IDENTIDAD ELECTRÓNICA

SUSCERTE
Superintendencia de Servicios de Certificación Electrónica

Gobierno Bolivariano de Venezuela | Ministerio para el Poder Popular para **Ciencia, Tecnología e Industrias Intermedias**

Venezuela
AHORA ES DE TODOS

Directorio

Hugo Rafael Chávez Frías
Presidente de la República Bolivariana de Venezuela

Jesse Chacón Escamillo
Ministro del Poder Popular para Ciencia, Tecnología e Industrias Intermedias

Niurka Hernández González
Superintendente de Servicios de Certificación Electrónica (SUSCERTE)

Gabriel Moliné
Director del Sistema Nacional de Gestión de Incidentes Telemáticos (VENCERT)
Adjunto a la Superintendente de Servicios de Certificación Electrónica (SUSCERTE)

Argenis Grillo
Asesor Legal

Sara Campins
Directora de Gestión Administrativa

Francis Ferrer
Directora de Inspección y Fiscalización

Piero Mangialomini
Director de Registro y Acreditación

Luisalba Blanco A.
Directora de Investigación y Desarrollo Tecnológico

Ildelen Pinzón
Recursos Humanos

Silvia Pernía
Relaciones Institucionales

Jorge Molero
Asesoría Técnica

Créditos

Redactores:
Richard Hernández
Kranya Berríos
Victor González

Revisión:
Jorge Molero
Luisalba Blanco A.
Silvia Pernía
María Esperanza Pérez

Colaboradores:
Emerson Medina
Lermi La Roche
Caribay Medina
Mayda Merchán
Esther González
Valleigny Crespo

Diseño gráfico:
Johann Sahmkow

Índice

INTRODUCCIÓN

La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), enmarcada en su misión de fortalecer el Sistema Nacional de Seguridad de la Información e impulsar el funcionamiento confiable del Sistema Nacional de Certificación Electrónica, publica su primer Libro titulado "Identidad Electrónica", el cual se perfila como una herramienta útil de divulgación para acercar al lector a estos temas; tópicos que deben ser del conocimiento público para afianzar la soberanía tecnológica y dar continuidad a la visión de la Institución en su contribución por la aplicación de políticas de inclusión que consoliden la transformación del país y la calidad de vida, mediante el uso masivo de plataformas tecnológicas seguras.

Dentro de este orden de ideas, el libro está estructurado en tres capítulos, el primero denominado Criptografía, donde se plantea la necesidad de la seguridad de la información en las organizaciones públicas y privadas, aspecto de gran importancia durante la evolución de la sociedad y donde su implementación se ha basado en el uso de un conjunto de reglas, planes y acciones que permiten asegurar la información manteniendo las propiedades de confidencialidad, integridad y disponibilidad de la misma.

En este contexto entra en juego la Criptografía como “técnica, ciencia o arte de la escritura secreta”, que se conoce desde hace casi cinco mil (5000) años y cuyo principio básico ha sido mantener la privacidad de la comunicación entre dos personas o entes, alterando el mensaje original de modo que sea incomprensible a otra diferente del destinatario.

El Segundo Capítulo, llamado Identidad Electrónica, refleja el concepto de identidad y cómo ésta define a un individuo o colectividad, de manera que el lector pueda entender perfectamente su significado e importancia y cómo ésta se asocia con los aspectos más sencillos y comunes de la cotidianidad.

Por otro lado, en este capítulo se precisan algunos de los casos exitosos dentro y fuera de las fronteras venezolanas con respecto a la Identidad Electrónica, gracias a la aplicación de estas herramientas.

El tercer capítulo, comprende el tema de la Certificación Electrónica, sus beneficios para el Estado y la ciudadanía, el Marco Legal que soporta su desarrollo, ámbito de aplicación y descripción de la Infraestructura Nacional de Certificación Electrónica, encabezada por SUSCERTE como la Autoridad de Certificación Raíz del Estado Venezolano.

En ese sentido, se dan a conocer los requisitos que el solicitante debe presentar para obtener la acreditación como Proveedor de Servicios de Certificación (PSC); además se mencionan los diferentes proyectos que SUSCERTE lleva a cabo en la actualidad, finalizando el capítulo con la Firma Electrónica y las características del certificado electrónico.

Esta publicación es el resultado del trabajo mancomunado realizado por el equipo SUSCERTE, quienes con su mayor esfuerzo hicieron realidad esta edición para generar en los ciudadanos y ciudadanas una verdadera identidad electrónica.

CAPÍTULO I CRIPTOGRAFÍA

La necesidad de seguridad de la información en las organizaciones públicas y privadas, ha crecido sorprendentemente en las últimas décadas. Antes del uso de la computadora, la seguridad de la información se obtenía utilizando medios físicos cuyo propósito era proteger el acceso a los documentos que contenían dicha información.

Por ejemplo, se llegaron a usar y actualmente se siguen utilizando como lineamientos de seguridad, las "cajas fuertes" para resguardar los documentos críticos para la organización tales como, contratos, las contraseñas escritas, entre otros.

Es importante destacar que también se usaban medidas procedimentales para asegurar y destruir la información escrita. Para asegurarla se pusieron en práctica los "procedimientos de clasificación de documentos" cuyo propósito no era otro, sino separar la documentación y resguardarla de acuerdo a su grado de importancia. Así mismo, para destruirla, se recurrió al uso de maquinarias para tales fines, donde la finalidad era destrozar el documento.

El término de seguridad de la información surge por la necesidad de proteger su contenido y a los sistemas que la administran. Actualmente, los términos de seguridad y de seguridad de la información son utilizados en nuestra cotidianidad. A continuación mostraremos las definiciones de cada uno de ellos.

De acuerdo con el diccionario de la Real Academia Española, la seguridad es:

Cualidad de seguro.

Dicho de un mecanismo: Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente.

De acuerdo al Ingeniero en Computación Gibran Granados Paredes en su publicación "Introducción a la Criptografía", se puede hablar de la Seguridad de la Información como el conjunto de reglas, planes y acciones que permiten asegurar la información manteniendo las propiedades de confidencialidad, integridad y disponibilidad de la misma.

1. La confidencialidad es la propiedad que posee un documento o mensaje de ser leído o entendido por el destinatario designado, es decir, consiste en que la información sea accesible sólo para aquellos que están autorizados.

2. La integridad radica en que la información sólo puede ser creada, modificada e incluso hasta borrada por quien esté autorizado a hacerlo.

3. La disponibilidad se fundamenta en que la información debe ser accesible por las personas autorizadas para su consulta o modificación de ser necesario.

Dentro de este orden de ideas, es importante resaltar otras visiones en cuanto a las propiedades de la seguridad de la información (confidencialidad, integridad y disponibilidad) enmarcadas en la criptografía. **En un artículo publicado en internet con el nombre "Integridad y Confidencialidad de la Información", la Ingeniera Clara Baonza, define la confidencialidad, integridad y disponibilidad de la siguiente manera:**

1. Confidencialidad: Necesidad de que esa información únicamente sea conocida por personas autorizadas.

2. Integridad: Hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación, como por ejemplo, la huella digital.

3. Disponibilidad: Capacidad de que la información este siempre disponible para ser procesada por las personas autorizadas.

De acuerdo con las definiciones anteriores, para que exista seguridad de la información hay que garantizar las propiedades de confidencialidad, integridad y disponibilidad. Para garantizar las propiedades de confidencialidad e integridad se puede usar los sistemas criptográficos, los cuales se apoyan en algoritmos complejos, los cuales se han visto fortalecidos con el desarrollo que ha tenido la criptografía. En los próximos párrafos se estarán revisando estas dos propiedades y cómo la criptografía ayuda a asegurar su cumplimiento.

A continuación se muestra lo que en un principio se entiende como “una comunicación habitual”, en este caso no existe ningún problema de seguridad informática. El mensaje que se envía, se recibe sin alteración alguna. (Ver figura N° 1.1)

Figura N° 1.1. Comunicación Habitual.
Fuente: (SUSCERTE, 2009)

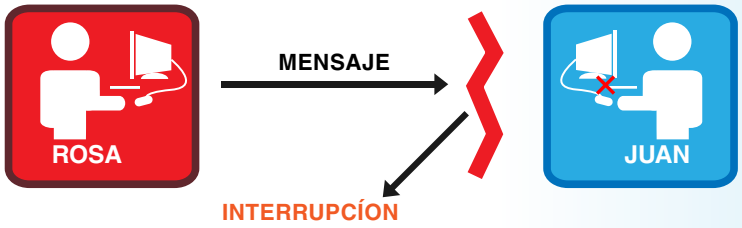


Figura N° 1.2. Comunicación con Interrupción.
Fuente: (SUSCERTE, 2009)

En el segundo caso se muestra uno de los problemas más grandes que existen en la actualidad, la interrupción de la transmisión del mensaje (ocasionado en la mayoría de los casos por virus, mal estado del cableado, etc.) que puede ser ocasionada por fallo del canal o de algún elemento del sistema de comunicación, ya sea de forma natural o intencional. Esto es traducido a un problema de disponibilidad. (Ver figura N° 1.2)

La interceptación de los datos por una intrusa o intruso (una intrusa o intruso, es una persona y/o ente externa al sistema), es algo muy común dentro de las comunicaciones, ya que muchas de las transmisiones son enviadas mediante protocolos que son conocidos por todos y a los mensajes no se les hace ningún tratamiento especial en cuanto a seguridad, en otras palabras, viajan tal cual se generan. Lo único que se hace es escuchar y/o visualizar todo lo que pasa por el canal sin alterar nada. Este es un problema de confidencialidad. (Ver figura N° 1.3)

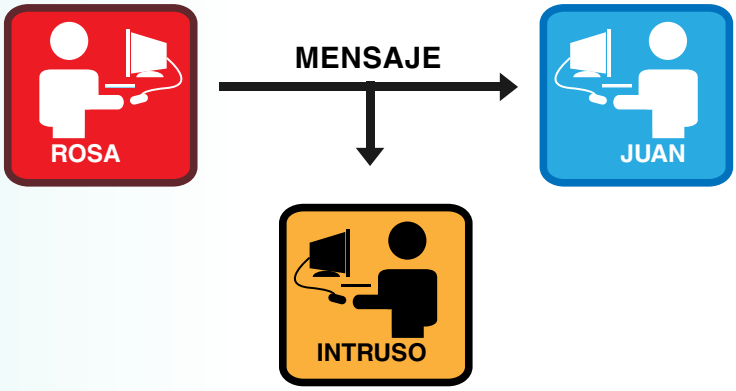


Figura N° 1.3. Comunicación con Interceptación.
Fuente: (SUSCERTE, 2009)

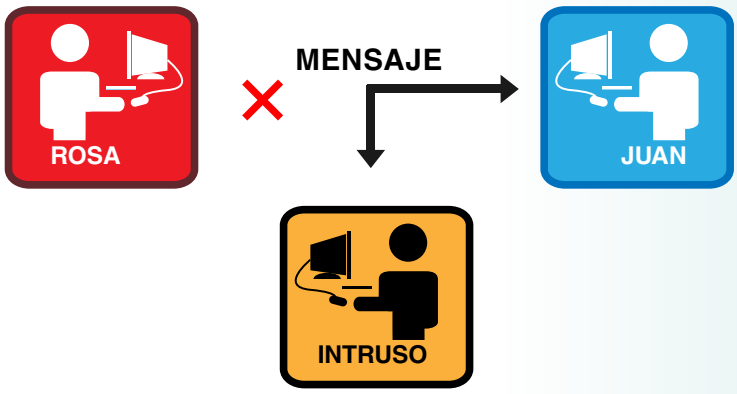


Figura N° 1.4. Generación de una Comunicación Falseada.
Fuente: (SUSCERTE, 2008)

Otra vulnerabilidad existente en las comunicaciones, es el problema de la generación de mensajes falsos, los cuales se producen cuando la intrusa o intruso genera un mensaje engañando al receptor, haciéndolo creer que es un emisor válido. Esto se traduce en un problema de integridad.
(Ver figura N° 1.4)

Finalmente tenemos la falsificación, la cual se produce cuando la intrusa o intruso captura un mensaje, se adueña de él y de la identidad del emisor y genera un nuevo mensaje con la identidad del emisor. Este es un problema de integridad y confidencialidad. (Ver figura N° 1.5)

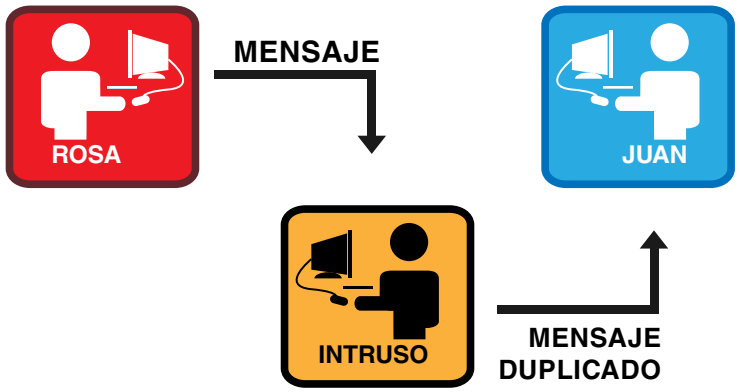


Figura N° 1.5. Comunicación con Falsificación.
Fuente: (SUSCERTE, 2009)

Después de observar los diferentes casos donde se compromete de alguna manera la información, se puede inferir que evitando los problemas de **disponibilidad, integridad y confidencialidad,** se tendría un sistema **"seguro".** Para lograr esto se debe aislar el sistema de los intrusos y hacerlo anti-fallos (a prueba de toda falla), lo cual es prácticamente imposible; lo ideal sería crear mecanismos que garanticen en cierta medida las propiedades de seguridad de la información.

