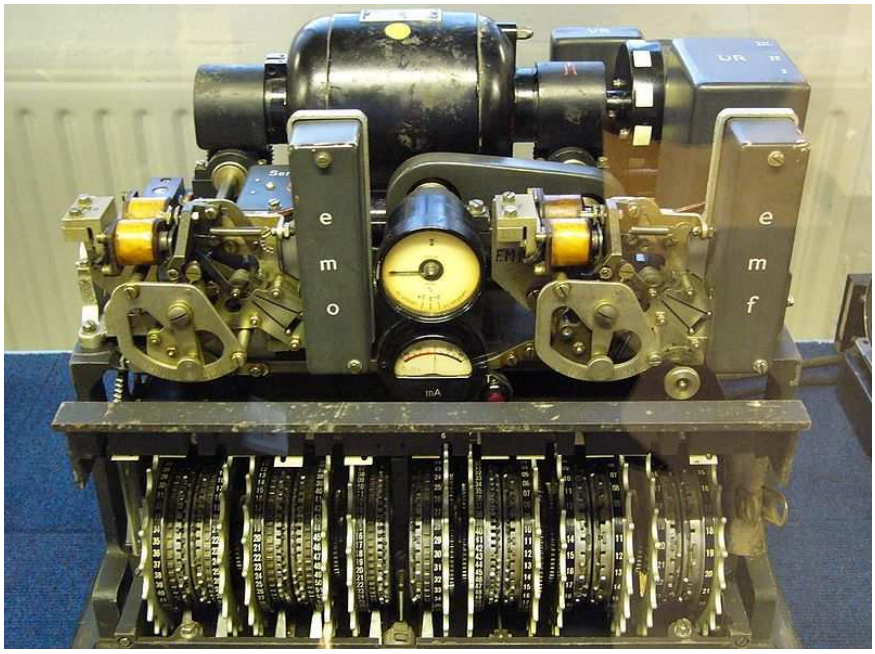
CRIPTOGRAFÍA

¿Qué es la Criptografía?

La principal aplicación de la criptografía es la de proteger información para evitar que sea accesible por observadores NO autorizados, proteger datos, pero también tiene otras aplicaciones.

La criptografía (del griego κρύπτω *krypto*, «oculto», y γράφω *graphos*, «escribir», literalmente «escritura oculta») es la técnica (bien sea aplicada al arte o la ciencia) que altera las representaciones lingüísticas de un mensaje.

La máquina alemana de cifrado Lorenz, usada en la Segunda Guerra Mundial para el cifrado de los mensajes para los generales de muy alto rango



OBJETIVO:

En esencia la criptografía trata de enmascarar las representaciones caligráficas de una lengua, de forma discreta. Si bien, el área de estudio científico que se encarga de ello es la Criptología.

Para ello existen distintos métodos, en donde el más común es el cifrado. Esta técnica enmascara las referencias originales de la lengua por un método de conversión gobernado por un algoritmo que permita el proceso inverso o descifrado de la información. El uso de esta u otras técnicas, permite un

intercambio de mensajes que sólo puedan ser leídos por los destinatarios designados como 'coherentes'. Un destinatario coherente es la persona a la que el mensaje se le dirige con intención por parte del remitente. Así pues, el destinatario coherente conoce el discretismo usado para el enmascaramiento del mensaje. Por lo que, o bien posee los medios para someter el mensaje criptográfico al proceso inverso, o puede razonar e inferir el proceso que lo convierta en un mensaje de acceso público. En ambos casos, no necesita usar técnicas criptoanalíticas.

Un ejemplo cotidiano de criptografía es el que usamos cuando mandamos una carta. El mensaje origen queda enmascarado por una cubierta denominada sobre, la cual declara el destinatario coherente, que además conoce el proceso inverso para hacer público el mensaje contenido en el sobre.

Hay procesos más elaborados que, por decirlo de alguna manera, el mensaje origen trata de introducir cada letra usada en un 'sobre' distinto. Por ejemplo, la frase 'texto de prueba', pudiera estar representada por la siguiente notación cifrada: CF, F0, 114, 10E, 106, 72, F3, F6, 75, 10C, 111, 118, FB, F6, F5. El 'sobre' usado es de notación hexadecimal, si bien, el cálculo hexadecimal es de acceso público, no se puede decir que sea un mensaje discreto, ahora, si el resultado de la notación hexadecimal (como es el caso para el ejemplo) es consecuencia de la aplicación de un 'método' de cierre del 'sobre' (como lo es la cola de sellado, o el lacre en las tradicionales cartas), el destinatario debe de conocer la forma de abrirlo sin deteriorar el mensaje origen. En otras palabras, debe de conocer la contraseña. Para el ejemplo, la contraseña es '12345678'.

