Universidad Nacional Pedro Henríquez Ureña
(UNPHU)

Facultad de Ciencias jurídicas y Políticas
Escuela de Derecho

Aplicación y Legislación de las Firmas Digitales en el Comercio Dominicano

Trabajo de Grado para optar por el titulo de :
Licenciado en Derecho

Sustentando por:
Br. Ricardo E. Rafael Pozo
00-0653

Br. Leticia Ledesma
99-1018

Asesor:
Lic. Federico Fernández

Santo Domingo, D. N.
2005

Índice

V- Procedimiento

VI- Procedimiento de Autorización

VII-Seguridad de las firmas digitales

VIII- Órgano Regulador

IX- Condiciones para el uso de Firma Digital en Interacciones Documentales entre Entidades del Estado o entre Personas Privadas y Entidades del Estado.

Agradecimiento y dedicatoria

A Dios:

Por darme la fuerza y la inteligencia necesaria para completar una etapa más de mi vida, confiando siempre en que me guiaras en cada paso de mi vida, y me llenaras de dicha para llegar a la cima.

A mis Padres:

Mami, gracias por ser siempre la amiga y compañera que nunca me dejo caer, gracias por apoyarme, y darme siempre aminos para salir adelante.

Papi, gracias por tu apoyo y confianza, por haber estado conmigo en las buenas y en las malas, por ser un ejemplo a seguir.

Este triunfo también es de ustedes.

A mis Hermanos:

Raúl Alexander,
Yordy Raúl,
Roberto Alexis

Más que simples hermanos fueron y han sido mis amigos, mis compañeros, quienes siempre me apoyaron y dieron ánimos para seguir adelante.

A mis Amigos/as:

Para triunfar en la vida hace falta luchar, espero que al igual que yo tengan la fuerza suficiente para llegar al final de este camino, y conseguir todo lo que se propongan.

A los Profesores:

A todos y cada uno de ustedes que de alguna manera pusieron su granito de conocimiento, para por conducirme por el camino de sabiduría, gracias por todo.

A Federico Fernández:

Gracias por ser no solo un profesor, sino también un amigo, una fuente de conocimiento siempre dispuesta para ser bebida por el que este sediento, este agradecimiento inmenso es para un profesor y amigo.

Ricardo E. Rafael Pozo

Primero quiero dar gracias a Dios por permitirme concluir esta nueva etapa de mi vida con éxito por que sin el todo este andar no hubiese sido igual.

Quiero agradecer a mi madre por el amor, esfuerzo y apoyo que me brindo, a mi abuelo por su ayuda y cariño, a mí hermana, muy especialmente a mi amiga Elegía Rojas y a todos mis familiares y amigos que de una forma u otra me ayudaron a concluir victoriosamente este andar. Mil gracias...

Leticia Ledesma

Introducción

Cansados, sedientos y con la fe quebrantada por las promesas de libertad y bienestar incumplidas, el pueblo de Israel encaró a Moisés; él se encomendó al Señor, y éste le respondió: "sube a lo alto del cerro y detente allí, yo te daré unas tablas de piedra, con la enseñanza y los mandamientos que tengo escritos en ellas, a fin de que le enseñes al pueblo". Es así como desde tiempos del antiguo testamento el documento escrito es la forma más confiable de comunicación y conservación de la información. En efecto, el hombre, en su afán cada vez mayor por comunicarse con sus semejantes, a ido desarrollando las técnicas para hacer del documento escrito una herramienta segura. Dicho documento escrito era contenido primero en piedra, luego en papiro, en papel, y actualmente hemos podido observar su evolución hacia el soporte informático.

El uso cada vez más cotidiano y difundido de las nuevas tecnologías en materia de transmisión de datos de toda índole, parece mostrar un escenario futuro en el cual los documentos de elaboración electrónica han de reemplazar paulatinamente a los documentos tradicionales o manuales (los creados en soporte "papel"), para gran parte de los actos documentados de la vida cotidiana.

El Internet ha permitido el desarrollo de diversos servicios virtuales de comunicación. A través de éste podemos transferir archivos y documentos a larga distancia, obtener información sobre temas específicos a través de los buscadores o navegadores, podemos hacer negocios por medio de los Web Sites, comunicarnos a través del correo electrónico o simultáneamente de forma interactiva con otras personas, incluso obteniendo audio y video a través de los denominados Chats.

Al efectuarse una operación comercial en Internet se presentan múltiples problemas, por ejemplo: ¿cómo saber que la tienda virtual existe verdaderamente?; una vez hecho el pedido, ¿cómo saber que la información no será cambiada?; o, cuando se envía el número de una tarjeta de crédito, ¿cómo estar seguros de que éste permanecerá en privado?. Para el comerciante también se presentan problemas, por ejemplo, ¿cómo saber que el cliente es honesto?, ¿que es quien dice ser?, ¿que no está suministrando ningún tipo de información falsa?, etc.

La principal amenaza a las transacciones realizadas por medios electrónicos la constituye la interceptación de mensajes. Aunque no está al alcance de todas las personas, un operador bien experimentado, como los llamados hackers, pueden "capturar" la información. En esta situación se corren los siguientes riesgos:

- Que el autor del mensaje sea suplantado
- Que la información sea alterada, tanto de manera dolosa como accidental
- Que el emisor del mensaje niegue haberlo enviado o el destinatario haberlo recibido
- Que el contenido del mensaje de datos sea leído por una persona no autorizada

Ante estos peligros se han establecido cuatro requisitos o criterios de seguridad que debe cumplir todo mecanismo de comercio electrónico que se diga seguro.

Autenticación: Se refiere a la seguridad que existe sobre de la identidad de las partes envueltas en una transacción.

Integridad: Consiste en garantizar que el mensaje no ha sido alterado ni manipulado durante el envío.

No rechazo (no repudio): Se relaciona con la identidad del emisor y con la integridad del mensaje. Asegura tanto el no rechazo en el origen, es decir, que el emisor no pueda negar haber enviado determinado mensaje, como el no rechazo del contenido de dicho mensaje.

Confidencialidad o Privacidad: Evita que la información sea leída por una persona no autorizada. Para alcanzar estos niveles de seguridad se han desarrollado nuevas tecnologías y mecanismos, siendo la más importante hasta el momento la *Encriptación o cifrado de datos.*

"La Firma". En él vemos como nuestra legislación así como muchas extranjeras, le atribuyen un gran valor a la firma, convirtiéndola en un requisito indispensable en variadas actuaciones de la vida jurídica, ya sea para la validez del acto o para fines probatorios, en caso de eventuales conflictos y ahora utilizamos la firma digital como medio probatorio del documento digital y el comercio electrónico que es nuestro tema a tratar.

Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, se entenderá satisfecho dicho requerimiento en relación con un documento digital o un mensaje de datos, si éste ha sido firmado digitalmente y la firma digital cumple con los requisitos de validez establecidos en la ley de comercio electrónico y firmas digitales.

En toda interacción con entidad pública que requiera de documento firmado, este requisito se podrá satisfacer con uno o más documentos digitales o mensajes de datos que sean firmados digitalmente conforme a los requerimientos contenidos en esta ley. La reglamentación de esta ley especificará en detalle las condiciones para el uso de firma digital, certificados y entidades de certificación en interacciones documentales entre entidades del Estado o entre personas privadas y entes estatales que a continuación le vamos a detallar.

Importancia del Tema

Con lo "chivo" que es el dominicano, es decir lo inseguro que es cuando se habla de comerció electrónico, de realizar una transacción, efectuar un contrato por Internet y lo mas importante firmar dicho contrato. Por ende era necesario en nuestro país la incorporación de seguridad jurídica en este medio.

La Firma Digital viene a ponerle seguridad al medio electrónico, no solo a imponer al documento firmado el sello de la personalidad del emisor, sino que también proporciona al receptor los medios para verificar que el contenido no ha sido modificado por terceros.

La Firma Digital es tan importante que la ley No.126-02 de Comercio Electrónico, Documentos y Firmas Digitales le da a valor probatorio a los documentos digitales y mensajes de datos firmados digitalmente y tendrán la misma fuerza probatoria otorgada a los actos bajo firma privada en el Código Civil y en el Código de Procedimiento Civil.

Planteamiento del Problema

Ya tenemos la Firma Digital como medio de seguridad para todas a casi todas las transacciones realizadas vía Internet es decir el comercio electrónico y todas sus dependencias.

Pero:

1-¿Como se que la firma digital que recibo es segura?

2-¿Se puede falsificar un Firma Digital?

3-¿Cuál es el valor jurídico del Firma Digital?

4-¿Cómo Funciona?

Objetivo Principal

Esta presentación tratara de explicar de manera precisa que es una Firma Digital, cuales son sus características, su aplicación, seguridad, procedimiento, autorización, entidad certificadora, órgano regulador, valor jurídico y como esta regulada en nuestro país por la Ley No. 126-02 Comercio Electrónico, Documentos y Firmas Digitales, reglamento de aplicación por medio del Decreto No. 335-03, la resolución No. 042-03 del Instituto Dominicano de telecomunicaciones (INDOTEL) y sus normas complementarias.

I-Disposición general de la ley de comercio electrónico y firmas digitales

I.1) Ámbito de aplicación

La Ley 126-02 será aplicable a todo tipo de información en forma de documento digital o mensaje de datos, la Ley está inspirada, entre otros, en los principios generales siguientes:

a) Facilitar el comercio electrónico entre y dentro de las naciones.

b) Validar transacciones entre partes que sean realizadas por las nuevas tecnologías de la información.

c) Promover y emplear la implantación de nuevas tecnologías.

d) Promover la uniformidad de aplicación de la Ley.

e) Apoyar las prácticas comerciales.

Salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado Dominicano en virtud de convenios o tratados internacionales;

b) En las advertencias escritas que, por disposiciones legales, deban ir necesariamente impresas en ciertos tipos de productos en razón al riesgo que implica su comercialización, uso o consumo.

A fin de que la República Dominicana pueda aprovechar los beneficios que le confiere la práctica del Comercio Electrónico y del Gobierno Electrónico y de las transacciones realizadas por medios electrónicos, así como para cumplir con los objetivos de la Ley y los principios antes citados, es necesario establecer el marco regulatorio apropiado para la correcta aplicación de la Ley.

Este marco regulatorio deberá facilitar la aplicación práctica de la normativa que reconoce la validez del documento digital, eliminar los obstáculos representados por las disposiciones de derecho interno a la vez que se provea de la certidumbre que permita que puedan instrumentarse transacciones a través de medios electrónicos de manera confiable, como es la Firma digital que viene a asegurar las transacciones electrónica.