La disponibilidad, generalmente, se trata de solucionar con sistemas redundantes. **La confidencialidad** se puede lograr usando un mecanismo que, aunque sea robada la información, permita que no se pueda acceder a ésta.

La integridad es más difícil de lograr, para ello se implementan varios mecanismos que garantizan la identidad de una persona y/o ente autorizado por el sistema para crear o hacer modificaciones a la información, de tal forma que se puede verificar posteriormente quién la creó o modificó. Además estos mecanismos permiten ver si la información ya creada, ha sufrido o no, alguna modificación no autorizada.

Los mecanismos para garantizar la integridad y la confidencialidad se implementan con sistemas criptográficos de ahí la importancia de la criptografía en la seguridad informática en los sistemas actuales.

Con el uso de las computadoras, y más aún con la llegada de Internet, fue indispensable el uso de herramientas automatizadas para la protección de archivos y otro tipo de información almacenada en la computadora. Algunas de estas herramientas son los cortafuegos **(también llamados firewalls),** los sistemas detectores de intrusos y el uso de sistemas criptográficos. Estas herramientas no sólo permiten proteger a la información, sino también a los sistemas informáticos que son los encargados de administrarla.

La palabra **criptografía** proviene según la Real Academia Española, de las palabras griegas **"criptos"** (oculto) y **"grafos"** (escritura). **La criptografía es la técnica, ciencia o arte de la escritura secreta,** su principio básico es mantener la privacidad de la comunicación entre dos personas, entes gubernamentales ó empresas privadas, entre otros, alterando el mensaje original de modo que sea incomprensible a toda persona distinta del destinatario; a esto se le puede atribuir de cierta forma la autenticación de quien manda el mensaje, de modo que un tercero no pueda hacerse pasar por el emisor.

A la transformación del mensaje original en el mensaje cifrado se le llama **cifrar,** y a la operación inversa, se le llama **descifrar;** estos pasos se realizan mediante un conjunto de reglas preestablecidas entre los comunicantes a la que se le denomina clave.

De acuerdo a lo expresado por **Andrew Nash, William Duane, Celia Joseph y Derek Brink** en el ejemplar **"PKI Infraestructura de Clave Pública",** la criptografía puede ser vista al momento de ser utilizada, como un proceso donde los cálculos matemáticos realizados para camuflar o cifrar cierta información con valor confidencial suelen ser sencillos. Al mismo tiempo el autor resalta que el proceso de descifrar la información, resulta bastante complicado, ya que sin saber la clave (método utilizado para camuflar la información) para cifrar el mensaje, es difícil de traducir.

Dentro de este orden de ideas, se puede deducir que el término clave no es mas que el parámetro que indicará las condiciones del cambio de un documento legible a un documento codificado. Tener la clave es adquirir el conocimiento necesario para la utilización de los códigos y de ésta manera poder cifrar y descifrar información. Es importante dejar claro, que tanto el emisor como el receptor deben definir la clave con la que se realizará el intercambio de información confidencial, pues ella es la que iniciará el proceso de codificación y decodificación del texto.

Cuando se tiene la clave, es posible leer el mensaje cifrado recibido, pero cuando no se tiene, es prácticamente imposible conseguir entender el conjunto desordenado de letras y números que estén en el documento recibido.

A continuación se presenta un ejemplo con el propósito de explicar lo anteriormente expuesto.

Ejemplo

1 Rosa desea enviar un mensaje a Juan, este mensaje es de carácter confidencial para ambos, por lo tanto Rosa hace uso de la **criptografía,** con la finalidad de garantizar que solo Juan pueda entender el mensaje. Es importante destacar que **Rosa y Juan** previamente establecieron la clave o medio a utilizar para cifrar o descifrar el mensaje. (Ver ilustración N° 1.1)

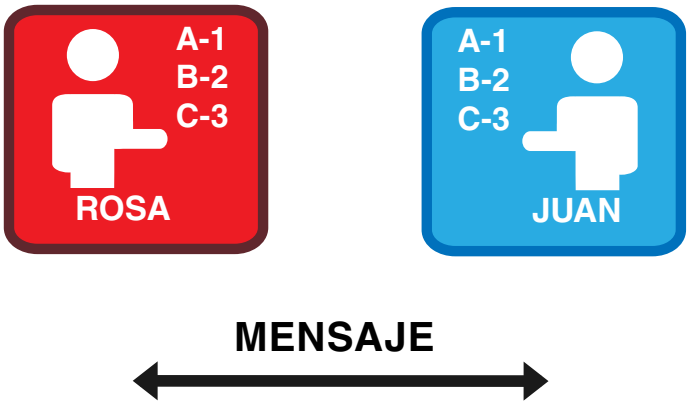


Ilustración N° 1.1 Envío de mensaje.
Fuente: (SUSCERTE, 2009)

Para este caso, **Rosa y Juan** establecieron como clave un método de sustitución bastante sencilla, que consiste en sustituir palabras del alfabeto por números, es decir, la letra **"a"** sera el numero **"1"** y así sucesivamente con el resto del alfabeto. Para evitar confusiones con la combinación de números después del **"10",** de igual manera, se acordó separar cada letra con un asterisco **(*)** para su rápida comprensión. Por ejemplo, el nombre de **"Juan"** se escribirá como **"10*22*1*14".**
(Ver tabla N° 1.1)

a	1
b	2
c	3
d	4
e	5
f	6
g	7
h	8
i	9
j	10
k	11
l	12
m	13
n	14

ñ	15
o	16
p	17
q	18
r	19
s	20
t	21
u	22
v	23
w	24
x	25
y	26
z	27

Tabla N° 1.1. Sustitución de letras por números.
Fuente: (SUSCERTE, 2009)

Visto de esta forma, si el mensaje de **Rosa** dice lo siguiente "Te espero hoy en el lugar acordado para darte la información que me pediste sobre Nicolás", utilizando la clave de sustitución explicada con anterioridad, resultaría lo siguiente **"21*5 5*20*17*5*19*16 8*16*26 5*14 5*12 12*22*7*1*19 1*3*16*19*4*1*4*16 17*1*19*1 4*1*19*21*5 12*1 9*14*6*16*19*13*1*3*9*16*14 18*22*5 13*5 17*5*4*9*20*21*5*20 20*16*2*19*5 14*9*3*16*12*1*20".** (Ver figura N° 1.6)

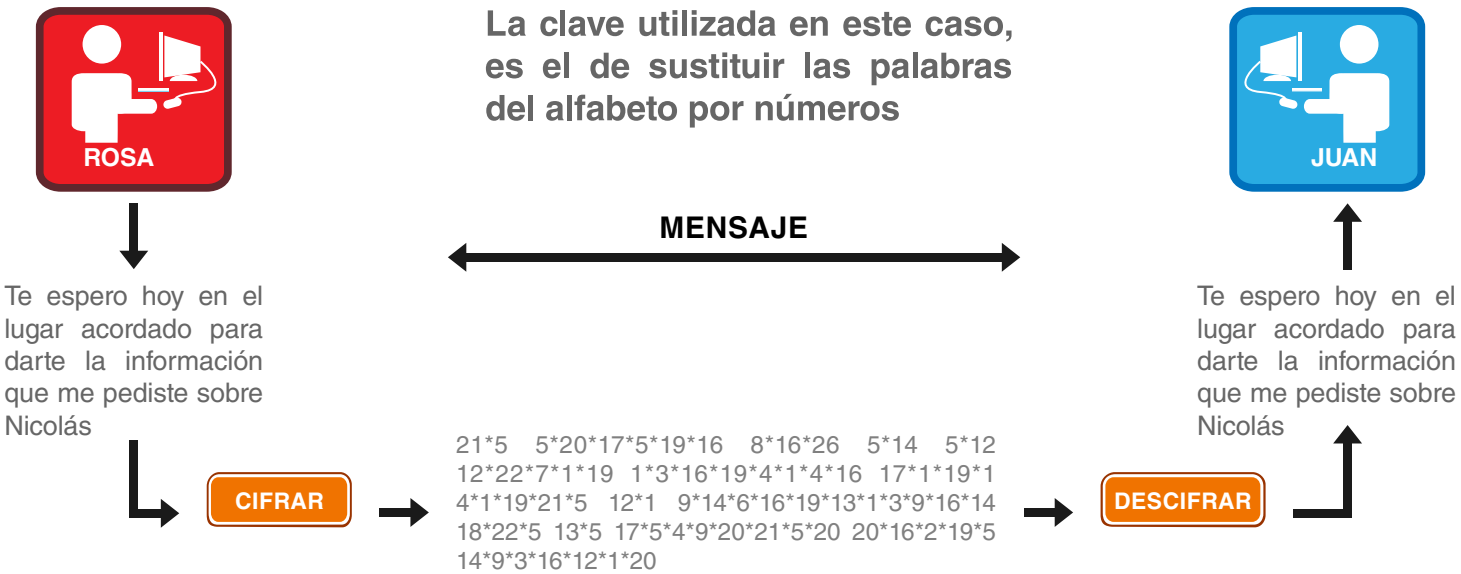


Figura N° 1.6. Intercambio de Información Cifrada.
Fuente: (SUSCERTE, 2009)

PROCESO CRIPTOGRÁFICO

Desde hace algún tiempo la criptografía se ha afianzado como herramienta de seguridad de la información en las Tecnologías de Información y Comunicación (TICs), constituyéndose como elemento indispensable para garantizar la debida protección en el manejo de la información.

¿Cómo funciona?

Haciendo uso del ejemplo anterior (Ver figura N° 1.6), se explica como se cifran mensajes con el propósito de brindar un mínimo de seguridad a la información que se desee transmitir. Observen que Rosa y Juan son, como se mencionó con anterioridad, respectivamente, el emisor y receptor de un determinado mensaje. Rosa transforma el mensaje original (texto plano o texto fuente), mediante un determinado procedimiento de cifrado controlado por una clave, el mensaje es enviado por un canal público. El destinatario (Juan) al tener conocimiento de la clave, previamente establecida, transforma ese mensaje cifrado en el texto fuente, recuperando así la información original enviada por Rosa.

Es importante resaltar que el proceso de cifrar es llevado a cabo por el emisor o dueño de la información y el proceso de descifrar, en la mayoría de los casos es realizado por el receptor o destinatario. El tipo particular de transmisión aplicada al texto fuente o las características de las claves utilizadas marcan la diferencia entre los diversos métodos criptográficos. Una primera clasificación con base en las claves utilizadas pueden ser las siguientes:

Cifrado Simétrico

Los sistemas de cifrado simétrico, consisten en la utilización de la misma clave para cifrar y descifrar una información. Este tipo de fuentes posee como ventaja la sencillez para su aplicación, ya que se utiliza la misma clave para cifrar y descifrar la información. El principal problema de éste tipo de técnica reside en que se debe disponer de un medio seguro para el intercambio de la clave entre el emisor y el receptor.