CONCEPTO:

En la jerga de la criptografía, la información original que debe protegerse se denomina *texto en claro* o texto plano. El *cifrado* es el proceso de convertir el *texto plano* en un galimatías ilegible, denominado *texto cifrado* o *criptograma*. Por lo general, la aplicación concreta del *algoritmo de cifrado* (también llamado *cifra*) se basa en la existencia de una *clave*: información secreta que adapta el *algoritmo de cifrado* para cada uso distinto. Cifra es una antigua palabra arábiga para designar el número cero; en la Antigüedad, cuando Europa empezaba a cambiar del sistema de numeración romano al arábigo, se desconocía el cero, por lo que este resultaba misterioso, de ahí probablemente que cifrado signifique misterioso.

Las dos técnicas más sencillas de *cifrado*, en la criptografía clásica, son la *sustitución* (que supone el cambio de significado de los elementos básicos del mensaje -las letras, los dígitos o los símbolos-) y la *transposición* (que supone una reordenación de los mismos); la gran mayoría de las *cifras* clásicas son combinaciones de estas dos operaciones básicas.

El *descifrado* es el proceso inverso que recupera el *texto plano* a partir del *criptograma* y la *clave*. El *protocolo criptográfico* especifica los detalles de cómo se utilizan los *algoritmos* y las *claves* (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de *protocolos*, *algoritmos de cifrado*, procesos de gestión de claves y actuaciones de los usuarios, es lo que constituyen en conjunto un *criptosistema*, que es con lo que el usuario final trabaja e interactúa.

Existen dos grandes grupos de *cifras*: los algoritmos que usan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado*, y los que emplean una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Los primeros se denominan *cifras simétricas*, de *clave simétrica* o de *clave privada*, y son la base de los algoritmos de cifrado clásico. Los segundos se denominan *cifras asimétricas*, de *clave asimétrica* o de *clave pública* y forman el núcleo de las técnicas de cifrado modernas.

En el lenguaje cotidiano, la palabra *código* se usa de forma indistinta con *cifra*. En la jerga de la criptografía, sin embargo, el término tiene un uso técnico especializado: los *códigos* son un método de criptografía clásica que consiste en sustituir unidades textuales más o menos largas o complejas, habitualmente palabras o frases, para ocultar el mensaje; por ejemplo, "cielo azul" podría significar «atacar al amanecer». Por el contrario, las *cifras* clásicas normalmente sustituyen o reordenan los elementos básicos del mensaje -letras, dígitos o símbolos-; en el ejemplo anterior, «rcnm arcteeaal aaa» sería un criptograma obtenido por *transposición*. Cuando se usa una técnica de códigos, la información secreta suele recopilarse en un *libro de códigos*.

Con frecuencia los procesos de cifrado y descifrado se encuentran en la literatura como *encriptado* y *desencriptado*, aunque ambos son neologismos erróneos —anglicismos de los términos ingleses *encrypt* y *decrypt*— todavía sin reconocimiento académico. Hay quien hace distinción entre *cifrado/descifrado* y *encriptado/desencriptado* según estén hablando de criptografía simétrica o asimétrica, pero la realidad es que la mayoría de los expertos hispanohablantes prefieren evitar ambos neologismos hasta el punto de que el uso de los mismos llega incluso a discernir a los aficionados y novatos en la materia de aquellos que han adquirido más experiencia y profundidad en la misma.

Ideológicamente cifrar equivale a escribir y descifrar a leer lo escrito

APLICACIONES:

- Modificar un mensaje de tal forma que sea completamente ilegible a no ser que se posea la clave para volver a ponerlo en su estado original.
- Verificar que un mensaje NO ha sido modificado INTENCIONADAMENTE porun tercero.
- Verificar que “alguien” es quien realmente dice ser.

HISTORIA DE LA CRIPTOGRAFÍA

La máquina *Enigma* utilizada por los alemanes durante la II Guerra Mundial.

Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares, de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo. Posiblemente, el primer criptosistema que se conoce fuera documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente Julio César lo empleó en sus campañas, uno de los más conocidos en la literatura (según algunos autores, en realidad Julio César no usaba este sistema de sustitución, pero la atribución tiene tanto arraigo que el nombre de este método de sustitución

ha quedado para los anales de la historia). Otro de los métodos criptográficos utilizados por los griegos fue la escítala espartana, un método de trasposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar.