I.2) Definiciones:

I.2.1) Comercio electrónico

Es toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más documentos digitales o mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial, comprenden, sin limitarse a ellas, las siguientes operaciones:

- Toda operación comercial de suministro o intercambio de bienes, servicios o información;
- Todo acuerdo de distribución;
- Toda operación de representación o mandato comercial;
- De compra de cuentas por cobrar, a precio de descuento (factoring);
- De alquiler o arrendamiento (leasing);
- De construcción de obras;

- De consultoría;
- De ingeniería;
- De concesión de licencias;
- De inversión;
- De financiación;
- De banca;
- De seguros;
- Todo acuerdo de concesión o explotación de un servicio público;
- De empresa conjunta y otras formas de cooperación industrial o comercial;
- De transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carreteras.

I.2.2) Documento digital

Es la información codificada en forma digital sobre un soporte lógico o físico, en la cual se usen métodos electrónicos, fotolitográficos, ópticos o similares que se constituyen en representación de actos, hechos o datos jurídicamente relevantes.

I.2.3) Mensajes de datos

Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

I.2.4 Intercambio electrónico de datos (EDI)

Es la transmisión electrónica de información de una computadora a otra, cuando la información está estructurada conforme a alguna norma técnica convenida al efecto.

I.2.5) Iniciador

Es toda persona que, al tenor de un mensaje de datos, haya actuado por su cuenta o en cuyo nombre se haya actuado, para enviar o generar dicho mensaje antes de ser archivado, si este es el caso, pero que no lo haya hecho a título de intermediario con respecto a ese mensaje.

I.2.6) Destinatario

Es la persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a ese mensaje.

I.2.7) Intermediario

Es toda persona que, en relación con un determinado mensaje de datos, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

I.2.8) Sistema de información

Se entenderá por esto todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma documentos digitales o mensajes de datos.

I.2.9) Firma digital

Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y el texto del mensaje, y que el mensaje inicial no ha sido modificado después de efectuada la transmisión.

I.2.10) Criptografía

Es la rama de las matemáticas aplicadas y la ciencia informática que se ocupa de la transformación de documentos digitales o mensajes de datos de su representación original a una representación ininteligible e indescifrable que protege y preserva su contenido y forma, y de la recuperación del documento o mensaje de datos original a partir de ésta. También están la Clave criptográfica privada, que es el valor o valores numéricos o caracteres binarios que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos o de un documento digital y Clave criptográfica pública, que es el valor o valores numéricos o caracteres binarios que son utilizados para verificar que una firma digital fue generada con la clave privada del suscriptor del certificado digital que ha emitido el mensaje de datos o el documento digital.

I.2.11) Entidad de certificación

Es aquella institución o persona jurídica que, autorizada conforme a la ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

I.2.12) Certificado

Es el documento digital emitido y firmado digitalmente por una entidad de certificación, que identifica unívocamente a un suscritor durante el período de vigencia del certificado, y que se constituye en prueba de que dicho suscriptor es fuente u originador del contenido de un documento digital o mensaje de datos que incorpore su certificado asociado.

I.2.13) Repositorio

Es un sistema de información para el almacenamiento y recuperación de certificados u otro tipo de información relevante para la expedición y validación de los mismos;

I.2.14) Suscriptor

Es la persona que contrata con una entidad de certificación la expedición de un certificado, para que sea nombrada o identificada en él. Esta persona mantiene bajo su estricto y exclusivo control el procedimiento para generar su firma digital.

I.2.15) Usuario

Es la persona que sin ser suscriptor y sin contratar los servicios de emisión de certificados de una entidad de certificación, puede, sin embargo, validar la integridad y autenticidad de un documento digital o de un mensaje de datos, con base en un certificado del suscriptor originador del mensaje.

I.2.16) Revocar un certificado

Es finalizar definitivamente el período de validez de un certificado, desde una fecha específica, en adelante.

I.2.17) Suspender un certificado

Es interrumpir temporalmente el período operacional de un certificado desde una fecha específica, en adelante.

II- Normas

El cumplimiento de las normas fijadas para la aplicación del Reglamento es obligatorio para las Entidades de Certificación. El INDOTEL tiene la potestad para efectuar, de oficio o a solicitud de parte, verificaciones de cumplimiento de las disposiciones legales y reglamentarias en las Entidades de Certificación cuando lo considere necesario en la forma dispuesta por la Ley y sus normas reglamentarias.

Los actos administrativos que impliquen la modificación de normas para la prestación de servicios de certificación digital establecerán los plazos en los cuales las Entidades de Certificación deberán adecuarse a las mismas. El incumplimiento de las disposiciones de las nuevas normas será calificado como falta muy grave y facultará al INDOTEL a dejar sin efecto la autorización, de conformidad con los artículos 56 y 57 de la Ley.

Las Entidades de Certificación contarán con reglas específicas sobre sus prácticas de certificación, consistentes en una descripción detallada de las políticas, procedimientos, mecanismos y condiciones de prestación de los servicios así como las obligaciones que asumen.

Las Prácticas de Certificación deben declarar el cumplimiento de los requisitos señalados en el artículo 68 del Reglamento, con excepción de la póliza de seguro que se acredita por medio de la presentación de la misma.

Las Prácticas de Certificación deben ser objetivas y no discriminatorias, deben estar publicadas de conformidad con el artículo 38 de la Ley y se deben comunicar a los suscriptores y usuarios de manera sencilla y en idioma español.

Las Políticas de Certificación estarán sujetas a la aprobación del INDOTEL y deberán ser remitidas junto a la solicitud de autorización y deberán ser publicadas y actualizadas en forma permanente y deben estar accesibles al público por medios electrónicos, en la dirección correspondiente al sitio de que disponga la Entidad de Certificación, en el boletín del INDOTEL y en el sitio de Internet del INDOTEL.

Las disposiciones de las Prácticas de Certificación deberá contener de manera enunciativa, por lo menos la siguiente información:

a) Datos generales: El nombre, la dirección física y el número telefónico de la Entidad de Certificación; el número del Registro Nacional de Contribuyente (RNC); la dirección electrónica, en la cual serán válidas las comunicaciones y notificaciones; el certificado digital que contiene la clave pública actual de la Entidad de Certificación; el resultado de la evaluación obtenida por la Entidad de Certificación en la última auditoría realizada por el INDOTEL; si la autorización para operar como Entidad de Certificación ha sido revocada o suspendida, este registro deberá incluir la fecha de la revocación o suspensión para operar para todos los casos en los cuales se haya producido; los límites impuestos a la Entidad de Certificación en la autorización para operar;

cualquier evento que sustancialmente afecte la capacidad de la Entidad de Certificación para operar.

b) Políticas de Certificación que contemplen al menos los siguientes contenidos: Introducción, la cual contendrá un resumen de las prácticas de certificación de que se trate, mencionando tanto la entidad que suscribe el documento, como el tipo de suscriptores y productos a los que son aplicables; Consideraciones generales, las cuales contendrán información sobre obligaciones, responsabilidades, cumplimiento de auditorías, confidencialidad, y derechos de propiedad intelectual, con relación a todas las partes involucradas; identificación y autenticación, en la cual se describan los procesos de autenticación aplicados a los solicitantes de certificados, así como los procesos para autenticar a los mismos cuando pidan la suspensión o la revocación de un certificado. En caso de operar con una Unidad de Registro, la entidad suministrará los datos de esta Unidad; requerimientos operacionales, los cuales contendrán información operacional y procedimientos a seguir para los procesos de solicitud de certificados, emisión de certificados, suspensión y revocación de certificados, procesos de auditoría, de seguridad, almacenamiento de información relevante, cambio de datos de creación de firma digital, superación de situaciones críticas, casos de fuerza mayor, caso fortuito, y procedimiento de término del servicio de certificación; controles de procedimiento, personal y físicos, describirán los controles de seguridad no técnicos utilizados por la entidad de certificación para asegurar las funciones de generación de datos de creación de firma digital, autenticación de usuarios, emisión de certificados, suspensión y revocación de certificados, auditoría y almacenamiento de información relevante; controles de seguridad técnica, señalarán las medidas de seguridad adoptadas por la Entidad de Certificación para proteger los datos de creación de su propia firma digital ; perfiles de certificados y del registro de acceso público, especificarán los formatos del certificado y del registro de acceso público; especificaciones de administración

de la política de certificación, señalarán la forma en que la misma está contenida en la Práctica, y los procedimientos para cambiar, publicar y notificar dicha política.

c) Plan de Cese de Actividades

d) Plan de Contingencia

e) Política de Protección de Datos Personales, acorde con la normativa complementaria a ser dictada por el INDOTEL.

f) El reconocimiento de certificados extranjeros por parte de la Entidad de Certificación, en caso de que corresponda.

Cada Entidad de Certificación y cada Proveedor de Servicios de Firma Electrónica mantendrán un Registro de certificados accesible al público, en el que se garantice la disponibilidad de la información actualizada contenida en él de manera regular y continua.

Dicho Registro contendrá los certificados emitidos por las Entidades de Certificación y por los Proveedores de Servicios de Firma Electrónica, indicando el estatus de los certificados de modo tal que señale, al menos, lo siguiente:

a) Si los mismos se encuentran vigentes, revocados, suspendidos o reactivados;

b) Si son reconocidos por la Entidad de Certificación en caso de que hayan sido emitidos por una Entidad de Certificación extranjera;

c) La Política de Certificación bajo la cual fue emitido;

d) Las fechas de emisión y vencimiento;

e) Todas las menciones relevantes para la utilización de los mismos. Las Entidades de Certificación y los Proveedores de Servicios de firma electrónica garantizarán el acceso al público de manera permanente a dicho registro por medios electrónicos.

En caso de que una Entidad de Certificación cese en la prestación del servicio, notificará tal situación a los suscriptores de los certificados emitidos por ella en la siguiente forma:

Cesación voluntaria: Con una antelación no menor a NOVENTA (90) días hábiles y señalando a los suscriptores que de no existir objeción a la transferencia de los certificados a otra Entidad de Certificación, la cual será indicada en dicha notificación, dentro del plazo de QUINCE (15) días hábiles luego de la recepción de la comunicación, se entenderá que el suscriptor ha consentido la transferencia de los mismos.

Cesación no voluntaria: La cancelación de la autorización será notificada inmediatamente a los suscriptores. En caso de que la Entidad de Certificación se encuentre en situación de traspasar los certificados a otra
Entidad de Certificación, informará tal situación en la forma y plazo señalados anteriormente. Si el suscriptor del certificado comunica que se opone a la transferencia en el plazo establecido, el certificado será revocado sin ningún trámite adicional.

III- Aplicación de la legislación en el comercio

III.1) Autorización:

Es el acto jurídico mediante el cual, en forma escrita y formal, el INDOTEL otorga a una Entidad de Certificación el derecho a emitir certificados digitales con valor legal de firma digital y proveer otros servicios de certificación previstos por la Ley No.126-02 y sus normas reglamentarias.