Se recomienda para emplear el cifrado simétrico la utilización de una clave difícil de adivinar, ya que hoy en día, existen aplicaciones y equipos de computación robustos usados con la finalidad de descifrar claves muy rápidamente. Es muy común en las personas colocar fechas de cumpleaños, aniversario, entre otros para crear la clave, ésto es contraproducente ya que una tercera persona interesada en descifrar la información utilizará estos datos en primera instancia, por lo tanto se recomienda tomar números aleatorios y fáciles de recordar, además dicha clave debe contener robustez en su longitud. Se considera una clave robusta (fuerte) cuando esta compuesta por números, letras (algunas en mayúsculas) y signos, además de tener una longitud de por lo mínimo doce (12) caracteres. Por ejemplo: "Adm1n1s7r4d0r".

A continuación se presenta un diagrama donde se puede constatar el funcionamiento del cifrado simétrico, para efectos de ejemplo se contará con los dos personajes Rosa y Juan, donde Rosa desea enviar cierta información confidencial para Juan. Haciendo uso de su clave pública (conocida por ambos) cifra la información, Juan al percatarse que ya le llegó la información se dispone a utilizar la clave pública (de Rosa) para descifrar la información enviada. (Ver figura N° 1.7)

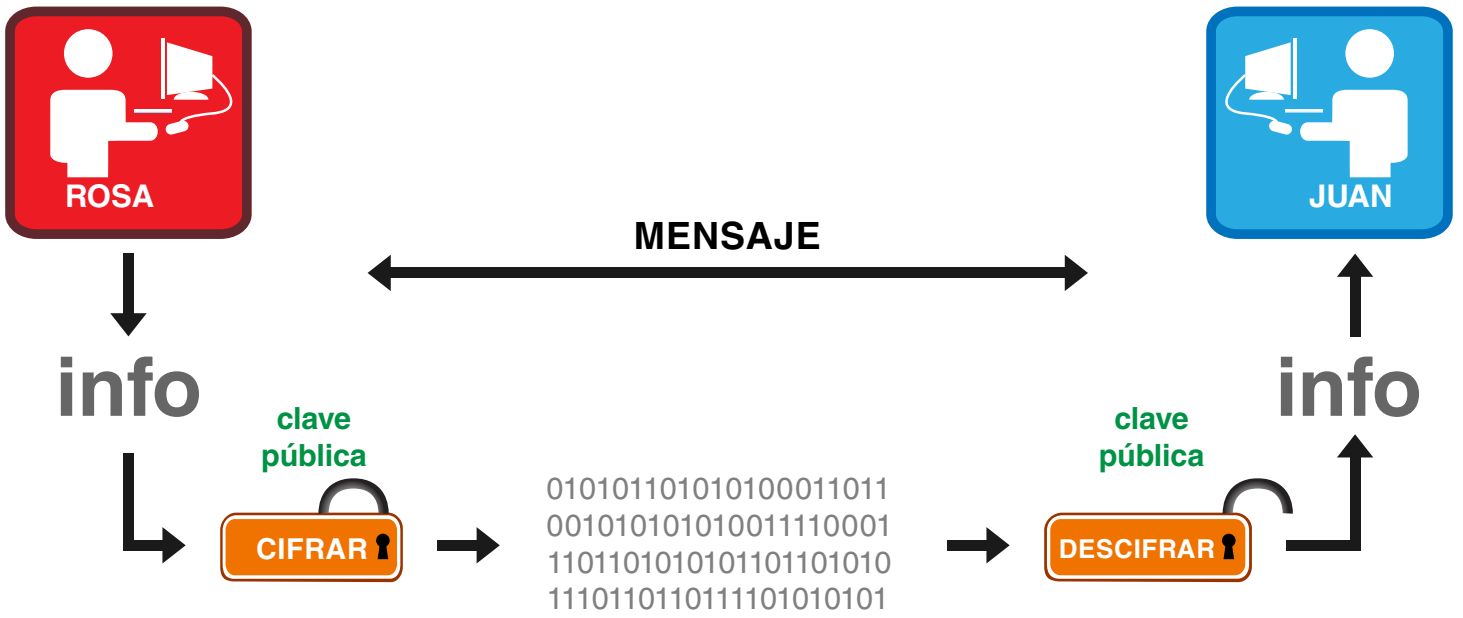


Figura N° 1.7. Cifrado Simétrico.
Fuente: (SUSCERTE, 2009)

Cifrado Asimétrico

El cifrado asimétrico, consiste en que las dos claves pertenecen a la misma persona a la que se 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 para que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

Para enviar un mensaje, el remitente usa la clave pública del destinatario y así se cifra el mensaje. Una vez cifrado, solamente con la clave privada del destinatario se puede descifrar; ni siquiera quien ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se desee comunicar con el destinatario lo pueda hacer.

A continuación se presenta un ejemplo de diagrama donde se puede visualizar el funcionamiento del cifrado asimétrico, para tal efecto se contará con dos personajes Juan y Rosa, donde Juan desea enviar cierta información confidencial para Rosa. Juan hace uso de la clave pública de Rosa para cifrar la información que desea enviar, Rosa al percatarse que ya le llegó la información enviada por Juan, se dispone a descifrar el contenido de la información mediante el uso de su clave privada, de este modo Rosa recibe de forma segura la información. (Ver figura N° 1.8)

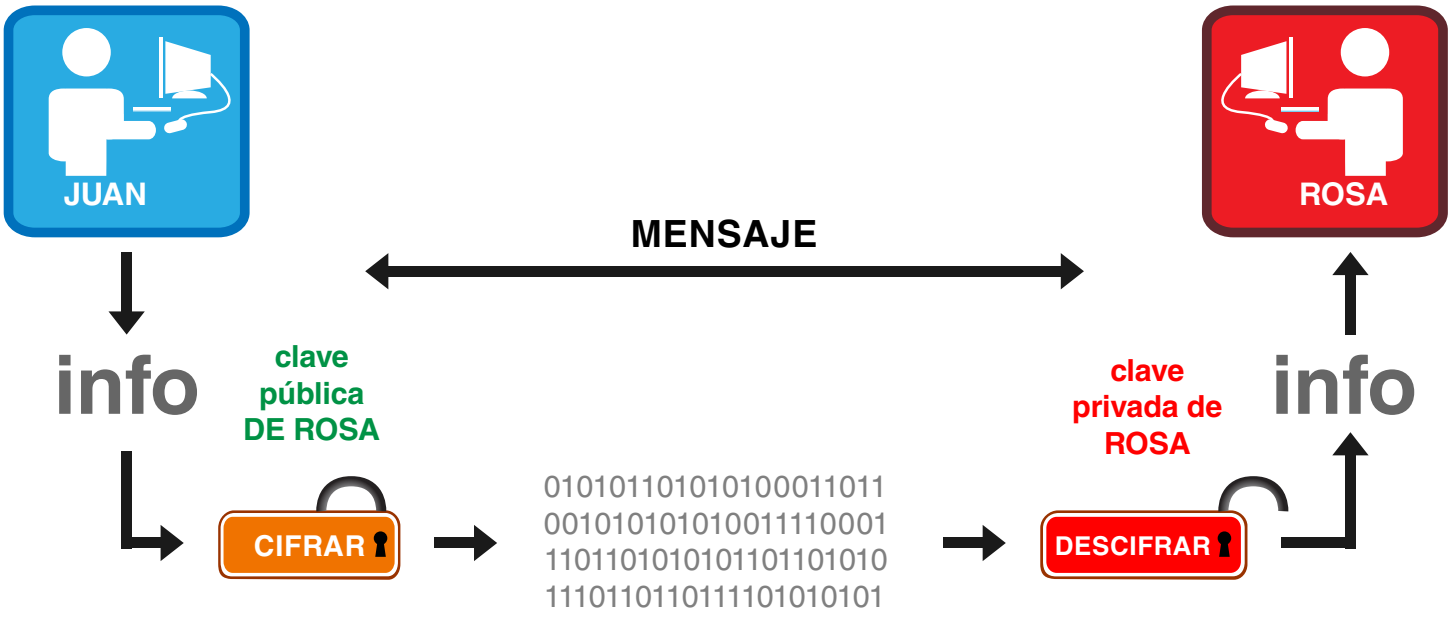


Figura N° 1.8. Cifrado Asimétrico.
Fuente: (SUSCERTE, 2009)

Cifrado Híbrido

Es el sistema de cifrado que usan tanto los sistemas de clave simétrica como asimétrica. Funciona mediante el cifrado de clave pública para compartir un código para el cifrado simétrico. En cada mensaje, la clave simétrica utilizada es diferente por lo que si un atacante pudiera descubrir ésta, solo le valdría para ese mensaje y no para los restantes.

La clave simétrica es cifrada con la clave pública, 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 simétrica y acto seguido usa la clave simétrica para descifrar el mensaje. (Ver figura N° 1.9)

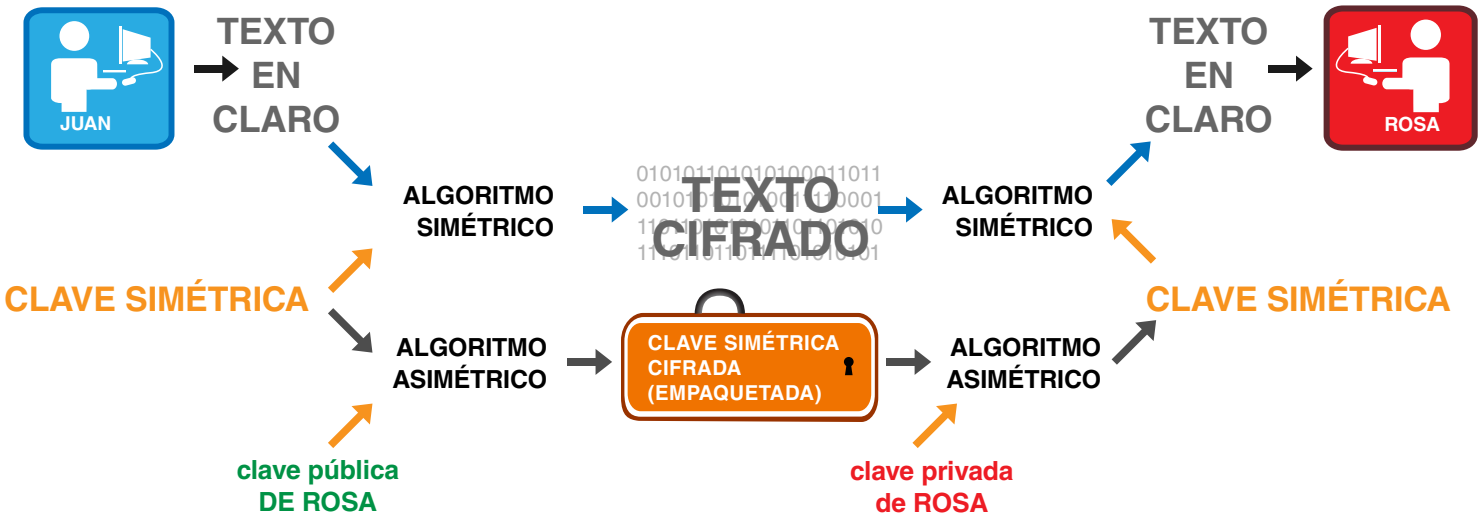


Figura N° 1.9. Cifrado Híbrido.
Fuente: (SUSCERTE, 2009)

CAPÍTULO II
IDENTIDAD ELECTRÓNICA

El Diccionario de la Real Academia Española define identidad como un "Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás." (Diccionario de la Lengua Española, 2001). La identidad es una necesidad básica del ser humano para poder responder a la pregunta ¿quién soy yo?, y es tan necesario como los sentimientos, emociones o el alimentarnos, y está estrechamente relacionado con la autoestima de la persona.