En 1465 el italiano Leon Battista Alberti inventó un nuevo sistema de sustitución polialfabética que supuso un gran avance de la época. Otro de los criptógrafos más importantes del siglo XVI fue el francés Blaise de Vigenère que escribió un importante tratado sobre "la escritura secreta" y que diseñó una cifra que ha llegado a nuestros días asociada a su nombre. A Selenus se le debe la obra criptográfica "Cryptomenytices et Cryptographiae" (Luneburgo, 1624). Durante los siglos XVII, XVIII y XIX, el interés de los monarcas por la criptografía fue notable. Las tropas de Felipe II emplearon durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés François Viète consiguió criptoanalizar aquel sistema para el rey de Francia, a la sazón Enrique IV, el conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. Por su parte, la reina María Estuardo, reina de Escocia, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

Durante la Primera Guerra Mundial, los Alemanes usaron el cifrado ADFGVX. Este método de cifrado es similar a la del tablero de ajedrez Polibio. Consistía en una matriz de 6 x 6 utilizado para sustituir cualquier letra del alfabeto y los números 0 a 9 con un par de letras que consiste de A, D, F, G, V, o X.

Desde el siglo XIX y hasta la Segunda Guerra Mundial, las figuras más importantes fueron la del holandés Auguste Kerckhoffs y la del prusiano Friedrich Kasiski. Pero es en el siglo XX cuando la historia de la criptografía vuelve a experimentar importantes avances. En especial durante las dos contiendas bélicas que marcaron al siglo: la Gran Guerra y la Segunda Guerra Mundial. A partir del siglo XX, la criptografía usa una nueva herramienta que permitirá conseguir mejores y más seguras cifras: las máquinas de cálculo. La más conocida de las máquinas de cifrado posiblemente sea la máquina alemana Enigma: una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la criptografía como en el del criptoanálisis no empezaron hasta entonces.

Tras la conclusión de la Segunda Guerra Mundial, la criptografía tiene un desarrollo teórico importante, siendo Claude Shannon y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas. A

mediados de los años 70, el Departamento de Normas y Estándares norteamericano publica el primer diseño lógico de un cifrador que estaría llamado a ser el principal sistema criptográfico de finales de siglo: el Estándar de Cifrado de Datos o DES. En esas mismas fechas ya se empezaba a gestar lo que sería la, hasta ahora, última revolución de la criptografía teórica y práctica: los sistemas asimétricos. Estos sistemas supusieron un salto cualitativo importante, ya que permitieron introducir la criptografía en otros campos que hoy día son esenciales, como el de la firma digital.

TIPOS DE CRIPTOGRAFÍA

- Criptografía simétrica, también conocida como "*criptografía clásica*" o de "*llave privada*". Este tipo de criptografía es anterior al nacimiento de los ordenadores.

- Criptografía asimétrica, también conocida como "*criptografía moderna*" o de "*llave pública*". Este tipo de criptografía se desarrollo en los años 70 y utiliza complicados algoritmos matemáticos relacionados con *números primos* y *curvas elípticas*.

CONTROVERSIAS

Respecto al uso de la criptografía existe una gran controversia sobre si se debe o no utilizar "*criptografía fuerte*". Este tipo de criptografía es muy segura y es prácticamente imposible desencriptar mensajes encriptados con este tipo de criptografía.
La controversia surge ya que este tipo de criptografía podría ser utilizado por organizaciones criminales para asegurar sus comunicaciones y de esta forma poder cometer sus actividades criminales de una forma más segura.
Hay "interesados" en que este tipo de criptografía no se utilize dando argumentos como el anterior. Argumento muy contundente.
Pero hay otro argumento también contundente y es el DERECHO A LA INTIMIDAD.

Firma digital

La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la *identidad* de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la *integridad* del documento o mensaje.

La firma electrónica, como la firma hológrafa (autógrafa, manuscrita), puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído y, en su defecto mostrar el tipo de firma y garantizar que no se pueda modificar su contenido.