III.2) Confiabilidad Técnica

Es la cualidad del conjunto de equipos de computación, software, protocolos de comunicación, seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos:

a) Protección contra la posibilidad de intrusión o uso no autorizado.

b) Garantía de la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento.

c) Aptitud para el desempeño de sus funciones específicas;

d) Cumplimiento de las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;

e) Cumplimiento con los estándares técnicos y de auditoria que establezca el INDOTEL.

III.3) Datos de creación de firma digital

Son aquellos datos únicos, tales como códigos o claves criptográficas privadas, que el suscriptor utiliza para crear su firma digital.

III.4) Datos de verificación de firma digital

Son aquellos datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital o mensaje de datos y la identidad del suscriptor.

III.5) Dispositivo de creación de firma digital

Es el dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

III.6) Dispositivo de verificación de firma digital

Es el dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del suscriptor.

III.7) Firma Digital

Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y el texto del mensaje, y que el mensaje inicial no ha sido modificado después de efectuada la transmisión.

III.8) Firma Electrónica

Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, que por acuerdo entre las partes se utilice como medio de identificación entre el emisor y el destinatario de un mensaje de datos o un documento digital y que carece de alguno de los requisitos legales para ser considerado firma digital.

III.9) Procedimiento de verificación de firma digital

Es el proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe constar por lo menos, de los pasos siguientes:

a) La verificación de que dicha firma digital ha sido creada durante el período de validez del certificado digital del suscriptor.

b) La comprobación de que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del suscriptor.

c) La verificación de la autenticidad y la validez de los certificados involucrados.

III.10) Proveedor de Servicios de Firma Electrónica

Es toda persona moral, nacional o extranjera, pública o privada, que preste servicios de certificación, y cuyos certificados digitales no tienen valor legal de firma digital, sin perjuicio de los demás servicios que puedan realizar.

III.11) Registro de Entidades de Certificación

Es el registro de acceso público que mantiene el INDOTEL en el cual constan las informaciones relativas a las Entidades de Certificación.

III.12) Unidad de Registro

Es toda persona moral o física, u organismo público, posibilitada a validar los datos de identidad de personas físicas y jurídicas, suscriptoras de certificados y en capacidad de prestar otros servicios de validación relacionados con las firmas digitales, conforme a la autorización otorgada a tales fines por el INDOTEL. En ingles, Registration Authority (RA).

IV- Entidades de Certificación

IV.1) Categorías

Las Entidades de Certificación, las Unidades de Registro y los Proveedores de Servicios de Firma Electrónica se encuentran regulados por la Ley, el presente Reglamento y sus normas complementarias, así como por las normas de derecho común aplicables.

IV.2) Entidades de Certificación

Son aquellas que, siendo personas jurídicas nacionales o extranjeras, públicas o privadas, y las Cámaras de Comercio y Producción, domiciliadas en la República Dominicana, que, previa solicitud, sean autorizadas por el INDOTEL en conformidad con la Ley, este Reglamento y las normas que dicte el INDOTEL, están facultadas para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así

como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales, sin perjuicio de los demás servicios que puedan realizar.

IV.3) Proveedores de Servicios de Firma Electrónica

Son aquellas personas morales, nacionales o extranjeras, públicas o privadas, que otorguen certificados digitales que carecen de valor legal de firma digital, sin perjuicio de los demás servicios que puedan realizar.

IV.4) Prestación de Servicios de Firma Electrónica

La prestación de servicios de certificación digital por Proveedores de Servicios de Firma Electrónica no requiere de autorización previa por parte del INDOTEL.

A los fines de proteger los derechos de los consumidores, el INDOTEL determinará la información a presentar y los procedimientos a cumplir por los Proveedores de Servicios de Firma Electrónica.

IV.5) Efectos de los Certificados emitidos por Proveedores de Servicios de Firma Electrónica

Los certificados y demás servicios de certificación prestados por los Proveedores de Servicios de Firma Electrónica no tienen el valor jurídico que la Ley otorga a la firma digital, esta circunstancia deberá constar en la información que suministren sobre sus servicios tanto en forma impresa como en formato digital, en el sitio de Internet de que dispongan y en general, en toda comunicación vinculada a los mismos.

Los Proveedores de Servicios de Firma Electrónica deberán comunicar expresamente tal circunstancia a los solicitantes y/o suscriptores de certificados digitales que emitan y a todo tercero que tome contacto con dicho Proveedor de Servicios de Firma Electrónica.

VI.6) Seguro

La Entidad de Certificación contará con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los requisitos que establezca la norma complementaria sobre las políticas de acreditación o autorización que dicte el INDOTEL.

IV.7) Obligaciones de las Entidades de Certificación

En adición a lo dispuesto en el artículo 40 de la Ley, las Entidades de Certificación tienen las siguientes obligaciones:

a) Comprobar por sí o por medio de una Unidad de Registro, en la cual haya delegado tal función, la identidad u otro dato de los solicitantes considerado relevante para los procedimientos de verificación de identidad previos a la emisión del certificado digital, según la Política de Certificación bajo la cual se solicita el certificado.

b) Mantener a disposición permanente del público las Políticas de Certificación y el Manual de Procedimientos, en aquellos aspectos que no contengan información confidencial, en los formatos que apruebe el INDOTEL a tales fines.

c) Cumplir cabalmente con las Políticas de Certificación acordadas con el suscriptor y con su Manual de Procedimientos, considerándose su incumplimiento como falta grave.

d) Garantizar la prestación establecida según los niveles definidos en el acuerdo de servicios pactado con el suscriptor, relativo a los servicios para los cuales solicitó autorización.

e) Informar al solicitante de un certificado digital, en un lenguaje claro y accesible, en idioma español, respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, si las hubiere, los precios de los servicios de certificación, uso, administración y otros asociados, incluyendo cargos adicionales y formas de pago, los niveles de servicio a proveer, las obligaciones que el suscriptor asume como usuario del servicio de certificación, su domicilio en la República Dominicana y los medios a los que el suscriptor puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

f) Disponer de un servicio de atención a suscriptores de certificados y usuarios, mediante acceso personal, telefónico y por Internet, que permita enviar las consultas y la pronta respuesta a la solicitud de suspensión o revocación de certificados.

g) Garantizar el acceso público, eficiente y gratuito de los suscriptores y usuarios al registro de certificados emitidos, suspendidos, revocados, reactivados o reconocidos.

h) Mantener actualizados los registros de certificados emitidos, suspendidos, revocados o reactivados por el término de CUARENTA (40) años, contado a partir de la fecha de la revocación o expiración de cada certificado.

i) Adoptar los procedimientos y resguardos de seguridad confiables, conforme lo establezca el INDOTEL para garantizar que las claves privadas de los

suscriptores no permanecerán en su poder ni podrán ser utilizadas por terceros en caso de que preste el servicio de generación de claves.

j) Informar al INDOTEL de modo inmediato la ocurrencia de cualquier evento que comprometa la correcta prestación del servicio; k) Garantizar la integridad de la información que mantienen bajo su control.

l) Respetar el derecho del suscriptor del certificado digital a no recibir publicidad de ningún tipo por su intermedio, salvo consentimiento expreso de éste;

m) Publicar por medios electrónicos y en un periódico de circulación nacional el certificado de clave pública correspondiente a la política de certificación para la cual obtuvo autorización.

n) Cumplir las normas y recaudos establecidos para la protección de datos personales, así como las demás normas aprobadas por el INDOTEL;

o) Cumplir con los requisitos establecidos en la Ley, el presente Reglamento y las normas que dicte INDOTEL que motivaron la autorización obtenida para la prestación de servicios de certificación.

p) En los casos de revocación de certificados contemplados en el numeral 6 del artículo 49 de la Ley, deberá sustituir en forma gratuita aquel certificado digital que ha dejado de ser seguro por otro que sí cumpla con estos requisitos.

El INDOTEL establecerá el proceso de reemplazo de certificados en estos casos. En los casos en los que un certificado digital haya dejado de ser seguro por razones atribuibles a su suscriptor, la Entidad de Certificación no estará obligada a sustituir el certificado digital.

q) Enviar los informes de estado de operaciones con carácter de declaración jurada que solicite el INDOTEL en las fechas y formatos determinados por la reglamentación que dicte el INDOTEL a tales fines.

r) Contar con personal idóneo y confiable, con antecedentes profesionales acordes a la función desempeñada, sin perjuicio de las responsabilidades legales que asume por los servicios suministrados.

s) Cumplir con los requerimientos realizados en virtud de sentencia con valor de la cosa irrevocablemente juzgada o autorización de un juez para entregar los datos.

t) Responder a los pedidos de informes por parte de los usuarios de certificados respecto de la validez y alcance de un certificado digital emitido por ella.

u) Informar al INDOTEL la terminación del contrato o las modificaciones respecto de los alcances o montos de la cobertura de los seguros.

IV.8) Responsabilidad de las Entidades de Certificación

En ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por una Entidad de Certificación comprometerá la responsabilidad civil del Estado en su calidad de órgano de control y vigilancia, ni en particular, la responsabilidad civil del INDOTEL, como entidad pública con personería jurídica.

IV.9) Recursos de las Entidades de Certificación

Para el desarrollo adecuado de las actividades para las cuales solicita autorización, la Entidad de Certificación evidenciará que cuenta con un equipo de profesionales, infraestructura física y tecnológica y recursos financieros, así como procedimientos y sistemas de seguridad que permitan:

a) Generar, en un ambiente seguro, las firmas digitales propias y todos los servicios para los cuales solicita autorización.

b) Cumplir con lo previsto en sus políticas y procedimientos de certificación.

c) Garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por el INDOTEL.

d) Expedir certificados que cumplan con:

Lo previsto en el artículo 44 de la Ley; los estándares tecnológicos aprobados por el INDOTEL; y la Política de Certificación correspondiente.

e) Garantizar la existencia de sistemas de seguridad física y lógica en sus instalaciones que aseguren el acceso restringido a los equipos que manejan los sistemas de operación de la Entidad de Certificación.

f) Proteger el manejo de la clave privada de la Entidad de Certificación mediante un procedimiento de seguridad que impida el acceso a la misma a personal no autorizado.

g) Proteger el acceso y el uso de la clave privada mediante procedimientos que exijan la participación de más de una persona;

h) Registrar las transacciones realizadas, a fin de identificar al autor y el momento de cada una de las operaciones.

i) Utilizar con exclusividad los sistemas que cumplan las funciones de certificación con ese propósito, sin que se les asigne ninguna otra función.

j) Proteger a todos los sistemas utilizados directa o indirectamente en la función de certificación con procedimientos de autenticación y seguridad de alto nivel de protección, que deben ser actualizados de acuerdo a los avances tecnológicos para garantizar la correcta prestación de los servicios de certificación.