Tal como lo declara la Ley Orgánica de Identificación de Venezuela, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.458 de fecha 14 de junio de 2.006, en su artículo 1:

"La presente Ley tiene por objeto regular y garantizar la identificación de todos los venezolanos y venezolanas que se encuentren dentro y fuera del territorio nacional, de conformidad con lo establecido en la Constitución de la República Bolivariana de Venezuela", por lo tanto, el Estado está en la obligación de facilitársela".

Cuando se habla de identidad, se asocia directamente con el proceso que permite lograr su identificación, el reconocimiento de las características que forman parte de algo o de alguien para poder asociar esas características con ese algo o ese alguien. Pero esta definición, más que aclarar el concepto lo puede llegar a confundir. Por ejemplo: Se puede reconocer cuáles son los meses del año que terminan con la letra "o"; se reconoce que dicha característica se asocia con los meses de Enero, Febrero, Marzo, Mayo, Junio, Julio y Agosto; en cambio, resultará distinto reconocer los meses que terminan con la vocal "e": Septiembre, Octubre, Noviembre y Diciembre. Un sólo mes se asocia con la terminación en la letra "i", que es el mes de Abril. De acuerdo al ejemplo anterior, se pueden identificar los meses del año según su terminación.

La identidad de una persona, asocia el proceso de identificación entre la persona y la identidad que debe contener. Hay personas que tienen señas muy particulares, como pueden ser lunares, formas de las orejas, etc., pero también existen las huellas dactilares, el iris y la cadena de ADN, como características propias de cada persona. Cada una de estas características pueden ayudar a reconocer la identificación de una persona, con la salvedad de que el procedimiento para lograr su identificación debe ser del uso de dispositivos especiales que permitan leer y comparar para asociar directamente con el que la persona tiene.

En los procesos electorales o de consulta organizados por el Consejo Nacional Electoral de la República Bolivariana de Venezuela, se viene utilizando para la identificación del ciudadano o ciudadana quien decide participar en dichos procesos, el documento de identidad nacional, que es la cédula de identidad y la verificación de la huella dactilar a través de unos dispositivos especiales denominados capta huella.

Los ejemplos anteriores son muy claros cuando la identidad se asocia a la persona, y son características propias que se pueden verificar. Pero existe otra noción de identidad asociada a un grupo social, que a pesar de las diferencias individuales que tiene cada uno de los integrantes, los agrupa y los identifica con dicho grupo. En una organización, comunidad, club y otras agrupaciones sociales, se les reconoce mediante un carnet de identificación que contiene las señas de la persona y adicionalmente elementos de seguridad que validan la procedencia del carnet.

La identidad de un colectivo no es una propiedad individual; involucra el entorno, la historia y la voluntad de un colectivo.

No es una característica innata sino que el colectivo y cada uno de sus integrantes debe desarrollarla, hasta que adquiera forma y se convierta en parte de la historia de su existencia.La identidad distingue un grupo de otros, así como la identidad individual distingue la individualidad de cada quien.

Así entonces hay una identidad como totalidad, como universo, que incluye varias partes o subsistemas: La identidad sexual o de género, la identidad física, la identidad psicológica, la identidad social, la identidad moral, la identidad ideológica, la identidad ciudadana y la identidad electrónica; cada una de estas tienen sus particularidades, pero extender la explicación de cada una de ellas, conllevaría a perder el objetivo de esta publicación, por lo que se profundizará en la última de las mencionadas, es decir, en La Identidad Electrónica

En algunos casos, se define la Identidad Electrónica como un conjunto de rasgos que caracterizan a un individuo o colectivo en un medio de transmisión electrónico. En efecto, cuando se habla de Identidad Electrónica no es más que la asociación entre un ente físico y un ente electrónico, es decir, es un conjunto de datos electrónicos asociados a cada persona: nombre, apellido, dirección de correo, contraseñas, etc., que hace diferente a un individuo de otro que usa el mismo tipo de identidad.

Ahora bien, la Identidad Electrónica no existe a priori. Se debe crear y vincular a la persona o colectividad identificada, en forma unívoca, siempre y cuando haya un proceso que determinará el nivel de confianza en el sistema de identificación electrónica. Un ejemplo de este proceso de creación de identidad electrónica es cuando se registran datos para abrir un correo electrónico, donde es necesario un nombre de usuario junto con una clave que identifique a la persona para acceder al mismo.

La mayoría de las personas que han navegado por Internet ya tienen algún tipo de "Identidad Electrónica" generada por sus transacciones en la red o por sus relaciones con tiendas virtuales, bancos en línea, compañías de seguros y otros sitios web. Generalmente, se trata de una "personalidad" electrónica que le permite ser reconocido e identificado tras la introducción de un nombre de usuario y una contraseña.

A un nivel muy sencillo, la Identidad Electrónica permite que una persona pueda mantener en línea una base de datos segura con toda su información personal, incluyendo, por ejemplo, herramientas personales tales como un calendario o un libro de direcciones. Por consiguiente, algunos ejemplos de "Identidad Electrónica" pueden ser su clave para acceder al correo electrónico; su nombre de usuario para acceder a un sistema en específico, el número de su tarjeta de débito que lo identifica ante un cajero o ante un portal en internet, la utilización del certificado electrónico para firmar un correo, entre otros.

IMPORTANCIA DE LA IDENTIDAD ELECTRÓNICA

La Identidad Electrónica está cobrando cada vez más importancia en el mundo, ya que hoy en día se puede encontrar lo inimaginable en la red y cada día más personas toman como primera opción, la búsqueda de información en Internet. La Identidad Electrónica está formando parte de la vida cotidiana. Se emplea para el celular, alarma de casa o carros, para acceder a la red, obtener dinero efectivo en cajeros automáticos, para acceder a cuentas de correo electrónico, para manejo de dinero, realizar compras, acceder a sistemas específicos, etc. Así, gracias a esta herramienta se pueden vender o comprar cosas en línea o realizar pagos de servicios sin tener que movilizarse.

Por el hecho de tener identidad física, no se tiene identidad electrónica. Ésta última se debe crear, y por tanto, ambas no necesariamente coinciden. En función de sus objetivos, cada individuo puede decidir si desea que sus identidades física y electrónica sean coincidentes o no, es decir, una persona de un sexo determinado puede crearse una identidad electrónica con el sexo opuesto, por ejemplo un hombre que se cree una identidad electrónica como una mujer, o vicerversa; también una persona que tenga edad de cuarenta y cinco (45) años y se cree una identidad electrónica como si fuese una persona de veintidos (22). Todo esto depende de la necesidad que presente esa persona al momento de crear su identidad.

Otro uso de la identidad electrónica, además de la identificación, es la protección de la información de una persona, del uso o abuso que puedan hacer terceros de ella. Por un mecanismo, explicado anteriormente como la criptografía, se puede utilizar la propia identidad electrónica de la persona para ayudar a cifrar la documentación y los datos y así protegerla de intrusos no autorizados a los documentos y archivos digitales de una persona. Así, ***la Identidad Electrónica es la principal medida para el control de acceso a servicios electrónicos o en línea.***

Por otro lado, existe una serie de desventajas al momento de utilizar un login o password como identidad electrónica, ya que es mucho más vulnerable para ser descubierto por otras personas. Es por ello que existe el Certificado Electrónico, que es un documento digital almacenado en un dispositivo (ver figura 2.1.), el cual al momento de utilizarlo asegura que la persona es quien dice ser; también se puede encontrar este Certificado Electrónico en software, ya que se puede instalar de una vez en la computadora.

Figura 2.1. Dispositivo donde se encuentra almacenado el Certificado Electrónico
Fuente: (SUSCERTE, 2009)

Visto de esta forma, la garantía de que se pueda usar la identidad electrónica con seguridad y privacidad, permite aprovechar las ventajas de muchas herramientas virtuales. Efectivamente, entre esas ventajas se encuentran que se puede dar a conocer objetivos y metas a través de la red como son los blogs, perfiles y otras aplicaciones donde se pueden colocar textos, imágenes y/o videos sobre actividades realizadas o sitios de interés. Otra ventaja que se obtiene al utilizar la identidad electrónica por la red es la inmediatez a la hora de compartir datos y la enorme difusión que éstos pueden alcanzar.

Los certificados electrónicos no son más que un documento electrónico que identifica a las personas y/u organizaciones y pueden reducir los peligros que una persona y/u organización se haga pasar por otra. Como cualquier documento, éste contiene información importante con respecto a su portador, por ejemplo; nombre, fecha de nacimiento y dirección.

De hecho, muchas de las organizaciones a nivel mundial ya usan estas tecnologías para realizar sus transacciones de comercio electrónico. Sin embargo, existen diversos problemas y limitaciones que restringen la aceptación de los certificados a nivel mundial.

A continuación se mostrará una tabla que señala las ventajas de la Identidad Electrónica a través del uso del Certificado Electrónico, las cuales serán explicadas más detalladamente en el Capítulo III "Certificación Electrónica." (Ver tabla 2.1).

VENTAJAS	
ESTADO VENEZOLANO	*Simplificación de trámites administrativos*
	Transparencia de procesos
	Eficiencia
	Habilitador para el Gobierno electrónico protagónico
	Disminución de corrupción
	Ahorro de costos
VENTAJAS	
CIUDADANOS	*Disminución de tiempos de respuestas*
	Mejorar la calidad de vida del ciudadano
	Acercar a las instituciones y servicios del estado a los ciudadanos donde quiera que estén.
	Desconcentración territorial
	Promueve el desarrollo endógeno
	Nueva geometría del poder

Tabla 2.1. Ventajas de la Identidad Electrónica
Fuente: (SUSCERTE, 2009)

Es por ello que basado en estas premisas, se sabe que el reto principal de la identidad electrónica radica en establecer un nivel de confianza entre las personas que se vayan a comunicar. De acuerdo a lo anterior, la identidad electrónica a su vez puede lograr varias metas como lo son:

1. La verificación de identidad puede impulsar el crecimiento de las organizaciones. Esto implica que una identificación más eficiente permitirá a las organizaciones crecer mucho más rápido. Este tipo de identidad es prioridad para muchas organizaciones ya que ofrece ventajas operativas, como agilizar la expedición de facturas, ventajas estratégicas, facilitar el acceso a nuevos mercados, etc.

2. El sistema ideal de identificación electrónica debe ser aceptado en todo el mundo y por todos los participantes en las transacciones. La aceptación universal facilitaría la interoperabilidad y reduciría el riesgo de fraudes. Las firmas y credenciales electrónicas deben tener validez legal en todo el mundo; deben garantizarse las transacciones entre fronteras en las que intervengan distintos participantes, y el usuario debe ser capaz de efectuar operaciones sin contratiempos.

3. Tener más proveedores y más clientes, así como recibir más pagos por medios digitales en los próximos tres años. Esto es muy importante para las organizaciones ya que con esto se incrementa la producción, se obtiene más clientela por medios electrónicos, aumenta el número de compradores, y se estima que en un futuro las cuentas por cobrar sean procesadas electrónicamente y se realicen los pagos por este medio.

CASOS DE ÉXITO DENTRO Y FUERA DE NUESTRAS FRONTERAS

Venezuela

El gobierno de la República Bolivariana de Venezuela, con el fin de mejorar la eficiencia de los servicios de identificación de ciudadanos venezolanos, migración y control de extranjeros, a través del Servicio Administrativo de Identificación, Migración y Extranjería (SAIME) concibe el Proyecto Identidad Electrónica, como un servicio integral orientado a la satisfacción de las necesidades de la sociedad, en materia de identificación, contribuyendo a garantizar la seguridad y soberanía tecnológica del Estado Venezolano.

Para atender la estrategia del Gobierno Bolivariano en materia de mejorar los servicios de identidad, es necesario garantizar a cada ciudadano un documento de identificación seguro, según los derechos consagrados en la Constitución de la República Bolivariana de Venezuela, que facilite el desarrollo de la Sociedad y del Gobierno Electrónico.

Venezuela es el primer país de América en emitir el Pasaporte Electrónico (ver figura 2.2.).Este documento se emite desde Marzo de 2007, es una lámina de policarbonato con grabados de láser y tiene un Chip con capacidad de almacenamiento de datos del usuario de 72kb. Los datos almacenados están firmados electrónicamente por SAIME, y poseen un certificado especial emitido por SUSCERTE. A continuación se puede ver la diferencia entre el pasaporte anterior y el electrónico (ver figura 2.3.)