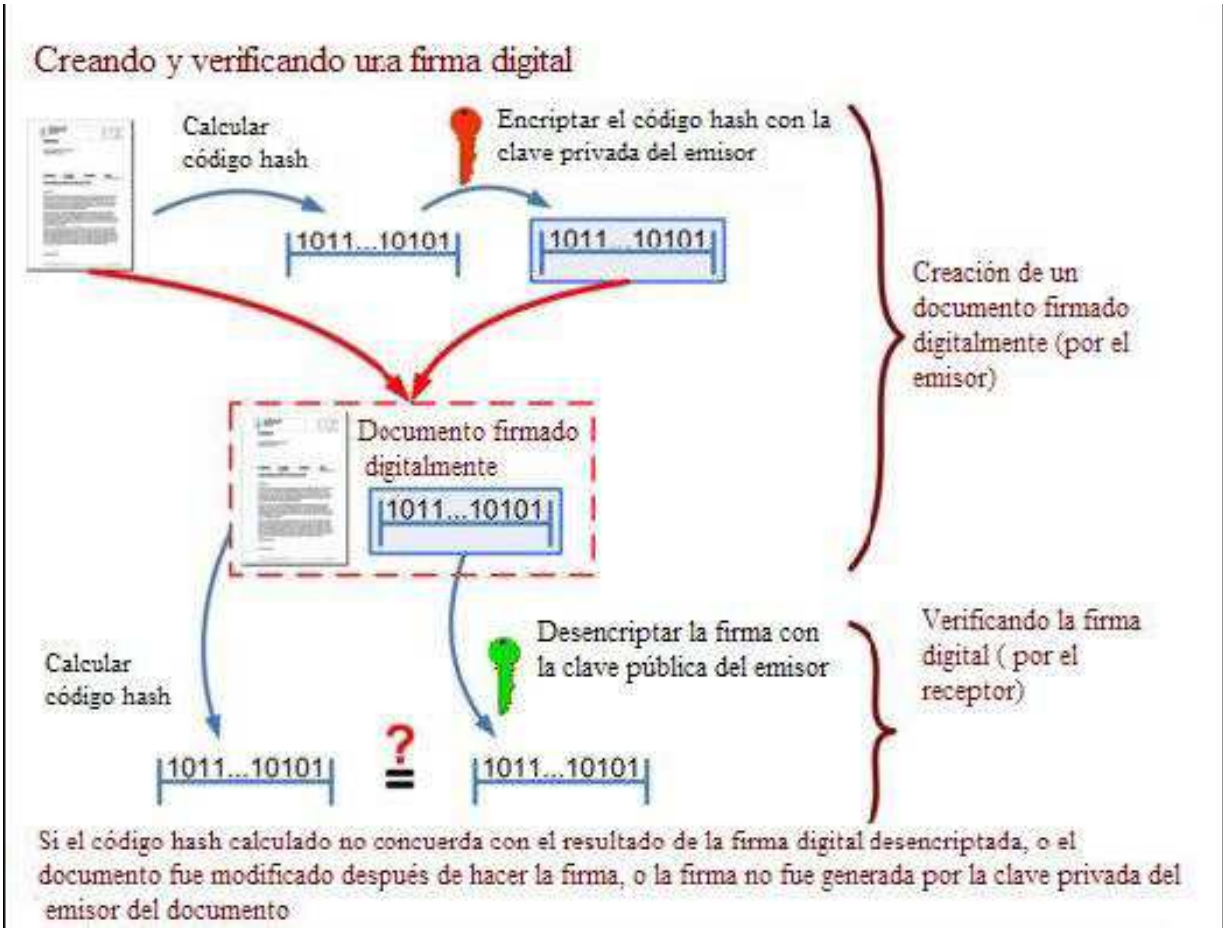
Terminología

Los términos de firma digital y firma electrónica se utilizan con frecuencia como sinónimos, pero este uso en realidad es incorrecto.

Mientras que firma digital hace referencia a una serie de métodos criptográficos, firma electrónica es un término de naturaleza fundamentalmente legal y más amplio desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos.

Un ejemplo claro de la importancia de esta distinción es el uso por la Comisión europea. En el desarrollo de la Directiva europea 1999/93/CE que establece un marco europeo común para la firma electrónica empezó utilizando el término de firma digital en el primer borrador, pero finalmente acabó utilizando el término de firma electrónica para desacoplar la regulación legal de este tipo de firma de la tecnología utilizada en su implementación.

La teoría



Mecánica de la generación y comprobación de una firma digital.

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital. El software de firma digital debe además efectuar varias validaciones, entre las cuales podemos mencionar:

- Vigencia del certificado digital del firmante,
- Revocación del certificado digital del firmante (puede ser por OCSP o CRL),
- Inclusión de sello de tiempo.

La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente. Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que

identifica inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. Ello no obstante, este tipo de operaciones no están pensadas para que las lleve a cabo el usuario, sino que se utiliza software que automatiza tanto la función de calcular el valor hash como su verificación posterior.

Las posibilidades de red

Para que sea de utilidad, una función *hash* debe satisfacer dos importantes requisitos:

1. debe ser difícil encontrar dos documentos cuyo valor para la función *hash* sea idéntico.
2. dado uno de estos valores, debe ser imposible producir un documento con sentido que de lugar a ese *hash*.

Existen funciones *hash* específicamente designadas para satisfacer estas dos importantes propiedades. SHA y MD5 son dos ejemplos de este tipo de algoritmos.