K) Garantizar la continuidad de las operaciones mediante un Plan de Contingencia actualizado y probado.

l) Disponer de los recursos financieros adecuados al tipo de actividad de certificación que desarrolla, acorde con los niveles de responsabilidad derivados de la misma.

Los criterios de evaluación de lo dispuesto en el apartado anterior serán establecidos por el INDOTEL de acuerdo a estándares internacionales y la reglamentación dictada a tales fines.

V- Procedimiento

V.1) Notificaciones

Todas las notificaciones a las que se refiere la Ley y el Reglamento serán formuladas por escrito, utilizando por lo menos uno de los siguientes métodos:

a) Documentos digitales o mensajes de datos firmados digitalmente, transmitidos por protocolos de comunicación electrónica tales como correo electrónico, transferencia de archivos, entre otros.

b) Facsímile, con la condición de que el remitente pueda dejar constancia de la recepción.

c) Correspondencia con acuse de recibo.

d) Aquellas efectuadas por funcionarios acreditados del INDOTEL mediante actas de notificación.

e) Acto de Alguacil.

f) Cualquier otro medio físico o electrónico mediante el cual el INDOTEL pueda dejar constancia de la certitud de su recepción.

Para los efectos de este Reglamento, toda notificación que se haga de conformidad con las letras c), d) y e) deberá ser entregada, para el caso de una persona física o natural, a su persona o en el domicilio constituido, y para el caso de una persona jurídica, entregadas a la persona de su representante legal o un(a) funcionario(a) acreditado(a) del notificado, o en su domicilio constituido, en ambos casos, dejando constancia del día, hora y lugar en que se practicó la notificación, así como el nombre de la persona que la recibió y su relación con el requerido. Cuando sea aplicable, se deberá entregar una copia íntegra de la Resolución o documento de que se trate.

En el caso en que la persona a ser notificada se niegue a recibir o firmar la notificación, el funcionario del INDOTEL o Alguacil actuante levantará un

acta dando constancia de dicha circunstancia y procederá de conformidad con las disposiciones del Código de Procedimiento Civil Dominicano.

Toda notificación a una persona natural o jurídica cuyo domicilio se desconozca, será efectuada de conformidad con las disposiciones del Código de Procedimiento Civil Dominicano.

Las notificaciones realizadas por los funcionarios acreditados del INDOTEL harán fe de su contenido, hasta prueba en contrario.

El INDOTEL tiene la facultad de modificar los mecanismos para efectuar las notificaciones previstas en este Reglamento.

Las Entidades de Certificación, las Unidades de Registro y los Proveedores de Servicios de Firma Electrónica deberán constituir una dirección de correo electrónico ante el INDOTEL en la cual se considerarán válidas las comunicaciones y notificaciones.

Las disposiciones del presente artículo se aplican igualmente a las comunicaciones entre los sujetos regulados y los usuarios y suscriptores de certificados digitales.

V.2) Constitución de Domicilio

Las Entidades de Certificación, las Unidades de Registro y los Proveedores de Servicios de Firma Electrónica deben constituir domicilio ante el INDOTEL al momento de depositar su solicitud de Autorización o al momento de efectuar su primera presentación.

Los cambios del domicilio constituido deberán ser informados al INDOTEL.

En el caso de personas jurídicas deberán informar al INDOTEL los nombres y cambios que ocurran entre los miembros de su Consejo de Administración o Junta Directiva.

V.3) Presentación de Observaciones u Objeciones

Toda persona que acredite un interés legítimo y directo sobre una solicitud de autorización que se esté llevando a cabo por ante el INDOTEL tendrá la oportunidad de presentar observaciones u objeciones relacionadas directamente con dicha solicitud, siguiendo los procedimientos aplicables. Las observaciones recibidas no serán vinculantes para el INDOTEL.

V.4) Confidencialidad

Todo solicitante de una Autorización podrá requerir por escrito, que cierta información no sea objeto de inspección pública. Dicha solicitud de confidencialidad deberá:

a) Identificar el documento que contiene la información, describir las razones que la motivan y el plazo durante el cual se requiere la confidencialidad de la información.

b) Explicar la forma y medida en que la revelación de la información podría resultar en un perjuicio competitivo sustancial para el solicitante.

El INDOTEL revisará la solicitud, y emitirá su decisión dentro de un plazo de QUINCE (15) días calendario, contados a partir del recibo de la

misma, haciendo constar, en el caso de que acceda a la solicitud, el plazo durante el cual la información mantendrá el carácter confidencial.

Si las condiciones que motivan la solicitud se mantienen y se acerca la fecha de vencimiento del plazo fijado por el INDOTEL, el solicitante podrá requerir una extensión del indicado plazo, siempre y cuando presente la solicitud con por lo menos DIEZ (10) días calendario de antelación al vencimiento del mismo.

El INDOTEL revisará la solicitud y actuará conforme prescribe el artículo 54 numeral 2 de este Reglamento.

El INDOTEL no divulgará, por ninguna razón, información declarada confidencial, salvo en los siguientes casos:

a) Se convierta del dominio público por causas no atribuibles a un acto ilícito u omisión del INDOTEL o por el vencimiento del plazo durante el cual se otorgó carácter confidencial a la información.

b) Se encuentre disponible por medio de otra fuente, de buena fe y sin limitación alguna de su uso.

V.5) Cambio de Información

Las Entidades de Certificación, las Unidades de Registro y los Proveedores de Servicios de Firma Electrónica, tienen la obligación de informar ante el INDOTEL cualquier cambio de la información que hayan presentado, que no requiera de la aprobación previa del INDOTEL, pero que pueda afectar la autorización otorgada, dentro de los TREINTA (30) días calendario siguientes a la fecha efectiva del cambio.

La falta de cumplimiento de esta obligación constituirá una falta muy grave, y será sancionada de conformidad con la Ley.

Si la información fuere necesaria para la solución de un proceso o controversia, el INDOTEL podrá requerir la abreviación del plazo.

V.6) Resoluciones y su Contenido

El INDOTEL tomará sus decisiones por medio de Resoluciones, las cuales serán fechadas, numeradas consecutivamente y registradas en un medio de acceso público. Las resoluciones de carácter general, y otras de interés público que el INDOTEL determine, deberán ser además publicadas en un periódico de circulación nacional.

Las resoluciones del INDOTEL deberán estar debidamente motivadas y como mínimo incluir:

a) Descripción de las posiciones de las partes y de los motivos para aceptar o rechazar cada una de ellas.

b) Los hechos relevantes en que se fundamenta su adopción.

c) Las normas que aplican.

d) El interés público protegido.

e) El dispositivo de la Resolución.

V.7) Publicidad

Todas las actuaciones ante el INDOTEL y sus actos podrán ser consultados por el público en general, salvo que, por solicitud motivada de parte interesada, en un caso concreto y por el tiempo que se fije, el INDOTEL, basándose en razones de secreto o reserva comercial o de otro tipo que se justifique, determine no hacerlo público.

V.8) Recursos

Las decisiones del Director Ejecutivo y del Consejo Directivo podrán ser objeto de un recurso de reconsideración, el cual deberá ser sometido dentro del plazo de DIEZ (10) días calendario, contados a partir de la notificación o publicación del acto. Tanto el Director Ejecutivo cuanto el Consejo Directivo deberán pronunciarse en un plazo máximo de TREINTA (30) días calendario desde la interposición.

Asimismo, las decisiones del Director Ejecutivo podrán ser objeto de un recurso jerárquico por ante el Consejo Directivo. El Consejo Directivo deberá pronunciarse en un plazo máximo de QUINCE (15) días calendario desde dicha interposición.

Las decisiones del Consejo Directivo serán objeto de recurso jerárquico ante la Jurisdicción de lo Contencioso Administrativo, en la forma y plazos previstos por las normas que rigen la materia.

V.9) Motivos de Impugnación

Los recursos contra las decisiones del Consejo Directivo sólo podrán basarse en las siguientes causas:

a) Extralimitación de facultades.

b) Falta de fundamento sustancial en los hechos de la causa.

c) Evidente error de derecho.

d) Incumplimiento de las normas procesales aplicables.

V.10) Obligatoriedad de Recurso Administrativo

La vía administrativa previa es obligatoria para los sujetos regulados que quieran recurrir a la vía judicial.

V.11) Ejecución del Acto Administrativo

Los actos administrativos del INDOTEL serán de ejecución inmediata y de cumplimiento obligatorio, salvo la decisión de una autoridad competente que suspenda su ejecución.

V.12) Entrega de información

El INDOTEL podrá solicitar a los sujetos regulados informes, datos contables y estadísticos en los casos siguientes:

a) Cuando existiera una controversia en la que el INDOTEL deba de intervenir.

b) Cuando existiere una imputación de infracción y la misma estuviere estrictamente vinculada al hecho imputado.

c) Cuando la información sea necesaria y tenga una vinculación directa con la formulación de políticas o normas.

d) En los procesos de auditoría establecidos por la Ley, este Reglamento y las normas complementarias.

Los informes deberán ser proporcionados en los plazos razonables que se fijen en cada oportunidad, los que no podrán ser inferiores a CINCO (5) días hábiles. En los casos previstos, los sujetos regulados deberán permitir el libre acceso del INDOTEL a los libros, documentación contable e información registrada bajo cualquier forma.

El INDOTEL podrá requerir directamente el auxilio de la fuerza pública para el ejercicio de las facultades que le confiere la Ley.

El INDOTEL podrá establecer los requisitos mínimos razonables que reunirá la contabilidad de los sujetos regulados. Asimismo, establecerá los requisitos mínimos razonables para el suministro y conservación de la información contable, de costos y de operaciones.

VI- Procedimiento de Autorización

VI.1) Autorización para operar como Entidad de Certificación

La autorización, es el procedimiento en virtud del cual el INDOTEL confirma que la Entidad de Certificación cuenta con los procedimientos, sistemas y los recursos humanos necesarios para brindar servicios de certificación digital.

Se requiere autorización por parte del INDOTEL para la provisión de los siguientes servicios vinculados a la firma digital, de acuerdo con lo establecido

por los artículos 35 inciso a), 36 y 56 numeral 1) de la Ley, sin perjuicio de la facultad reglamentaria del INDOTEL para modificar el presente listado:

a) Servicios de emisión, administración, registro y conservación de certificados digitales.

b) Servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos.

c) Servicios de registro y estampado cronológico de documentos digitales.

d) Servicios de almacenamiento seguro de documentos digitales.

e) Servicios prestados por Unidades de Registro.

f) Servicios de certificación de documentos digitales firmados digitalmente.

g) Otros servicios o actividades relacionados a la firma digital a ser determinados por el INDOTEL.