Figura 2.2. Carátula del Pasaporte
Fuente: (SUSCERTE, 2009)

Pasaporte manual

Pasaporte Electrónico

Figura 2.3. Tipos de Pasaporte
Fuente: (SUSCERTE, 2009)

Por otro lado, hay un proyecto en ejecución como lo es la Cédula Electrónica que se constituirá en la base fundamental del gobierno electrónico, permitiendo una relación entre los ciudadanos y las administraciones públicas a través del uso de tecnologías avanzadas de la información y de las telecomunicaciones, pudiendo asociar a un solo documento una gama de servicios, que se traducen en una disminución en la cantidad de trámites, reducción de costos administrativos y garantía de seguridad en las transacciones de los servicios; a su vez, nos permitirá ejercer controles más efectivos para combatir el flagelo de la corrupción.

Se logrará el derecho fundamental y constitucional de la identificación del ciudadano, al eliminar problemas de fraude y usurpaciones de identidad.

La identificación efectiva de la ciudadanía traerá para el país beneficios en cuanto a la existencia de una base de datos única y confiable con la información actualizada de toda la población, la posibilidad de intercambio de información con los diferentes organismos del Estado, la garantía sobre la plena identidad de todos los ciudadanos, la autenticación del ciudadano mediante el uso de recursos tecnológicos existentes para la confrontación y validación del documento contra la identidad del portador y el mejoramiento del servicio de identificación y registro civil.

Argentina

Entre uno de sus proyectos más importantes en materia de Identidad Electrónica, se puede encontrar que se ha llevado a cabo la emisión del certificado raíz de la Infraestructura de Firma Digital de la República Argentina, en el marco de la Ley N° 25.506 y sus normas complementarias. Esta instalación tiene como objetivo emitir certificados digitales para aquellas entidades del Sector Público y Privado que soliciten y obtengan autorización para operar como certificadores licenciados, de acuerdo al artículo "Lanzamiento de la Autoridad Certificante Raíz de la República de Argentina". (Firma Digital Argentina, 2008)

En este país se denomina "Infraestructura de Firma Digital" al conjunto de leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes de telecomunicaciones. (Firma Digital Argentina, 2006)

Ecuador

En este país el Presidente Rafael Correa ha firmado el decreto 1356 de fecha 29 de septiembre de 2008, que da vía libre para que las rúbricas digitales se utilicen en el sector público y privado. Es por ello que las tradicionales cédulas de identidad ya no serán necesarias porque unos dispositivos, algo parecidos a un disco extraible o pendrive, funcionarán para firmar los documentos de manera electrónica.

La responsabilidad de este importante proyecto está en manos del Banco Central, que actualmente es la autoridad que concede esa certificación. Adicionalmente, la entidad necesita de la acreditación del Consejo Nacional de Telecomunicaciones (Conatel).

Unión Europea

Como se muestra en el artículo "Identidad Electrónica: facilitar el acceso a los servicios públicos en toda la UE", La Comisión Europea anunció un proyecto piloto cuyo objetivo es garantizar el reconocimiento de los sistemas nacionales de identidad electrónica (eID) y facilitar el acceso a los servicios públicos en trece (13) Estados miembros. Los ciudadanos utilizan actualmente en la Unión Europea unos treinta (30) millones de tarjetas nacionales de identidad electrónica para acceder a diversos servicios públicos, tales como las prestaciones por desempleo y de seguridad social, así como para presentar sus declaraciones de impuestos. El proyecto de la Comisión permitirá que los ciudadanos de la Unión Europea demuestren su identidad y utilicen los sistemas nacionales de identidad electrónica (contraseñas, tarjetas de identidad, códigos PIN y otros) no solamente en su país, sino también en la Unión Europea. El plan consiste en armonizar y conectar estos sistemas, sin sustituir lo que ya existe.

Sin sustituir a los regímenes nacionales, el nuevo sistema permitirá a los ciudadanos identificarse electrónicamente de forma segura y tratar con las administraciones públicas desde una oficina abierta al público, desde su computadora personal o, idealmente, desde cualquier dispositivo móvil. Esto significa, por ejemplo, que un estudiante podrá inscribirse en una universidad extranjera

sirviéndose de la identidad electrónica de su país. Existen ya algunos servicios entre los países miembros, como un portal de Internet belga que permite a las organizaciones extranjeras registrarse para dar empleo a ciudadanos procedentes de Suecia, por ejemplo.

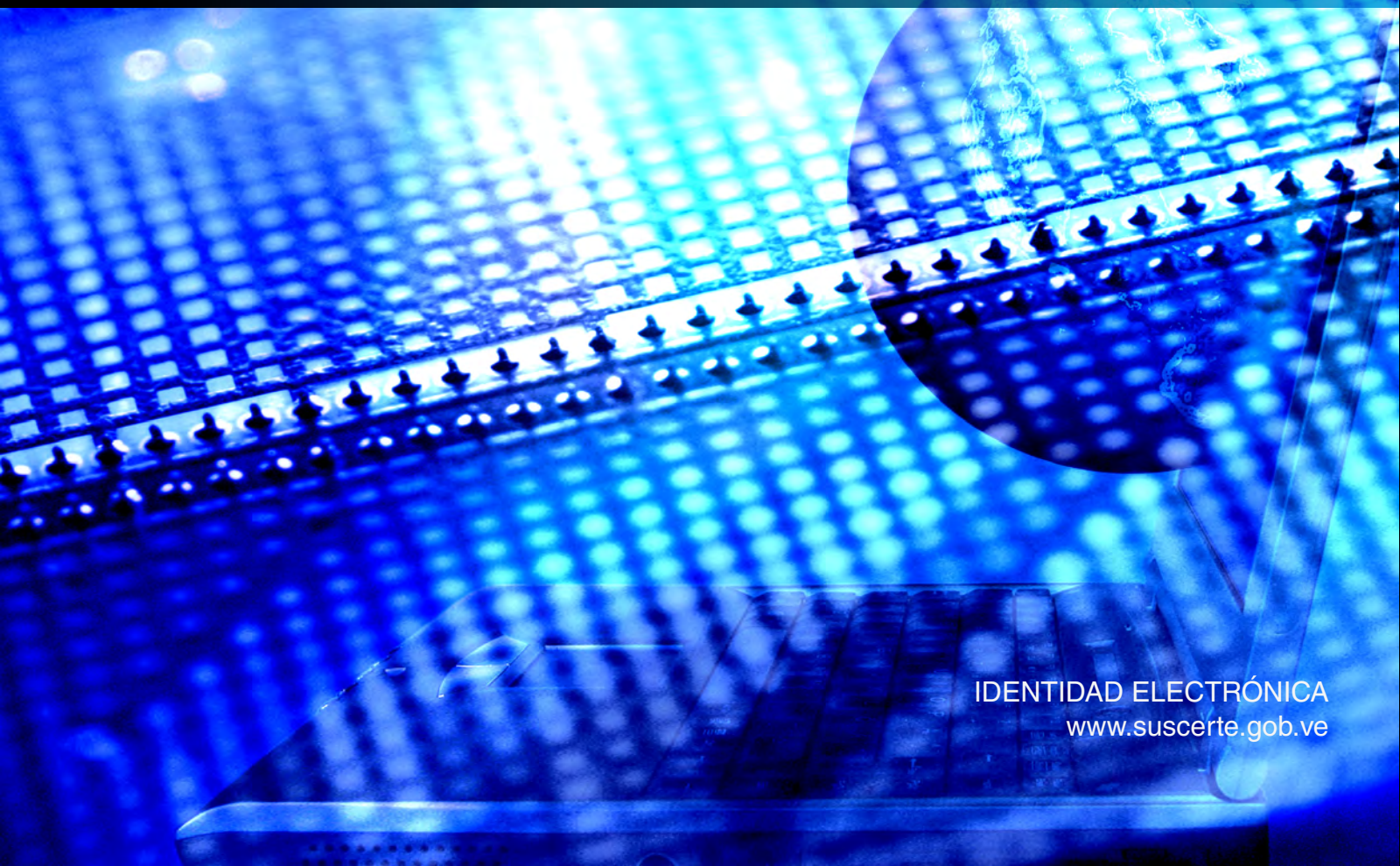
Un acceso fácil a los servicios públicos en toda la Unión Europea es algo esencial para los ciudadanos comunitarios que se desplazan por Europa por motivos profesionales, de estudio o de ocio, y contribuye a potenciar la movilidad de los trabajadores en Europa. (Press Releases, 2008).

REFLEXIÓN

Finalmente, y como reflexión, es importante que cada uno de los individuos que conforman una sociedad posean su identidad electrónica, ya que esto les permite interactuar con las Instituciones de su país y de esta manera colaborar en el proceso de generación del Gobierno Electrónico. El cambio cultural no es difícil, pero hay que dar el primer paso donde cada individuo utilice esta innovadora manera de identificarse, y así aproveche todas las ventajas que la tecnología puede llevarle a su vida cotidiana, como por ejemplo, firmar algún documento desde su casa sin necesidad de trasladarse.

Adicionalmente, la tecnología avanza a pasos agigantados y poco a poco esta herramienta va siendo más necesarias en todas y cada una de nuestras actividades, por ello, se irán incrementando las aplicaciones que necesiten y permitan el uso de los certificados electrónicos.

CAPÍTULO III
CERTIFICACIÓN ELECTRÓNICA



La Certificación Electrónica se define como el proceso mediante el cual se generan certificados electrónicos, garantizando la integridad de un documento digital o una acción cometida sobre éste.

Los certificados electrónicos pueden identificar a las personas y/u organizaciones, convirtiéndose de esta manera en documentos de identidad que contienen información importante con respecto a su portador, por ejemplo: nombre, fecha de nacimiento o constitución y dirección. Además, contienen el dato más importante para la identificación de la persona natural o jurídica: La clave pública de su signatario. La función de esta clave es establecer un parámetro técnico que permita darle seguridad a una información y el acceso a ella cuando sea necesario o deseado.

Al mismo tiempo, un certificado electrónico, emitido y firmado por un PSC permite autenticar a su signatario. Esto apunta a un rol significativo de la certificación electrónica en el modelado de la identidad del usuario, permitiéndole identificarse de forma segura y confiable en los portales del gobierno, la banca por internet, las empresas, entre otros.

Los certificados electrónicos son generados siguiendo los estándares internacionales, con la finalidad de unificar criterios y lograr a futuro su uso en otros países. El estándar utilizado es el X.509 V3, el cual define la estructura de los certificados, desarrollado por la Unión Internacional de Telecomunicaciones (UIT) y la Organización Internacional para la Estandarización (ISO).

Básicamente el estándar X.509 V3 tiene una serie de campos básicos, entre los cuales están:

- La identificación del signatario
- La clave pública del signatario
- El período de validez
- El nombre de la autoridad o entidad emisora.

A su vez, el estándar presenta una serie de extensiones, como la localización de la información de estado de certificado, la ubicación del certificado de la entidad emisora, los campos alternativos del nombre del signatario, las restricciones de uso y la información de las políticas.

BENEFICIOS DE LA CERTIFICACIÓN ELECTRÓNICA PARA EL ESTADO Y LA CIUDADANÍA VENEZOLANA

En lo particular, el Decreto Ley sobre Mensaje de Datos y Firmas Electrónicas (LSMDFE) brinda un aval para que la certificación electrónica ofrezca un conjunto de beneficios tanto para el Estado Venezolano como para la Ciudadanía.

Para el Estado Venezolano:

- *La simplificación de trámites administrativos:* Con el uso de los certificados electrónicos, el usuario podrá autenticarse (es decir, identificándose según quien dice ser) en los portales del gobierno y la empresa privada. De ésta manera podrá realizar las transacciones en línea de forma segura y eficiente, eliminando el flagelo de procesos largos y engorrosos de los trámites administrativos.

• *Habilitador para el Gobierno electrónico protagónico:* La masificación de los certificados electrónicos en los ciudadanos venezolanos, impulsará el desarrollo y la independencia tecnológica del país, promoviendo a su vez la política de Estado de fortalecer el Gobierno electrónico en los procesos y actividades de la Administración Pública Nacional.