Algunos sistemas de cifrado de clave pública se pueden usar para firmar documentos. El firmante cifra el *hash* calculado de un documento con su clave privada y cualquiera que quiera comprobar la firma y ver el documento, no tiene más que usar la clave pública del firmante para descifrar el *hash*, y comprobar que es el que corresponde al documento.

La solución

Un algoritmo efectivo debe hacer uso de un sistema de clave pública para cifrar sólo la firma. En particular, el valor "hash" se cifra mediante el uso de la clave privada del firmante, de modo que cualquiera pueda comprobar la firma usando la clave pública correspondiente. El documento firmado se puede enviar usando cualquier otro algoritmo de cifrado, o incluso ninguno si es un documento público. Si el documento se modifica, la comprobación de la firma fallará, pero esto es precisamente lo que la verificación se supone que debe descubrir.

El Digital Signature Algorithm es un algoritmo de firmado de clave pública que funciona como hemos descrito. DSA es el algoritmo principal de firmado que se usa en GnuPG.

Formato de la firma electrónica

Regulaciones en diferentes países

El marco común de firma electrónica de la Unión Europea

El mercado interior de la Unión Europea implica un espacio sin fronteras interiores en el que está garantizada la libre circulación de mercancías. Deben satisfacerse los requisitos esenciales específicos de los productos de firma electrónica a fin de garantizar la libre circulación en el mercado interior y fomentar la confianza en la firma electrónica.

En ese sentido la Directiva 1999/93/CE sienta un marco común para la firma electrónica que se concretó con la transposición de la Directiva a las diferentes legislaciones nacionales de los países miembros.

Ley sobre firma electrónica en Chile

Esta ley fue publicada el 15 de septiembre del año 2003 por el Ministerio Secretaría General de la Presidencia, la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma, reconoce que los órganos del Estado podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica simple. Igualmente señala que estos actos, contratos y documentos, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos en soporte de papel.

Firma Digital en Costa Rica

En Costa Rica, la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley 8454) es firmada el 22 de agosto del 2005. Esta Ley faculta la posibilidad de vincular jurídicamente a los actores que participan en transacciones electrónicas, lo que permite llevar al mundo virtual transacciones o procesos que anteriormente requerían el uso de documentos físicos para tener validez jurídica, bajo el precepto de presunción de autoría y responsabilidad, además lo anterior sin demérito del cumplimiento de los requisitos de las formalidades legales según negocio jurídico.

La ley de firma electrónica en España

En España existe la Ley 59/2003, de Firma electrónica, que define tres tipos de firma:

- Simple. Datos que puedan ser usados para identificar al firmante (autenticidad)
- Avanzada. Además de identificar al firmante permite garantizar la integridad del documento y la integridad de la clave usada, utilizando para ello un DSCF (dispositivo seguro de creación de firma, el DNI electrónico). Se emplean técnicas de PKI.
- Reconocida. Es la firma avanzada y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante). En ocasiones, esta firma se denomina *cualificada* por traducción del término inglés *qualified* que aparece en la Directiva Europea de Firma Electrónica.

Firma Electrónica en Guatemala

En Guatemala, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas (Decreto 47-2008), fue publicada en el diario oficial el 23 de septiembre de 2008. El Ministerio de Economía de ese país tiene bajo su responsabilidad el regular este tema, y abrió en el mes de Junio de 2009 el Registro de Prestadores de Servicios de Certificación, publicando su sitio web con copia de la ley e información importante sobre el tema.

Firma Digital en Nicaragua

El 2 de julio de 2010 se aprobó en Nicaragua la Ley de Firma Electrónica , siendo la Dirección General de Tecnología, adscrita al Ministerio de Hacienda y Crédito Público, la entidad acreditadora de la firma electrónica.

La Ley de firma digital en Perú

En el Perú se ha dictado la Ley de Firmas y Certificados Digitales (Ley 27269), la cual regula la utilización de la firma electrónica, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otro análoga que conlleve manifestación de voluntad.

Aplicaciones

- Mensajes con autenticidad asegurada
- Mensajes sin posibilidad de repudio
- Contratos comerciales electrónicos
- Factura Electrónica
- Desmaterialización de documentos
- Transacciones comerciales electrónicas
- Invitación electrónica
- Dinero electrónico
- Notificaciones judiciales electrónicas
- Voto electrónico
- Decretos ejecutivos (gobierno)
- Créditos de seguridad social
- Contratación pública
- Sellado de tiempo

Espero y te sea útil esta pequeña aportación

Realizado por Hellis Molina Pogan

Saludos maestra: A.L.T.J.