Además, las Entidades de Certificación deben solicitar autorización para efectuar transferencias, cesiones, arrendamientos, otorgamientos del derecho de uso, constitución de gravámenes o transferencia de control accionario en los términos que se establece la Ley, el Reglamento y las normas complementarias a ser dictadas por el INDOTEL.

VI.2) Requisitos para solicitar autorización

La solicitud de autorización para la prestación de servicios de certificación digital es voluntaria.

Para obtenerla la solicitante, deberá cumplir, al menos, con las siguientes condiciones:

a) Demostrar la confiabilidad necesaria de sus servicios de acuerdo con las normas técnicas y de procedimientos aprobadas por el INDOTEL.

b) Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos.

c) Emplear personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma digital y los procedimientos de seguridad y gestión adecuados.

d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación.

e) Haber contratado un seguro apropiado en los términos que señala el artículo 16 del Reglamento.

f) Contar con la capacidad tecnológica informática y de comunicaciones necesaria para el desarrollo de la actividad de certificación

g) Cumplir los demás recaudos que establezca el INDOTEL.

El cumplimiento de dichas condiciones será evaluado por el INDOTEL de conformidad con las normas técnicas y de procedimientos aplicables a la prestación del servicio, durante el procedimiento de autorización.

VI.3) Contenidos de la solicitud de autorización

En la solicitud de autorización, las Entidades de Certificación especificarán las actividades o servicios para las cuales requieren autorización, y acreditarán ante el INDOTEL por los medios que éste determine, lo siguiente:

a) Documentación demostrando su personería jurídica.

b) Autorización del organismo de dirección correspondiente para iniciar el procedimiento de obtención de autorización para operar como Entidad de Certificación, cuando se trate de instituciones.

c) Políticas de certificación para la cual solicita autorización, que respaldan la emisión de sus certificados, Manual de Procedimientos, Plan de Seguridad, Plan de Cese de Actividades y Plan de Contingencia de acuerdo con los requisitos establecidos por las normas emitidas por el INDOTEL.

d) Toda otra documentación requerida por el INDOTEL.

VI.4) Procedimiento de Solicitud

Recibida la solicitud de autorización, el INDOTEL procederá a analizar la admisibilidad de la misma mediante la verificación de los antecedentes requeridos, en un plazo de DIEZ (10) días hábiles.

De ser inadmisible la solicitud, dentro de los TRES (3) días hábiles se procederá a comunicar al solicitante tal situación. En dicha comunicación, se otorgará plazo no inferior a QUINCE (15) días hábiles, para que complete los

antecedentes, información o documentación, bajo la advertencia de ser rechazada la solicitud.

Una vez admitida la solicitud, el INDOTEL procederá a un examen sobre el cumplimiento de los requisitos y obligaciones exigidas por la Ley y el Reglamento para obtener la autorización. Este examen se realizará mediante la elaboración de una auditoría de inicio, ya sea por el INDOTEL o por terceros, certificando dentro del plazo de NOVENTA (90) días hábiles contados desde la fecha de la admisibilidad de la solicitud, prorrogables por una vez e igual período y por motivos fundados, que el interesado cumple los requisitos y obligaciones para ser autorizado y que dispone de un plazo de VEINTE (20) días hábiles para presentar la póliza de seguros que exige el Reglamento, a pena de ser rechazada la solicitud.

VI.5) Incumplimiento de los Requerimientos Técnicos o de Procedimientos

En caso de que el INDOTEL determine que la Entidad de Certificación no cumple con los requerimientos fijados en las normas para el desarrollo de la actividad, señalará si estos incumplimientos son subsanables, y si no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley, el Reglamento y las normas complementarias.

En caso de que los incumplimientos no sean subsanables, el INDOTEL procederá a dictar una resolución en la que rechaza la solicitud de autorización.

Si los incumplimientos son subsanables y no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley, el Reglamento y las normas complementarias, el INDOTEL otorgará un plazo para la subsanación de los incumplimientos. Vencido dicho plazo, el INDOTEL verificará si se han

aplicado las medidas correctivas, y procederá a dar continuidad al trámite en caso afirmativo o a dictar una resolución rechazando la solicitud de autorización.

VI.6) Alcance del Otorgamiento de la Autorización y de la Inscripción en el Registro de Entidades de Certificación

El otorgamiento de la autorización no implica que el INDOTEL, las entidades de auditoría o cualquier organismo del Estado, garantice la provisión de los servicios de certificación o los productos ofrecidos por la Entidad de Certificación. La responsabilidad por la prestación de los servicios de certificación digital corresponde exclusivamente a cada entidad de certificación.

La inscripción en el Registro no exime a la Entidad de Certificación de la obligación de obtener otras autorizaciones necesarias para ofrecer otros servicios y para la efectiva implementación de los sistemas autorizados.

VI.7) Duración de la Autorización

La autorización para funcionar como entidad de certificación tendrá un plazo de duración de cinco (5) años, pudiendo ser renovada, previo dictamen favorable de auditoría. Su vigencia se encontrará condicionada al resultado de las auditorías periódicas y a las inspecciones dispuestas por el INDOTEL.

Las Entidades de Certificación deberán efectuar anualmente un informe de estado de operaciones con carácter de declaración jurada en el cual conste el cumplimiento de las normas establecidas en la Ley, en el Reglamento y las normas complementarias. Las Entidades de Certificación serán sometidas a

auditorías periódicas. El formato y procedimientos para la auditoría serán determinados por el INDOTEL.

VI.8) Causas de suspensión de la autorización

El INDOTEL dispondrá de oficio la suspensión de la autorización en los siguientes casos:

a) Falta de presentación del informe de estado de operaciones con carácter de declaración jurada anual.

b) Falsedad de los datos contenidos en el informe de estado de operaciones con carácter de declaración jurada anual.

c) Dictamen desfavorable de auditoría basado en causas graves.

d) Informe de la inspección dispuesta por el INDOTEL desfavorable basado en causas graves.

e) Cuando la Entidad de Certificación no permita la realización de auditorías o inspecciones dispuestas por el INDOTEL.

f) Cuando el titular de la Entidad de Certificación haya sido condenado en causa penal con sentencia de carácter de cosa juzgada.

VI.9) Revocación de la autorización

El INDOTEL podrá dejar sin efecto la autorización mediante Resolución debidamente motivada, por las causas siguientes.

Dicha Resolución deberá ordenar la cancelación de la inscripción en el Registro de Entidades de Certificación.

VI.10) Causas de Revocación de la Autorización

La autorización a las Entidades de Certificación se dejará sin efecto por las siguientes causas:

a) Por solicitud de la Entidad de Certificación, ante el INDOTEL con una antelación no menor a NOVENTA (90) días hábiles previa a la cesación de actividades prevista, indicando el destino que dará a los certificados, a los datos y documentación de apoyo de ellos, para lo cual deberá cumplir con lo dispuesto en el artículo 11 del Reglamento, y garantizar el pago del aviso que deberá ser publicado de conformidad con lo dispuesto a continuación.

b) Por pérdida de las condiciones que sirvieron de fundamento a su autorización, la que será calificada por el INDOTEL en cumplimiento de la facultad de inspección.

c) Por reincidencia en las causas de suspensión de la autorización indicadas en el Reglamento.

d) Por incumplimiento grave o reiterado de las obligaciones que establece la Ley.

e) Por el estado de cesación de pagos de la Entidad de Certificación, declarado por sentencia irrevocable del tribunal competente.

f) Por reincidencia en la comisión de infracciones graves o muy graves.

g) Por imposibilidad de cumplimiento del objeto social del autorizado según su mandato estatutario en la medida en que esté relacionado con la autorización otorgada.

h) Por la suspensión injustificada del servicio.

i) Por haber efectuado una transferencia, cesión, arrendamiento, otorgamiento del derecho de uso, constitución de gravámenes o transferencia de control accionario sin autorización del INDOTEL.

j) Por cualquier otra acción de las Entidades de Certificación que decida el INDOTEL, mediante resolución debidamente motivada y que atente en forma deliberada en contra de los principios de la Ley.

En los casos de las letras b), c), d), e), f), g) h) e i), la Resolución deberá ser adoptada previo traslado de cargos y audiencia del afectado, para lo cual el INDOTEL dará un plazo de CINCO (5) días hábiles para que éste presente por escrito la respuesta a los cargos formulados. Recibida esta, el INDOTEL deberá resolver dentro del plazo de QUINCE (15) días hábiles, prorrogables por el mismo período por motivos fundamentados.

En los casos que los incumplimientos o condiciones objetivas impliquen un grave riesgo para la Infraestructura de Clave Pública de la República Dominicana, el INDOTEL podrá suspender preventivamente de inmediato todas o algunas de las actividades de la entidad infractora, mediante Resolución motivada.

VII-Seguridad de las firmas digitales

VII.1) Firma digital segura

Para la emisión de certificados de firma digital segura contemplada en el artículo 32 de la Ley, la Entidad de Certificación deberá comprobar fehacientemente la identidad del solicitante antes de su emisión, y cumplir con las normas técnicas y de procedimientos que dicte el INDOTEL.

La Entidad de Certificación podrá efectuar dicha comprobación por sí o por medio de Unidades de Registro, requiriendo la comparecencia personal y directa del solicitante o de su representante legal si se tratare de una persona jurídica.

La comprobación de los datos de identidad de las personas que soliciten la emisión de un certificado digital enmarcado en una Política de Certificación para firma digital segura, se efectuará en base al número de la Cédula de Identidad y Electoral, al del Pasaporte o al de cualquier otro documento oficial de identidad personal que el Estado Dominicano adopte en el futuro.

En el caso de que la persona física no sea de nacionalidad dominicana, la comprobación de los datos de identidad del solicitante de un certificado digital enmarcado en una Política de Certificación para firma digital segura se efectuará en base al número de Pasaporte.

El INDOTEL establecerá los procedimientos y documentos que serán considerados para la comprobación de la identidad de las personas menores de edad que soliciten la emisión de un certificado digital.

VII.2) Resguardo de la clave privada

Los datos de creación de una firma, cuando sean generados por la Entidad de Certificación, deben ser entregados al suscriptor del certificado a fin de garantizar la recepción de los mismos en forma personal y confidencial. A partir de este momento la clave privada queda bajo el control y responsabilidad del suscriptor para los efectos previstos en la Ley.

Queda prohibido a la Entidad de Certificación mantener copia de los datos de creación de firma digital una vez que éstos hayan sido entregados a su suscriptor, momento desde el cual éste comenzará a ser responsable de mantenerlos bajo su exclusivo control.