• *Descentralización:* El estado venezolano se perfila como estado pionero en la descentralización de trámites administrativos mediante el impulso regional de la implementación de certificados electrónicos para realizar transacciones electrónicas en los portales del gobierno sin necesidad de trasladarse los ciudadanos del interior hacia la capital.

• *Ahorro:* El uso de la plataforma tecnológica acarrea un ahorro evidente en uso de papel y otros insumos para el Estado Venezolano respondiendo a políticas de protección ambiental y a las iniciativas de Gobierno sin papel.

Para la Ciudadanía:

• *Autenticación:* Su uso genera esquemas de confianza entre la identidad del usuario que accede al sistema y el portal del gobierno o empresas.

• *Disminución de tiempos de respuestas:* El usuario podrá gestionar un mayor número de trámites a través de internet.

• *Acceso Gobierno - Ciudadano:* Permitirá al ciudadano común mantener esa condición de portabilidad y movilidad permanente de sus operaciones en línea con los portales del estado en cualquier parte del país.

• *Disponibilidad:* Organizar información para tenerla "a la mano". Conocer el estado de un trámite.

• *Fortalecimiento del Desarrollo Endógeno:* Busca la implementación de estrategias autóctonas para la consolidación de las instituciones públicas y el fomento de la participación ciudadana orientada en las necesidades del colectivo en materia de certificación electrónica, seguridad de la información, automatización de trámites, entre otras.

A fin de establecer las bases confiables para una eficaz identificación por medios electrónicos, el Estado ha regulado la actividad mediante una Ley especial y su reglamento; de igual modo ha promovido el uso de los certificados electrónicos en otros instrumentos normativos, para que la Administración Pública pueda brindar sus servicios electrónicamente.

MARCO LEGAL

Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas

El Decreto-Ley N° 1.204 de fecha 10/02/2001 publicado en la Gaceta Oficial N° 37.148 del 28/02/2001, tiene por objeto, otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico (video, música, fotografía, entre otros), independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular lo relativo a los PSC y los Certificados Electrónicos.

Una de las características más resaltantes de esta normativa, es que atribuye valor legal y probatorio a los mensajes de datos (documentos electrónicos) y el uso en los mismos de la firma electrónica.

Los documentos electrónicos tienen la misma garantía legal que los documentos en papel, tal como lo establece la Ley Sobre Mensajes de Datos y Firma Electrónica en su Artículo 4°:

"Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este decreto ley. Su promoción, control,

contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil. La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas". (p. 317.496)

De acuerdo a lo anterior, es conveniente establecer las siguientes distinciones:

1. Si el certificado electrónico es emitido por un PSC, constituirá plena prueba, pues la ley le otorga la misma validez que a la firma autógrafa, ya que éste debe cumplir con los requisitos del Art.16.

2. Si el certificado electrónico no es emitido por un PSC y no cumple los requisitos del citado artículo, en caso de un litigio, el juez valorará los documentos firmados electrónicamente conforme a las regla de la sana crítica (lógica y máximas de experiencia)

En este orden de ideas, es conveniente acotar que la responsabilidad del signatario del certificado se asumirá por medio de una declaración, negocio u otro acto y no desaparecerá porque el medio en cuestión sea electrónico, salvo que alguna condición legal exija lo contrario.

Por último, este decreto ley pretende convertirse en la piedra angular del comercio y gobierno electrónico, generando confianza y estimulando su uso en el Estado Venezolano.

Reglamento Parcial del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas

Publicado en la Gaceta Oficial N° 38.086 del 14 de Diciembre de 2004, bajo el Decreto Nº 3.335 de Diciembre de 2004 y tiene por objeto desarrollar la normativa que regula la acreditación de los PSC ante SUSCERTE, la creación del Registro de Auditores, estándares, planes y procedimientos de seguridad de conformidad con el Decreto Ley.

Características

Como su nombre lo indica, este Reglamento Parcial dedica su contenido a regular fundamentalmente el procedimiento de acreditación de los PSC, definiendo a continuación una serie de requisitos técnicos, legales y financieros:

- Las obligaciones de los PSC acreditados.

- Las formalidades que deberá cumplir el PSC en caso de suspensión del servicio ya sea por motivo de mantenimiento y mejoras en sus sistemas, o bien por caso fortuito o fuerza mayor.

- Reconoce a su vez la validez de los certificados electrónicos extranjeros, siempre y cuando sea garantizados por un PSC debidamente acreditado por SUSCERTE.

- Establece las inspecciones ordinarias y extraordinarias como mecanismo de control y supervisión de los PSC acreditados por SUSCERTE.

- Ordena la creación del Registro de Auditores y dispone el procedimiento de inscripción.

- Finalmente establece los estándares, planes, procedimientos de seguridad y requisitos técnicos que deberán llevar a cabo los PSC.

INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA

La Infraestructura Nacional de Certificación Electrónica es el conjunto de servidores, programas (software), dispositivos criptográficos, políticas, normas y procedimientos, dispuestos y utilizados de manera exclusiva por la Autoridad de Certificación Raíz y los PSC acreditados para la generación, almacenamiento y publicación de los certificados electrónicos, así como también, para la publicación de información y consulta del estado de vigencia y validez de dichos certificados. Esta Infraestructura se basa en dos pilares fundamentales, tales como la confianza y la tecnología.

La confianza está enmarcada en el desarrollo e implementación de políticas de seguridad para satisfacer los niveles requeridos de confidencialidad en la administración y emisión de certificados electrónicos. La tecnología está definida como una herramienta para el mantenimiento y actualización de plataformas de hardware y software que dan soporte a la Infraestructura Nacional de Certificación Electrónica.

La Infraestructura Nacional de Certificación Electrónica, fue concebida según Providencia emitida el 2 de marzo de 2007, en la cual se establecen las Normas Técnicas bajo las cuales SUSCERTE coordinará e implementará el modelo jerárquico de dicha infraestructura, para que los PSC emitan los certificados electrónicos en el Marco del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas y su Reglamento.

A continuación se menciona como están constituidos los elementos de la Infraestructura Nacional de Certificación Electrónica:

1. La Autoridad de Certificación Raíz del Estado Venezolano, operada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), ente rector que dicta las normas y estándares de uso, acreditación, supervisión y control de los PSC.

2. El PSC es la entidad encargada de emitir los Certificados Electrónicos a los usuarios.

3. El Certificado Electrónico, documento electrónico emitido por un PSC que vincula a un signatario con su clave pública.

4. La Firma Electrónica, es un conjunto de datos que vincula de manera única el documento al signatario y garantiza la integridad del documento electrónico. Es importante resaltar dos aspectos vinculantes: La integridad, que su contenido no ha variado desde el momento en que se firmó y la autoría, quien firmó el documento.

5. El documento electrónico, representación de actos o hechos en formato electrónico.

Para graficar la explicación anterior, se muestra a continuación los elementos de la Infraestructura Nacional de Certificación Electrónica (ver figura 3.1):

Figura 3.1. Elementos que Conforman la Infraestructura Nacional de Certificación Electrónica. Fuente (SUSCERTE, 2009)

En esta perspectiva, SUSCERTE promueve y divulga el uso de los certificados y firma electrónica en Venezuela, es por ello que en febrero de 2007 crea la Autoridad de Certificación (AC) Raíz del Estado Venezolano, la cual es la encargada de acreditar a los PSC que se encuentren aptos para operar en el país, fortaleciendo con esto al Sistema Nacional de Certificación Electrónica (SNCE).

A su vez, debe señalarse que la AC Raíz se encarga de emitir, renovar, revocar y suspender los certificados electrónicos a:

- La propia Autoridad de Certificación Raíz del Estado Venezolano.

- Las Autoridades de Certificación de los PSC acreditados, una vez que éstos cumplan los requisitos establecidos en el Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas y su Reglamento Parcial y obtengan su Acreditación.

- Las Autoridades de Certificación para casos especiales en proyectos de interés nacional.

Estos procedimientos están definidos en la Ley sobre Mensajes de Datos y Firmas Electrónicas y en la Declaración de Prácticas de Certificación y Política de Certificados de la AC Raíz de Venezuela.

Para emitir o renovar un certificado, se debe verificar y aprobar las exigencias establecidas en la LSMDFE, su Reglamento Parcial y en la normativa sublegal vigente emitida por SUSCERTE, y de esta manera, la AC Raíz procederá a realizar la emisión del certificado al PSC, acto que será publicado mediante Gaceta Oficial de la República Bolivariana de Venezuela.

Por otro lado, la revocación o suspensión de un certificado es producto de diversas circunstancias:

- Compromiso de la clave privada de la AC Raíz.

- Compromiso o sospecha de la clave privada asociada al certificado del PSC.

- Cuando el PSC solicite a la AC Raíz, la suspensión temporal de su certificado.

- Por resolución judicial o administrativa que lo ordene.

- Por la variación de los datos del certificado.

Estas circunstancias generan un rompimiento en la cadena de confianza, en estos casos, las entidades autorizadas para solicitar la revocación de acreditación de un PSC de la Infraestructura Nacional de Certificación Electrónica de Venezuela son:

- La autoridad competente a la conformidad con la LSMDFE.

- El PSC

- La AC Raíz

La AC Raíz del Estado Venezolano emite, renueva, revoca, suspende y firma su propio certificado electrónico, de acuerdo a lo establecido en la Declaración de Prácticas de Certificación y Políticas de Certificados, siendo este el primer nivel de la Infraestructura Nacional de Certificación Electrónica. Este certificado se denomina certificado electrónico raíz o certificado electrónico auto-firmado.

Las Autoridades de Certificación principales de los PSC Acreditados están subordinadas a la AC Raíz del Estado Venezolano, siendo por lo tanto, el segundo nivel de la Infraestructura Nacional de Certificación Electrónica. Estas autoridades podrán emitir, renovar, revocar y suspender los certificados electrónicos a los signatarios y a sus AC subordinadas.

El PSC podrá adicionalmente emitir Certificados Electrónicos a Autoridades de Certificación subordinadas a su AC principal, las cuales constituyen el tercer nivel en la jerarquía de la Infraestructura Nacional de Certificación Electrónica.

Los PSC acreditados constituirán Autoridades de Registro (AR) para controlar la generación de los Certificados Electrónicos de sus AC. Las AR

se encargarán de realizar las peticiones a las AC correspondientes, para la emisión, renovación, revocación y suspensión de los certificados electrónicos, una vez comprobada la veracidad y exactitud de los datos suministrados por los signatarios. Las AR deben almacenar los datos que demuestren el cumplimiento por parte del signatario de los requisitos necesarios para la solicitud.

Para explicar mejor la idea anterior, se muestra a continuación la Estructura Jerárquica que compone a la Infraestructura Nacional de Certificación Electrónica (ver figura 3.2).

