "Hackeo". Lo cual causa una doble moral, por un lado existe la ética a la cual han sido fieles y por ello prestan servicios profesionales a miles de empresas en el mundo asegurando su infraestructura; por otro, conocer y usar métodos propios de los BlackHat que incluyen ataques de denegación de servicio e ingeniería social agresiva entre otros. Según el escrito, están por encima del bien y del mal electrónico, lo cual concluye que solo una amplia capacidad moral autodeterminada por ellos mismos los convierte en profesionales con la capacidad de determinar adecuadamente y con las regulaciones de la actual sociedad.

### Hacker de sombrero blanco

Un hacker de sombrero blanco (del inglés, white hat), Penetran la seguridad del sistema, suelen trabajar para compañías en el área de seguridad informática para proteger el sistema ante cualquier alerta.

### Hacker de sombrero negro

Por el contrario, los hackers de sombrero negro (del inglés, black hat), también conocidos como "crackers" muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos hacking. rompe la seguridad informática, buscando la forma de entrar a programas y obtener información o generar virus en el equipo o cuenta ingresada.

### Hacker de sombrero gris

Son aquellos que poseen un conocimiento similar a al hacker de sombrero negro y con este conocimiento penetran sistemas y buscan problemas, cobrando luego por su servicio para reparar daños.

### Otros usos

En los últimos años, los términos sombrero blanco y sombrero negro han sido aplicados a la industria del posicionamiento en buscadores (search engine optimization, SEO), originando la denominación black hat SEO. Las tácticas de posicionamiento en buscadores de los hackers de sombrero negro, también llamada spamdexing, intento de redireccionar los resultados de la búsqueda a páginas de destino particular, son una moda que está en contra de los términos de servicio de los motores de búsqueda, mientras que los hackers de sombrero blanco, utilizan métodos que son generalmente aprobados por los motores de búsqueda.

### Phreaker

De phone freak ("monstruo telefónico"). Son personas con conocimientos amplios tanto en teléfonos modulares como en teléfonos móviles.

La meta de los phreakers es generalmente superar retos intelectuales de complejidad creciente, relacionados con incidencias de seguridad o fallas en los sistemas telefónicos, que les permitan obtener privilegios no accesibles de forma legal.

El término "Phreak" es una conjunción de las palabras phone (teléfono en inglés), hack y freak (monstruo en inglés). También se refiere al uso de varias frecuencias de audio para manipular un sistema telefónico, ya que la palabra phreak se pronuncia de forma similar a frequency (frecuencia).

### Lamer o script-kiddie

Es un término coloquial inglés aplicado a una persona falta de habilidades técnicas, generalmente no competente en la materia, que pretende obtener beneficio del hacking sin tener los conocimientos necesarios. Su alcance se basa en a buscar y descargar programas y herramientas de intrusión informática, cibervandalismo, propagación de software malicioso para luego ejecutarlo como simple usuario, sin preocuparse del funcionamiento interno de estos ni de los sistemas sobre los que funcionan. En muchos casos presume de conocimientos o habilidades que no posee.

### Newbie

La palabra es un anglicismo, que se traduciría como "hacker novato". Es una palabra usada en argot informático para referirse a alguien que acaba de iniciarse en el hacking y tiene poca experiencia. Algunas hipótesis sitúan la extensión de su uso a raíz de su popularidad dentro de las Fuerzas Armadas de los Estados Unidos de América, a finales del siglo XX. Otras variantes del término son Newby y newbee. El término "novato" a secas ("n00b", comúnmente escrito) se utiliza más a menudo en los juegos en línea.