El incumplimiento de las disposiciones sobre resguardo de la clave privada dispuestas anteriormente constituye una falta muy grave que dará lugar a la inmediata suspensión de la autorización, sin perjuicio de la responsabilidad civil y penal que pudiera corresponder.

VII.3) Alcance del Uso de Certificados Digitales

El certificado digital podrá ser usado por su suscriptor de conformidad con las disposiciones establecidas en la Política de Certificación de la Entidad de Certificación con quien se ha contratado la emisión y administración del mismo.

El certificado digital deberá permitir, a quien lo reciba, verificar, en forma directa o mediante consulta electrónica o por cualquier otro medio razonablemente disponible, que ha sido emitido por una Entidad de Certificación con la finalidad de comprobar la validez del mismo.

VII.4) Suspensión de Certificados Digitales

Las Entidades de Certificación procederán a suspender la vigencia del certificado cuando se verifique alguna de las siguientes circunstancias:

a) Solicitud del suscriptor del certificado;

b) Iniciación del trámite de ausencia con presunción de fallecimiento del suscriptor del certificado, o por iniciación de un procedimiento de declaratoria de incapacidad, en ambos casos, mediante decisión provisional del Juez competente.

c) Decisión de la Entidad de Certificación en virtud de razones técnicas, circunstancia que será comunicada en forma inmediata en un plazo máximo de VEINTICUATRO (24) horas al suscriptor del certificado y al INDOTEL.

d) Mediante sentencia de un tribunal con autoridad de la cosa irrevocablemente juzgada.

e) En virtud de las demás causas dispuestas en la Política de Certificación de cada Entidad de Certificación debidamente aprobada por el INDOTEL.

VII.5) Efectos de la Suspensión del Certificado

El efecto de la suspensión del Certificado es la cesación temporal de sus efectos jurídicos conforme a los usos que le son propios e impide el uso legítimo del mismo por parte del suscriptor, a partir de la notificación y durante el lapso que ésta perdure.

La suspensión del Certificado terminará por cualquiera de las siguientes causas:

a) Por la decisión de la Entidad de Certificación de revocar el Certificado, en los casos previstos en la Ley, el reglamento y las normas técnicas complementarias.

b) Por la decisión de la Entidad de Certificación de levantar la suspensión del Certificado, una vez que cesen las causas que la originaron.

c) Por la decisión del suscriptor del certificado, cuando la suspensión haya sido solicitada por éste, y este hecho sea comunicado a la Entidad de Certificación.

d) Por sentencia del tribunal con autoridad de la cosa irrevocablemente juzgada que declara la incapacidad, o la ausencia temporal con presunción de fallecimiento o el fallecimiento por ausencia definitiva del suscriptor del certificado, que implica su revocación.

e) En virtud de las demás causas dispuestas en la Política de Certificación debidamente aprobada por el INDOTEL.

VII.6) Revocación de Certificados Digitales

Los certificados digitales quedarán sin efecto por la revocación practicada por la Entidad de Certificación.

La revocación tendrá lugar cuando la Entidad de Certificación constate y comunique de manera formal por los medios establecidos en el artículo 51 del Reglamento alguna de las siguientes circunstancias:

a) La solicitud del suscriptor del certificado digital.

b) La solicitud de un representante legal del suscriptor del certificado, acreditando la representación invocada.

c) Si se determina que un certificado digital fue emitido en base a una información falsa que en el momento de la emisión hubiera sido objeto de verificación.

d) Si se determina, en virtud de la auditoría realizada, que los procedimientos de emisión o verificación han dejado de ser seguros.

e) Por condiciones especiales definidas en las Políticas de Certificación.

f) Por decisión judicial o de entidad administrativa competente, debidamente motivada.

g) Por fallecimiento del titular o disolución de la persona jurídica suscriptor.

h) Por declaración judicial de ausencia con presunción de fallecimiento del suscriptor.

i) Por declaración mediante sentencia con autoridad de la cosa irrevocablemente juzgada de incapacidad jurídica del suscriptor.

j) Por la determinación de que la información contenida en el certificado ha dejado de ser válida.

k) Por la cesación de la relación de representación, laboral o contractual respecto de una persona jurídica o de un organismo público.

l) En caso de revocación, ordenada por el INDOTEL, de la autorización para funcionar otorgada a la Entidad de Certificación, siempre que no se haya decidido la transferencia del certificado a otra Entidad de Certificación.

m) Por la cesación de actividades de la Entidad de Certificación y siempre que no se haya decidido la transferencia del certificado a otra Entidad de Certificación.

El efecto de la revocación del certificado digital es la cesación permanente y definitiva de los efectos jurídicos de éste conforme a los usos que le son propios e impide su uso legítimo a partir del momento de la revocación.

VII.7) Procedimiento de Suspensión o Revocación

La revocación de un certificado digital podrá producirse de oficio o a solicitud de su suscriptor por la concurrencia de algunas de las causas previstas en la Ley, el Reglamento, normas complementarias o en las políticas de certificación debidamente aprobadas por el INDOTEL.

La solicitud de suspensión o revocación, según corresponda, será dirigida a la Entidad de Certificación o a la Unidad de Registro dependiente de la misma, en cualquiera de las formas que prevean sus Políticas de Certificación.

La suspensión o revocación del certificado deberá ser notificada inmediatamente en un plazo máximo de VEINTICUATRO (24) horas a su suscriptor, por los medios establecidos en el artículo 51 del Reglamento, sin perjuicio que deba publicarse en el Registro de acceso público que señala el artículo 51 de la Ley.

Tratándose de la suspensión por razones técnicas o revocación del certificado digital por las circunstancias previstas en los incisos b), i) o j) del tema VII.6, dicha decisión deberá ser comunicada al suscriptor con una anterioridad de, por lo menos, VEINTICUATRO (24) horas a su puesta en práctica, indicando la causa que la provoca y el momento en que se hará efectiva, por los medios establecidos en el artículo 51 del Reglamento.

El término de la vigencia del certificado será oponible a terceros desde el momento de la publicación de la suspensión o revocación en el registro de acceso público que señala el artículo 51 de la Ley.

VII.8) Reconocimiento de Certificados Extranjeros

Las Entidades de Certificación podrán reconocer los certificados digitales emitidos por Entidades de Certificación extranjeras, bajo su responsabilidad.

Para ello la Entidad de Certificación demostrará al INDOTEL que los certificados a ser reconocidos por ella, han sido emitidos por un prestador de servicios de certificación no establecido en República Dominicana que cumple con normas técnicas y de procedimientos equivalentes a las establecidas en la Ley, el Reglamento, sus normas complementarias y modificaciones, para el desarrollo de la actividad. En particular, deberá acreditar que los certificados a ser reconocidos por ella, cumplen las disposiciones referentes a contenidos mínimos de los certificados, establecidas en las normas emitidas por el INDOTEL.

El INDOTEL verificará el cumplimiento de las disposiciones legales y reglamentarias, y publicará la información sobre el reconocimiento en el Registro de Entidades de Certificación. En caso de que la Entidad de Certificación no acredite el cumplimiento de los recaudos legales y

reglamentarios para el reconocimiento de certificados extranjeros, el INDOTEL mediante resolución motivada, rechazará la solicitud de reconocimiento.

Una vez practicado el reconocimiento la Entidad de Certificación, en un plazo de TRES (3) días hábiles, comunicará tal situación al INDOTEL y la publicará, inmediatamente en un plazo máximo de VEINTICUATRO (24) horas, en el Registro de acceso público contemplado en el artículo 51 de la Ley.

El reconocimiento de certificados deberá estar declarado en las Prácticas de Certificación.

VIII- Órgano Regulador

VIII.1) Facultad Regulatoria

El INDOTEL está facultado para establecer:

a) Los estándares tecnológicos aplicables en consonancia con estándares internacionales vigentes.

b) Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos internacionales vigentes.

c) Las condiciones mínimas de emisión de certificados digitales.

d) Los casos en los cuales deben suspenderse o revocarse los certificados digitales.

e) Los datos considerados públicos contenidos en los certificados digitales.

f) Los mecanismos que garanticen la validez y autoría de las listas de certificados revocados;

g) La información que los sujetos regulados deberán publicar por la Internet.

h) La información que las Entidades de Certificación deberán publicar en los medios establecidos por el reglamento.

i) Los procedimientos mínimos de revocación de los certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operación de las Entidades de Certificación, en el caso que éstas cesen en su actividad.

j) El sistema de inspección y auditoría sobre los sujetos regulados, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación de entidades para efectuar auditorías y los criterios y estándares de auditoría mínimos que deberán cubrir.

k) Las condiciones y procedimientos para el otorgamiento y revocación de las autorizaciones.

l) El procedimiento de instrucción y la gradación de sanciones previstas en la Ley, en virtud de reincidencia y/u oportunidad.

m) Los procedimientos aplicables para el reconocimiento de certificados extranjeros.

n) Los acuerdos de reconocimiento mutuo de certificados digitales con otros países.

o) Las condiciones de aplicación de la Ley y el reglamento en el sector público dominicano, incluyendo la autorización para prestar servicios de certificación digital para sus entidades y jurisdicciones.

p) Los contenidos mínimos de las políticas de certificación de acuerdo con estándares nacionales e internacionales;

q) Las condiciones mínimas que deberán cumplirse en el caso de cesación de actividades de una Entidad de Certificación;

r) Los tipos de riesgos que cubrirán los seguros que deberán ser contratados por las Entidades de Certificación, y los montos correspondientes de contratación y cobertura.

s) Las condiciones de prestación de otros servicios en relación con la firma digital y otros aspectos contemplados en la Ley.

t) La modificación y actualización de los temas considerados en los apartados precedentes.