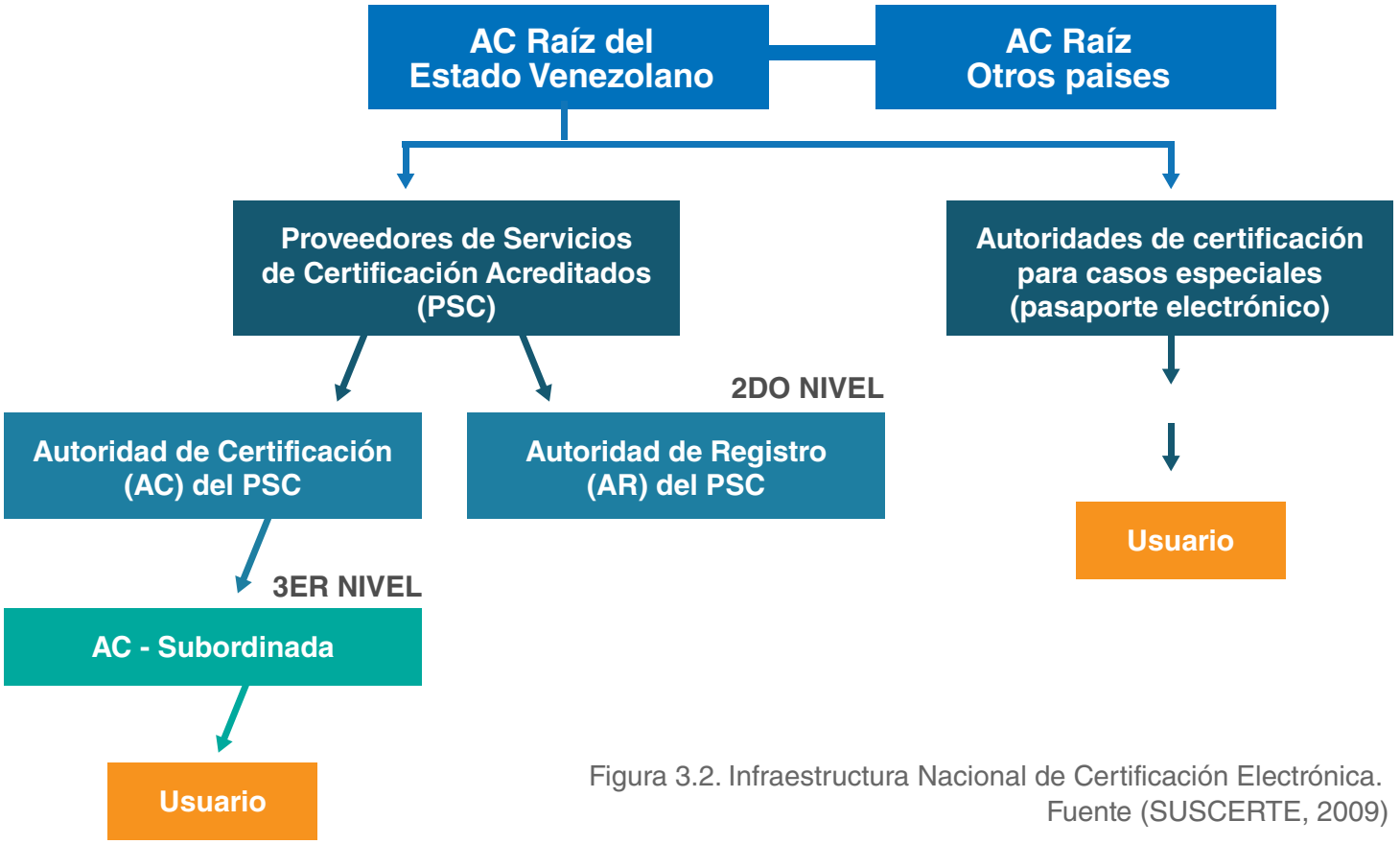


Figura 3.2. Infraestructura Nacional de Certificación Electrónica.
Fuente (SUSCERTE, 2009)

Actualmente en Venezuela existen dos PSC, los cuales fueron acreditados por SUSCERTE el 18 de julio de 2008, uno de carácter público, la Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico (FII), y otro de carácter privado, Proveedor de Certificados PROCERT C.A. De igual manera existen organismos que han dado los primeros pasos a fin de acreditarse en un futuro cercano.

Proceso de acreditación

SUSCERTE contempla el proceso de acreditación bajo su norma N° 27-04/08, disponible en su sitio web www.suscerte.gob.ve. Dicha norma tiene como objeto y campo de aplicación la descripción de todos los recaudos que deben presentarse por parte de los solicitantes a PSC, así como el recorrido del proceso de acreditación con respecto a dicha solicitud.

Es importante mencionar que los recaudos exigidos por SUSCERTE para la acreditación de los PSC son de tipo técnico, económico-financiero, legal y de auditoría, los cuales deben cumplirse a cabalidad para lograr la aprobación de su solicitud de acreditación.

SUSCERTE ofrece además a los interesados en convertirse en PSC acreditados, la Norma SUSCERTE N° 40 "Guía de estándares tecnológicos y lineamientos de seguridad para la Acreditación como Proveedor de Servicios de Certificación" , la cual contiene la descripción y aspectos a evaluar de todos los recaudos técnicos exigidos para la acreditación e incluso presenta una serie de anexos donde se especifica la documentación solicitada y se ejemplifica la estructura de muchos de los recaudos solicitados.

Uno de los recaudos técnicos que debe documentar el solicitante se presenta en la Norma SUSCERTE N° 22 Modelo para la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificados (PC) de los PSC, donde se detalla el contenido que se debe colocar en el recaudo conformado por su DPC y PC, además de presentarse los usos de los certificados electrónicos, entre otros aspectos de interés para quienes adquieran su certificado.

Cabe destacar que en la Norma SUSCERTE N° 32 Infraestructura Nacional de Certificación Electrónica: estructura, certificados y listas de certificados revocados, se especifican los tipos de certificados que pueden emitir los PSC tales como los que van destinados a las personas naturales, personas jurídicas, entre otros.

Respecto a los recaudos de auditoría, el solicitante debe aprobar una auditoría que efectuará un auditor de su preferencia, siempre que se encuentre registrado ante SUSCERTE, quien utilizará las normativas establecidas por la Superintendencia para la realización de la auditoría.

Certificación Cruzada

Se define la certificación cruzada como un acto por el cual una certificadora acreditada reconoce la validez de un certificado emitido por otra, sea nacional, extranjera o internacional, asumiéndolo como si fuera de propia emisión, bajo su responsabilidad. Este esquema está establecido mediante previos acuerdos de reconocimiento mutuo entre Autoridades de Certificación extranjeras.

La certificación cruzada se requiere por la necesidad de interoperabilidad en la Infraestructura de Claves Públicas (ICP), útil para ayudar al soporte de transacciones entre usuarios que no tienen una misma tecnología, ofreciendo mayor flexibilidad y libertad de elección entre los proveedores de servicio conjuntamente con los usuarios; permitiendo a su vez, establecer una diversificación y masificación del uso de firmas electrónicas y la emisión de certificados para usuarios y servidores, entre entes certificadores que dependen de AC raíz distintas.

De conformidad a la LSMDFE: "Los Certificados Electrónicos emitidos por proveedores de servicios de certificación extranjeros tendrán la misma validez y eficacia jurídica reconocida en el presente Decreto-Ley, siempre que tales certificados sean garantizados por un Proveedor de Servicios de Certificación, debidamente acreditado conforme a lo previsto en el Decreto-Ley, que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, seguridad, validez y vigencia del certificado".

"Los certificados electrónicos extranjeros, no garantizados por un Proveedor de Servicios de Certificación debidamente acreditado conforme a lo previsto en el presente Decreto-Ley, carecerán de los efectos jurídicos que se atribuyen en el presente Capítulo, sin embargo, podrán constituir un elemento de convicción valorable conforme a las reglas de la sana crítica".

Estampado de Tiempo

El Estampado o Sellado de Tiempo es el mecanismo para proporcionar certidumbre probatoria del momento en que un documento electrónico es generado, enviado o recibido. Es decir el "sellado" es un archivo informático que vincula la información a una fecha y a una hora específica, esta vinculación se produce a través

de un sistema seguro de tiempo sincronizado con la Escala de Tiempo Universal. Su aplicabilidad es de suma importancia puesto que garantiza que unos datos han existido antes de un momento determinado (fecha y hora) y no han sido alterado, pudiéndose extender ampliamente en documentos electrónicos (correos electrónicos, imágenes, video, entre otros); en Firmas Electrónicas y en la Validez de los Certificados Electrónicos.

En Venezuela, la Dirección de Hidrografía y Navegación de la Armada de la República Bolivariana de Venezuela (DHN) con sede en el Observatorio Naval Cagigal, es el Organismo encargado de emitir la hora legal en Venezuela. Actualmente el país no cuenta con un Proveedor que preste el servicio de Sellado de Tiempo, razón por la cual actualmente SUSCERTE contempla entre sus proyectos el desarrollo de este servicio.

LA FIRMA ELECTRÓNICA, FOMENTANDO LA CONFIDENCIALIDAD, AUTENTICIDAD E INTEGRIDAD DE LOS DATOS.

La firma electrónica es la forma análoga de una firma escrita, la cual identifica al firmante y lo relaciona con los datos firmados. Toda persona está acostumbrada a usar su firma autógrafa, especialmente para sus actos civiles y mercantiles, pues firma cheques, contratos, entre otros. Por lo tanto cada día se acerca el momento en que la firma electrónica se emplee con mayor auge.

La seguridad de la firma electrónica se basa en el uso de la criptografía , es decir, se vale de mecanismos de cifrado de la información para que no sea accedida por terceras personas no autorizadas, estas características de cifrado otorgan las siguientes propiedades a la firma electrónica:

- Autenticidad, vincula de forma única el documento a su autor
- Integridad, verifica la no alteración de los datos del documento original, desde que fue firmado.
- No repudio, garantiza que el emisor no pueda negar o repudiar su autoría o existencia, ser susceptible de verificación ante terceros.

Existen concepciones erradas sobre lo que es la firma electrónica, y en muchos casos se le confunde con una firma manuscrita escaneada, una contraseña, un sistema biométrico, o un documento cifrado, no debemos olvidar que la firma electrónica es información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

La aplicación de la firma electrónica es diversa, y se puede utilizar en la firma de datos enviados mediante un formulario web, imágenes, una base de datos, una transacción electrónica segura, un correo, una hoja de cálculo o documento de texto, el código fuente de un programa, uno o varios archivos en general.

La firma electrónica es un conjunto de datos que vincula de manera única el documento al usuario y garantiza la integridad del documento electrónico, se genera como resultado de la aplicación de una función matemática llamada "función de Hash", lo cual podemos decir que es una especie de impresión digital de un mensaje.

A través del siguiente ejemplo, se explicará como se genera una Firma Electrónica: Rosa necesita enviar un mensaje a Juan:

El mensaje dice lo siguiente: "Estimado Juan: Te envío la minuta de la reunión sostenida ayer en SUSCERTE. Atentamente, Rosa". Al mensaje de Rosa se le aplica una "función de Hash", la cual genera un valor único, de manera que si alguien intenta alterar su mensaje, éste genera automáticamente un nuevo código Hash, pudiéndose comprobar luego que ha sido modificado. La firma electrónica es por lo tanto, una forma segura de conseguir una autenticación.

En el paso siguiente, Rosa cifra el valor Hash con su clave privada, la consecuencia de esto es la generación de un archivo electrónico que representa su firma electrónica. Luego, la firma electrónica generada por Rosa se anexa al material (documento) que será enviado electrónicamente a Juan.

Juan, luego de recibir el mensaje, se le aplica la función de Hash para obtener la impresión digital del mensaje. Al mismo tiempo, él descifra el mensaje con la utilización de la clave pública de Rosa, con ello se obtiene, nuevamente, otra impresión digital del mensaje. A continuación podemos observar una ilustración de lo explicado (ver figuras 3.3 y 3.4):

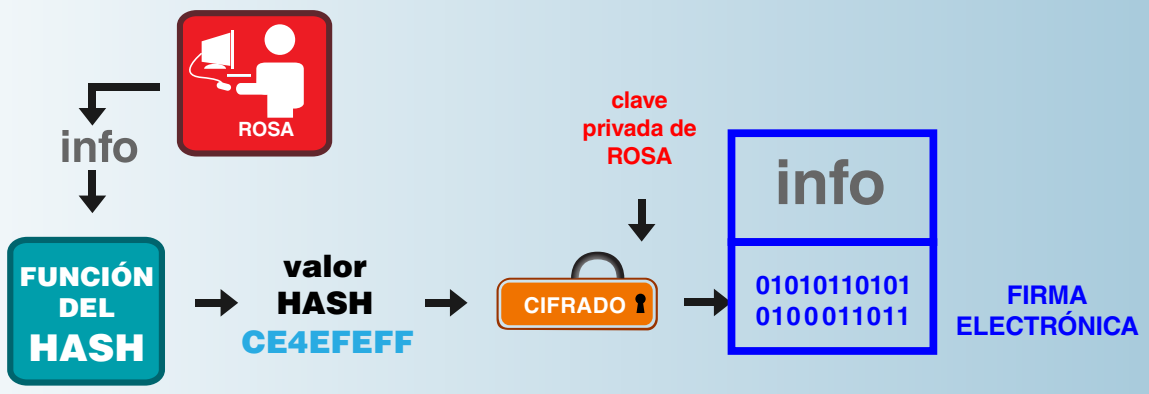


Figura 3.3. Proceso de Generación de la Firma Electrónica. Fuente (SUSCERTE, 2009)

Figura 3.4. Proceso de Validación de la Firma Electrónica. Fuente (SUSCERTE, 2009)

Fortalezas y usos del certificado electrónico

A continuación se resaltarán tres aspectos fundamentales que fortalecen el uso del certificado electrónico:

1. Las claves privadas que se usan en los procesos de cifrado y firma requieren una garantía de exclusividad de uso y por ello se debe generar y custodiar en un dispositivo seguro.

2. Los procesos de firma electrónica requieren un gran volumen de operaciones y por tanto necesitan de una alta velocidad de proceso.

3. El algoritmo empleado en el proceso de generación, cifrado y firma, debe estar certificado por un laboratorio acreditado por la Autoridad de Certificación correspondiente.

Tipos de certificados electrónicos

• Certificados de Personas Naturales: Autoriza la firma y/o cifrado de los mensajes de correo electrónico y documentos con el certificado electrónico de su signatario.

• Certificados de Personas Jurídicas: Con este tipo de certificado se autoriza la firma y/o cifrado de los mensajes de correo electrónico y documentos con el certificado electrónico, en nombre de la persona jurídica o entidad del Estado venezolano que figura en el certificado electrónico como signatario.

• Certificados para Servidores: Permite incorporar el protocolo Secure Sockets Layer (SSL) en un servidor Web. Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando toda la información que se envían ambas partes. Los certificados de servidor no pueden ser utilizados como certificados electrónicos que respalden firmas electrónicas del suscriptor.

• Certificados para operadores del PSC: Otorga a las personas responsables de las tareas e la Autoridad de Registro (AR) y la Autoridad de Certificación (AC).

Dispositivos de almacenamiento de certificados electrónicos.

Existen diversos dispositivos para la generación y custodia de las claves, aunque no todos ofrecen iguales prestaciones y garantías. Entre ellos se pueden mencionar: la Tarjeta Inteligente, las tarjetas criptográficas o tokens y los HSMs (Hardware Criptográfico).

A continuación se describen cada uno de los dispositivos:

• Tarjeta Inteligente: Consiste en una tarjeta criptográfica que genera y almacena las claves criptográficas que componen el certificado electrónico (ver figura 3.5).

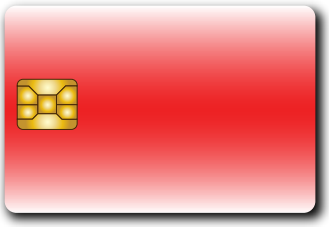


Figura 3.5. Tarjeta Inteligente Fuente (SUSCERTE, 2009)

• Token USB: El token es un hardware criptográfico que genera y almacena las claves criptográficas que componen el certificado electrónico, del mismo modo que la tarjeta inteligente. El token se puede conectar a una computadora por el puerto USB y funciona simultáneamente como una tarjeta inteligente y un lector (ver figura 3.6).

Figura 3.6. Token USB Fuente (SUSCERTE, 2009)

• HSM (Hardware Security Module): Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar mayor rapidez en las operaciones criptográficas (ver figura 3.7).

Figura 3.7. Módulo HSM Fuente (SUSCERTE, 2009)

El uso de HSM es una solución que ofrece un mayor nivel de prestaciones, calidad de servicio y garantías de seguridad, de hecho, es capaz de almacenar miles de claves internamente con mecanismos de respuestas ante la manipulación, es decir, detectando cualquier intento malicioso de acceso a sus memorias y reaccionando ante cualquier ataque, borrando las mismas.

Todas las funciones de éste tipo de dispositivos han sido sometidas a revisión por parte de un laboratorio acreditado y por tanto están certificadas, lo que representa sin duda, una garantía en cuanto a seguridad.

Basados en éste tipo de tecnología, han aparecido en el mercado Servidores Criptográficos de Firma de uso específico o recurso dedicado, los cuales engloban en una única plataforma lo siguiente:

- Aplicación de Firma Electrónica con capacidad para firmar documentos en múltiples formatos y estándares (Xades, PDF, PKCS#7, etc).

- Hardware Criptográfico (HSM).

- Servidor hardware y sistema operativo en red.

Estos dispositivos se presentan como plataformas muy eficientes para realizar procesos de Firma electrónica, ya que permiten una fácil integración con las aplicaciones corporativas o departamentales con funciones de firma, consiguiendo un elevado rendimiento en procesos automatizados de Firma Electrónica.

Tiempo de vida de los certificados

El tiempo de vida de almacenamiento que se recomiendan para los certificados se muestra a continuación (ver tabla 1.2):

Tipo de Certificado	Dispositivo para Generación y Almacenamiento del par de claves	Duración máxima (años)
Persona Natural	Software (guardado en discos)	1
	Hardware (token criptográfico)	3
Persona Jurídica	Software (guardado en discos)	1
	Hardware (token criptográfico)	3
Servidor y/o Aplicaciones	Software (guardado en discos)	3
	Hardware (HSM)	5

Tabla 1.2. Tiempo de Vida de los Certificados.
Fuente (SUSCERTE, 2009)

GLOSARIO DE TÉRMINOS

Algoritmo	Conjunto de instrucciones que le dice a la computadora los pasos específicos para llevar a cabo una tarea.
Autoridad de Certificación	Entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública.Jurídicamente es un caso particular de Prestador de Servicios de Certificación.
Base de Datos	Conjunto de datos pertenecientes a un mismo contexto o a una misma persona y almacenados sistemáticamente para su posterior uso.
Blogs	Sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores.
Cadena de ADN	Ácido nucleico que contiene la información genética usada en el desarrollo y funcionamiento de organismos vivos.
Certificado Electrónico	Mensaje de datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica.
Chip	Circuito integrado de un soporte de silicios, formado por transistores y otros elementos electrónicos miniaturizados.
Cifrar	Transcribir en letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar.
Clave	Código de signos convenidos para la transmisión de mensajes secretos o privados.
Confidencialidad	Propiedad de que la información no esta disponible o divulgada a individuos, entidades o procesos no autorizados. Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas.
Código Fuente	Texto escrito en un lenguaje de programación específico y que puede ser leido por un programador.
Comercio Electrónico	Compra y venta de productos o de servicios a través de medios electrónicos, tales como el Internet. también conocido como e-commerce.

GLOSARIO DE TÉRMINOS (continuación)

Descifrar	Declarar lo que está escrito en cifra o en caracteres desconocidos, sirviéndose de clave dispuesta para ello, o sin clave, por conjeturas y reglas críticas.
Destinatario	Persona a quien va dirigido el Mensaje de Datos.
Diagrama	Dibujo en el que se muestran las relaciones entre las diferentes partes de un conjunto o sistema.
Disponibilidad	Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada. Dicho de una cosa: Que se puede disponer libremente de ella o que está lista para usarse o utilizarse.
Documento	Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.
Emisor	Persona que origina un mensaje de datos por si mismo, o a través de terceros autorizados.
Estándar X.509 V3	Recomendación del Grupo de Telecomunicaciones de la Unión Internacional de Telecomunicaciones, que define un marco para la prestación, por el directorio de servicios, de autenticación a sus usuarios. La versión 3 fue aprobada el 09 de Agosto de 1997.
Firewall	Elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.
Firma Electrónica	Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.
Formulario Web	Tipo de formulario que es presentado en un navegador y puede ser rellenado a través de una red como Internet.
Huella Dactilar	Impresión visible o moldeada que produce el contacto de las crestas papilares.
Internet	Red informática. Un conjunto de ordenadores desplegados por todo el mundo y conectados entre sí intercambiándose información.

GLOSARIO DE TÉRMINOS (continuación)

Interoperabilidad	Condición necesaria para que los usuarios (humanos o mecánicos) tengan un acceso completo a la información disponible.
Kilobyte (KB)	Unidad de almacenamiento de información cuyo símbolo es el kB (a veces se utiliza KB).
Litigio	Pleito, altercación en juicio, disputa, contienda.
Login o Password	Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada. Dicho de una cosa: Que se puede disponer libremente de ella o que está lista para usarse o utilizarse.
Mensaje	Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.
Plataformas Tecnológicas	Agrupación de elementos de tecnología de la información que comprende todo el equipo de cómputo (hardware), programas (software), bases de datos, servicios prestados, personal y políticas que sustentan las acciones en materia de certificación electrónica.
Proveedor de Servicios de Certificación	Persona dedicada a proporcionar Certificados Electrónicos y demás actividad es previstas en este Decreto-Ley.
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información, adicionalmente pueden involucrarse otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad.
Signatario	Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.
Sistemas redundantes	Cierta repetición de la información contenida en un mensaje, que permite, a pesar de la pérdida de una parte de este, reconstruir su contenido.
Software	Equipamiento lógico o soporte lógico de un computador digital.
Transacción Electrónica Segura	Protocolo estándar para operaciones seguras con tarjetas de crédito sobre redes inseguras, especialmente Internet.

REFERENCIAS BIBLIOGRÁFICAS

Diccionario de la Lengua Española (2001). Real Academia Española. (Edición 22°). Recuperado el 8 de Junio de 2009, en http://www.rae.es/rae.html

Diccionario Informático Alegsa. Recuperado el 02 de Septiembre del 2009, en http://www.alegsa.com.ar

Firma Digital Argentina (2008, Agosto 15). Lanzamiento de la Autoridad Certificante Raíz de la República de Argentina. Recuperado el 8 de Junio de 2009, en http://www.pki.gob.ar/index.php?option=com_frontpage&Itemid=1

Firma Digital Argentina (2006, Agosto 23). Firma Digital. Recuperado el 8 de Junio de 2009, en http://www.pki.gob.ar/index.php?option=content&task=view&id=91&Itemid=102

Fondonorma -ISO/IEC 27001:2006. Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. República Bolivariana de Venezuela.

Leandro F. Meiners & Montero, Victor. Seguridad Informática e Interoperabilidad en PKI. Departamento de Computación. Facultad de Ciencias Exactas y Naturales. Universidad de Buenos Aires. Argentina.

Millán, G. L, Martínez, P. G., & Skarmeta, A. F. (2004). Infraestructuras de Certificación Cruzada. Departamento de Ingeniería de la Información y las Comunicaciones. Universidad de Murcia. España.

Nash, A., & Duane, W. (2002). PKI Infraestructura de Claves Públicas. Colombia: Mc. Graw Hill. Press Releases (2008, Mayo 30). Identidad Electrónica: facilitar el acceso a los servicios públicos en toda la UE. Recuperado el 8 de Junio de 2009, en http://www.actica.org/actica/esociedad/idue0805.pdf

República Bolivariana de Venezuela (2001). Decreto Ley de Mensajes de Datos y Firmas Electrónicas publicada en la Gaceta Oficial de la República Bolivariana de Venezuela No 37.148 de fecha 28 de febrero del 2001.

República Bolivariana de Venezuela (2006). Ley Orgánica de Identificación de Venezuela, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.458 de fecha 14 de junio de 2.006.

Rodríguez, J. (2008, 02 de Junio). Seguridad y eficacia en el proceso de firma electrónica de documentos. Recuperado el 21 de Mayo del 2009, en http://www.vnunet.es/es/vnunet/opinion/2008/06/02/seguridad_y_eficacia_en_proceso_de_firma_electronica_de_documento

Superintendencia de Servicios de Certificación Electrónica "SUSCERTE". (2008, 06 de Julio). Declaración de Prácticas de Certificación y Políticas de Certificados de la Autoridad de Certificación Raíz de Venezuela. Recuperado el 11 de Mayo del 2009, en http://www.suscerte.gob.ve/images/Norma-054.pdf

Superintendencia de Servicios de Certificación Electrónica "SUSCERTE". (2008, 01 de Julio). Infraestructura Nacional de Certificación Electrónica: Estructura, Certificados y Lista de Certificados Revocados. Recuperado el 11 de Mayo del 2009, en http://www.suscerte.gob.ve/images/Norma-032.pdf

Superintendencia de Servicios de Certificación Electrónica "SUSCERTE" (2008, Julio). Esquema de autenticación, integridad y confidencialidad aplicables a la automatización de trámites. Presentación realizada en la Universidad Fermin Toro, Cabudare, Edo Lara.

www.suscerte.gob.ve

Gobierno **Bolivariano** de Venezuela | Ministerio para el Poder Popular para **Ciencia, Tecnología e Industrias Intermedias**

Venezuela
AHORA ES DE TODOS