VIII.2) Funciones del INDOTEL

Sin perjuicio y en adición a las funciones asignadas por la Ley, el INDOTEL ejercerá la función de entidad de vigilancia y control de las actividades desarrolladas por los sujetos regulados. Tendrá, en especial, las siguientes funciones:

a) Autorizar, la operación de Entidades de Certificación en el territorio nacional.

b) Velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de los sujetos regulados y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad.

c) Efectuar las inspecciones y auditorías previstas en la Ley, el Reglamento y las normas complementarias.

d) Definir reglamentariamente los requerimientos técnicos que califiquen la idoneidad de las actividades desarrolladas por los sujetos regulados.

e) Aprobar las políticas de certificación, el manual de procedimientos, el plan de seguridad, el plan de cese de actividades y el plan de contingencia, presentados por las Entidades de Certificación que requieren autorización.

f) Evaluar las actividades desarrolladas por los sujetos regulados conforme a los requerimientos definidos en los reglamentos técnicos.

g) Denegar, revocar o suspender la autorización para operar a las Entidades de Certificación que no cumplan con los requisitos establecidos por la Ley, el Reglamento y las normas complementarias.

h) Requerir en cualquier momento a los sujetos regulados para que suministren información relacionada con los certificados, las firmas digitales emitidas y los documentos en soporte informático que custodien o administren.

i) Disponer el proceso de instrucción y la posterior aplicación de sanciones por el incumplimiento de las obligaciones derivadas de la prestación de servicio;

j) Ordenar la revocación o suspensión de certificados cuando la Entidad de Certificación los emita sin el cumplimiento de las formalidades legales.

k) Emitir certificados en relación con las firmas digitales de las Entidades de Certificación, en caso de considerarlo necesario.

l) Publicar en la Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos, direcciones de la Internet y certificados digitales de: las Entidades de Certificación, las Entidades de Certificación cuyas autorizaciones hayan sido revocadas.

m) Administrar los recursos generados de acuerdo con lo dispuesto por el artículo 44 del reglamento, provenientes de las distintas fuentes de financiamiento.

n) Fijar en casos concretos, el concepto y los importes de todo tipo de costos, derechos y multas previstas.

o) Solicitar ampliación o aclaración sobre la documentación presentada por los sujetos regulados.

p) Velar por el correcto manejo y mantenimiento de la confidencialidad, por parte de los sujetos regulados, de las informaciones de los suscriptores y sus respectivos certificados digitales.

q) Velar por la observancia de las disposiciones legales sobre la promoción de la competencia y la protección de los derechos de los consumidores y usuarios, en los mercados atendidos por las entidades de certificación.

r) Permitir el acceso público permanente a la información actualizada del Registro de Entidades de Certificación y a los certificados de clave pública de

las mismas, por medio de conexiones de telecomunicaciones públicamente accesibles. Esto también se aplica a la información sobre nombres, domicilio constituido, dirección electrónica y números telefónicos propios, de las Entidades de Certificación y las Unidades de Registro.

s) Supervisar la ejecución del plan de cese de actividades de las Entidades de Certificación que cesan sus funciones.

t) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas.

u) Supervisar la ejecución de planes de contingencia de las Entidades de Certificación.

v) Efectuar las tareas de control del cumplimiento de las recomendaciones formuladas en los dictámenes de auditoría a los sujetos regulados, para determinar, en su caso, si el auditado ha tomado las acciones correctivas correspondientes.

w) Recibir los reclamos de los suscriptores y usuarios de certificados digitales relativos a la prestación del servicio por parte de los sujetos regulados.

x) En su calidad de suscriptor de un certificado digital, debe cumplir idénticas obligaciones que los suscriptores de certificados y que las Entidades de Certificación, en relación con el resguardo de las medidas de seguridad sobre su clave privada y su certificado digital.

VIII.3) Fijación de Costos y Derechos

El INDOTEL podrá fijar y cobrar, a los sujetos regulados por la Ley y el Reglamento, derechos por los costos de procesamiento y derechos de supervisión, para cubrir total o parcialmente su costo operativo y de las inspecciones y auditorías realizadas por sí o por terceros contratados a tal efecto.

Los recursos propios del INDOTEL se integrarán con:

a) Los importes provenientes de los costos y derechos, previstos en el apartado anterior, correspondientes a los siguientes servicios:

1. servicios de certificación digital.

2. servicios de certificación digital de fecha y hora ciertas.

3. servicios de almacenamiento seguro de documentos digitales.

4. servicios prestados por Unidades de Registro.

5. servicios prestados por terceras partes confiables.

6. servicios de certificación de documentos digitales firmados digitalmente.

7. otros servicios o actividades relacionados a la firma digital.

b) Los importes provenientes de los derechos de supervisión aplicados a los sujetos regulados.

c) Los subsidios, herencias, legados, donaciones o transferencias bajo cualquier título que reciba.

d) Los ingresos percibidos por el pago de las multas aplicadas a los sujetos regulados.

e) Las asignaciones presupuestarias que en su caso le asigne el Gobierno Central, en el Presupuesto de Ingresos y Ley de Gastos Públicos.

f) Los demás fondos, bienes o recursos que puedan serle asignados en virtud de la Ley de Telecomunicaciones.

g) Las contribuciones provenientes de aplicaciones que utilicen firmas digitales, a ser determinados por las normas respectivas.

VIII.4) Facultad de Inspección

A los fines de efectuar las auditorías, el INDOTEL ejercerá la facultad de inspección conferida por la Ley No.126-02 y la Ley de Telecomunicaciones.

El INDOTEL ejercerá la facultad de inspección sobre las Entidades de Certificación, las Unidades de Registro y los Proveedores de Servicios de firma digital y velará por el cumplimiento de las disposiciones legales y reglamentarias por parte de los mismos. En relación con las Entidades de Certificación, el INDOTEL velará por la observancia de los requisitos que se aprobaron al momento de otorgarse la autorización y las obligaciones que imponen la Ley, el Reglamento y las normas complementarias.

El INDOTEL ejercerá la facultad de auditoría e inspección sobre los sistemas y procedimientos de los proveedores de servicios o infraestructura contratados por la Entidad de Certificación.

La facultad de inspección comprende tanto la inspección ordinaria como la extraordinaria. La inspección ordinaria consiste en la facultad de practicar auditorías periódicas a las instalaciones de las entidades sujetas al control y vigilancia del INDOTEL, como asimismo realizar un monitoreo permanente sobre el desarrollo de la actividad. La inspección extraordinaria será practicada de oficio o por denuncia motivada sobre la prestación del servicio, ordenada por el INDOTEL mediante resolución fundada.

Las inspecciones podrán ser practicadas por medio de funcionarios de planta o por peritos especialmente contratados y habilitados para estos fines por el INDOTEL, los que en el ejercicio de sus funciones, podrán requerir a las entidades sujetas a vigilancia y control información adicional a la proporcionada originariamente.

La información solicitada por el INDOTEL deberá ser proporcionada dentro del plazo de cinco (5) días hábiles, contados desde la fecha de la solicitud.

El INDOTEL fijará los criterios que deben cumplir los terceros contratados para efectuar las inspecciones y auditorías.

VIII.5) Registro de Entidades de Certificación

El INDOTEL mantendrá un Registro de Entidades de Certificación, el cual formará parte del Registro Nacional. Sin perjuicio de lo que pudiera disponer el INDOTEL, el Registro de Entidades de Certificación contendrá los siguientes datos:

a) Número de resolución que concede la autorización.

b) Nombre o razón social de la Entidad de Certificación, su domicilio, el nombre de su Representante Legal, el número de su teléfono, la dirección electrónica de su sitio de dominio y de la cuenta de correo electrónico en la cual serán válidas las notificaciones, así como los datos de la compañía de seguros con que ha contratado la póliza de seguros, en su caso.

c) El Certificado Digital que contiene la clave pública de la Entidad de Certificación.

d) La fecha en que expira la autorización para operar.

e) El resultado de la evaluación obtenida por la Entidad de Certificación en la última auditoría e inspección realizada por el INDOTEL.

f) Estatus de la autorización para operar señalando si ésta en algún momento ha sido revocada, suspendida o ha caducado.

El acceso a los datos públicos del Registro de Entidades de Certificación, deberá poder efectuarse tanto en soporte papel como por medios electrónicos. Deberá garantizarse el acceso regular y continuo, así como la permanente actualización de la información.

VIII.6) Protección de los Derechos de los Suscriptores y Usuarios

A los efectos de atender los reclamos presentados por suscriptores y usuarios de servicios de certificación, el INDOTEL dictará una norma complementaria sobre protección de los derechos de los suscriptores y los usuarios.

Los sujetos regulados deben disponer de un operador para responder llamadas telefónicas de los usuarios VEINTICUATRO (24) horas al día, SIETE (7) días de la semana o debe grabar electrónicamente las quejas y llamadas de los usuarios. Se podrá utilizar una combinación de operadores y grabadoras.

En caso de que se utilicen grabadoras la compañía deberá contactar al usuario a más tardar el próximo día laborable luego de la recepción del mensaje grabado. Deberán asimismo prestar el servicio de atención de consultas mediante el acceso por la Internet.

Los sujetos regulados deberán suministrar a los usuarios, a través de una línea telefónica de acceso gratuito o dirección electrónica, dedicada al servicio al cliente, las siguientes informaciones:

a) Número de inscripción en el Registro de Entidades de Certificación.

b) Recibir y aceptar reportes, solicitudes sobre revocación o suspensión de certificados.

c) Tarifas e impuestos aplicables.

d) Fecha de expiración de la autorización, si existe.

e) Consultas u otra información relevante para la utilización del servicio.

VIII.7) Normas de Conducta

Ningún funcionario o empleado del INDOTEL podrá revelar información confidencial obtenida en el ejercicio de sus funciones. La revelación de tales

informaciones será sancionada con el cese de las funciones de dicho empleado, sin perjuicio de otras acciones civiles o penales en su contra.

Esta obligación de confidencialidad se hará extensiva a las entidades auditoras contratadas por el INDOTEL.

Ningún funcionario o empleado del INDOTEL, mientras esté en ejercicio de su cargo, podrá recibir pago alguno por ningún concepto de empresas sujetas a la facultad reglamentaria del INDOTEL. Tampoco podrán tener ninguna relación laboral, participación accionaría u otro vínculo con alguna entidad regulada. Dicha prohibición se extenderá por el período de UN (1) año posterior al abandono del cargo o función.

Se encuentran prohibidos los contactos informales o individuales entre las partes interesadas y el personal del INDOTEL, sobre temas pendientes de resolución. Esas comunicaciones deberán ser formales y accesibles a los interesados o sus representantes en casos de actos de alcance general, ya sea participando en las reuniones o conociendo las presentaciones o actas respectivas, en la forma en que lo reglamente el INDOTEL.

Los funcionarios del INDOTEL estarán sujetos a los principios del Código de Ética del INDOTEL.

VIII.8) Conflicto de Intereses para Entidades Auditoras

Para el cumplimiento de las funciones de entidad de vigilancia y control el INDOTEL podrá contratar expertos, a cuyos contratos se incorporarán las normas de conducta previstas.

No podrán efectuar auditorías las entidades auditoras o las personas que se encuentren directa o indirectamente vinculadas con los sujetos regulados.

VIII.9) Facultades de la Junta Monetaria y de la Superintendencia de Bancos

La Junta Monetaria, en uso de la facultad regulatoria que le confiere la Ley Nº 126-02 y la Ley Nº 183-02 Monetaria y Financiera en materia de operaciones y servicios financieros asociados a los medios de pagos electrónicos que realice el sistema financiero nacional, establecerá los requisitos relativos a las condiciones de uso de los servicios de certificación en dicho sistema.

La Superintendencia de Bancos, en su condición de supervisor del sistema financiero nacional, dictará los instructivos y circulares que considere necesarios con la finalidad de que las entidades de intermediación financiera den fiel cumplimiento a las condiciones establecidas por la Junta Monetaria.

IX- Condiciones para el uso de Firma Digital en Interacciones Documentales entre Entidades del Estado o entre Personas Privadas y Entidades del Estado.

IX.1) Validez de los Documentos Digitales

En las relaciones entre organismos públicos entre sí o entre personas privadas y entes estatales no se negarán efectos jurídicos, validez o fuerza obligatoria a una declaración de voluntad u otra declaración por la sola razón de haberse hecho en forma de documento digital o mensaje de datos.

Los órganos de la administración del Estado Dominicano podrán ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos por medio de firma electrónica o digital, según la naturaleza del acto.

Para tal efecto, los actos administrativos, formalizados por medio de documentos digitales y que consten en decretos o resoluciones, en acuerdos de órganos colegiados, así como la celebración de contratos, la emisión de cualquier otro documento que exprese la voluntad de un órgano del Estado en ejercicio de sus potestades legales y, en general, todo documento que revista la naturaleza de instrumento público o aquellos que deban producir los efectos jurídicos de éstos, deberán suscribirse mediante firma digital.

IX.2) Provisión de certificados para uso del Estado

Los organismos del Estado podrán contratar, de acuerdo con las normas que rigen la contratación administrativa, los servicios de certificación de firma digital con una Entidad de Certificación, cuando mediante resolución fundada constaten su conveniencia técnica y económica. La estimación de dicha conveniencia estará basada en criterios de calidad de servicio y precio.

En caso contrario, podrán constituirse como prestador de servicios de certificación, solicitando al INDOTEL la respectiva autorización para funcionar como Entidad de Certificación.

En aquellas aplicaciones en las que el Estado interactúe con la comunidad, se deberá admitir el uso de Certificados Digitales emitidos por Entidades de Certificación pertenecientes al sector público o al sector privado, indistintamente. No podrán establecerse criterios discriminatorios, en la

medida que se satisfagan todos los requisitos funcionales, legales y reglamentarios.

IX.3) Unidades de Registro pertenecientes al Estado

En las entidades y jurisdicciones pertenecientes a órganos del Estado, las áreas de recursos humanos cumplirán las funciones de Unidad de Registro para los agentes y funcionarios de su jurisdicción. En su caso, y si las aplicaciones de que se trate lo requieren, la máxima autoridad del organismo podrá asignar, adicionalmente, a otra unidad las funciones de Unidad de Registro.

El INDOTEL autorizará el funcionamiento de dichas Unidades de Registro y supervisará su actividad.

IX.4) Presentación de documentos digitales

Los organismos del Estado deberán establecer mecanismos que garanticen la opción de remisión, recepción, mantenimiento y publicación de información en formato digital, siempre que esto sea aplicable, tanto para la gestión de documentos entre organismos como en su interacción con los ciudadanos, tales como ventanilla única electrónica, disponibilidad de una dirección de correo electrónico o un formulario en la página de Internet para la atención de consultas, medios de entradas electrónica, contrataciones públicas electrónicas, seguimiento de expedientes por la Internet, y otras aplicaciones que permitan la consulta de información, la remisión de documentación y el seguimiento de los trámites por la Internet

IX.5) Archivo de Documentos Digitales (Repositorios)

Los órganos de la Administración del Estado que utilicen documentos digitales deberán contar con un Repositorio o Archivo electrónico a los efectos de su guarda y conservación una vez que haya finalizado su tramitación, de conformidad con las normas que regulan su competencia.

El Repositorio será responsabilidad del respectivo funcionario a cargo del archivo, sin perjuicio de la celebración de convenios de cooperación entre diferentes organismos para la guarda y conservación de documentos digitales.

El Repositorio deberá contar con una autorización para operar dispuesta por el INDOTEL.

IX.6) Requisitos mínimos para Archivo de Documentos Digitales

El Repositorio deberá garantizar la seguridad, integridad y disponibilidad de la información contenida en él.

El INDOTEL fijará las normas técnicas referidas a copias de resguardo, medidas de seguridad física y lógicas que garanticen la confidencialidad, integridad y disponibilidad de la información, y las medidas de protección de la privacidad de los datos personales.

IX.7) Comunicaciones electrónicas

Los órganos de la Administración del Estado podrán relacionarse por medios electrónicos con los particulares, utilizando mensajes de datos o documentos digitales, cuando éstos hayan consentido expresamente en esta forma de comunicación.

IX.8) Fijación de la hora oficial electrónica

El INDOTEL analizará las alternativas y regulaciones necesarias para la fijación de día y hora oficial en los medios electrónicos, así como el diseño de los mecanismos de distribución de la hora oficial en Internet, a fin de que tanto los organismos públicos como las Entidades de Certificación procedan a tomar de allí la hora como insumo para su registro y distribución posterior, y para el suministro del servicio de registro y estampado cronológico.

Esta hora oficial en medios electrónicos e Internet será utilizada para la determinación de fecha y hora cierta en la realización de actos para los cuales la determinación fehaciente de la hora constituye un elemento esencial, tales como la presentación de escritos en formato digital en instancia judicial y administrativa como medio de prueba documental, la realización de compras electrónicas o las notificaciones electrónicas.

El INDOTEL coordinará las acciones con los órganos del Estado responsables de la fijación de la hora oficial a fin de elaborar las normas para la fijación de la hora oficial en medios electrónicos y su distribución por la Internet ,a la cual deberán ajustarse los servidores de los organismos públicos y de los sujetos regulados.

Una vez aprobadas dichas normas, los sujetos regulados por la Ley, los proveedores de servicios de la Internet, los organismos públicos, deberán ajustar sus servidores a la hora oficial electrónica fijada, y la distribuirán de acuerdo con la reglamentación que se dicte.

Las comunicaciones y notificaciones electrónicas deberán contar con estampado cronológico, basado en fecha y hora electrónica ciertas.

X- Valor Probatorio de La Firma Digital

De la evolución del marco jurídico a principios de los años 90 con la difusión masiva de Internet y la necesidad de establecer mecanismos de comunicación seguros sobre redes públicas, inherentemente inseguras, comienzan a utilizarse distintos instrumentos tecnológicos que constituyen lo que se denomina una PKI (Public Key Infrastructure o Infraestructura de Clave Pública).

Luego de establecidas las soluciones tecnológicas, y de puestos en funcionamiento distintos esquemas de infraestructura, aparecen a mediados de los 90 las primeras leyes relacionadas con el reconocimiento jurídico de los documentos digitales y las firmas electrónicas.

Las primeras normas, leyes que marcaron un rumbo en la siguiente generación de instrumentos legales internacionales, fueron las Leyes de los Estados de Utah y California de los Estados Unidos de América y la Ley de Alemania.

En este estadio normativo se buscaba aportar un reconocimiento al valor jurídico de los documentos electrónicos, pero no se pretendía ir más allá del valor necesario para operar un conjunto de aplicaciones específicas. No se encontraba entre los objetivos primarios generar un marco de interoperabilidad entre distintas infraestructuras, dado que aún eran incipientes y muy escasas. Estas primeras normas asociaban el reconocimiento legal del equivalente con la firma manuscrita a la solución tecnológica provista por la criptografía asimétrica. Es así como se observa que las definiciones de firma digital de las normas más antiguas, eran las definiciones de la tecnología aplicable en ese momento, que actualmente perdura.

Bajo este escenario surgen en los años siguientes leyes que establecen distintos modos de reconocimiento del valor legal de la firma electrónica/digital basada en certificados en otros estados de EE.UU., en los países de Italia, Argentina, Colombia, Canadá, Australia y Singapur, entre otros.

Paralelamente al desarrollo netamente normativo, algunos países tuvieron un amplio impulso en la implementación de infraestructuras a nivel de las Administraciones Públicas, como por ejemplo el gobierno de Canadá, a través de su "Government of Canada Public Key Infrastructure"; las iniciativas de Australia con la iniciativa "Gatekeeper"; etc. La República Argentina cuenta ya en 1998 con una Infraestructura de Firma Digital para el Sector Público Nacional.

En todas estas infraestructuras siempre existe la figura de un órgano responsable de acreditar o habilitar el funcionamiento de aquellas Autoridades Certificantes o Entidades de Certificación, que cumplen con las normas técnicas y los procedimientos de certificación que se encuentran correctamente implementados bajo la normativa establecida.

Estos esquemas de reconocimiento varían desde la mera mención de aquellos certificadores que se encuentran acreditados a operar dentro del marco normativo, hasta infraestructuras tecnológicas complejas en las cuales se define una jerarquía de confianza estructurada a partir de un certificado raíz único para todo el esquema y ámbito de aplicación. Así, por ejemplo, el Estado de Utah definía un procedimiento de acreditación, lo mismo que el Estado de California y otros estados de EEUU, que desde el punto de vista de implementación se remitía simplemente al control de determinadas características técnicas y a la publicación es su sitio web de cuáles eras las Autoridades Certificantes que estaban acreditadas en el marco de la ley.

Por otra parte, países como Canadá, Singapur y Argentina establecían un sistema de acreditación consistente en la creación, a nivel del órgano acreditador, de una Autoridad Certificante capaz de emitir los certificados de aquellas Autoridades Certificantes habilitadas en el marco de su normativa.

Este esquema de acreditación se conoce como Autoridad Certificante Raíz (AC Raíz): el organismo público competente en la materia, licencia a las prestadoras de servicios de certificación mediante la emisión de su certificado digital, unificando en un solo acto la emisión de la licencia con la emisión del certificado. Este esquema es actualmente compartido por la ICP (Infraestrutura de llaves públicas) de Brasil, entre otros países.

Pueden citarse otras normas internacionales que establecen esquemas de licenciamiento bajo la forma de AC Raíz, en los cuales el procedimiento de acreditación de entidades certificadoras se realiza mediante la emisión de su certificado digital por parte del órgano de contralor (AC Raíz).

A lo largo de los años, en EEUU proliferan iniciativas a nivel estadual o de manera casuística para trámites personales, contemplados en sendas normas que regulan el uso de firmas electrónicas, hasta que en el año 2000 surge la E-SIGN (Electronic Signature in Global and National Commerce Act), ley de alcance federal, que establece parámetros en común acerca del reconocimiento jurídico de la firma electrónica.

Esta ley, de características amplias, no especifica los procedimientos que se deben cumplir para quedar abarcada dentro de su espectro.

En nuestro país la ley 126-02 le a dado valor jurídico a las Firmas Digitales. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo

tipo de información por la sola razón de que esté en forma de documento digital o mensaje de datos.

Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, se entenderá satisfecho dicho requerimiento en relación con un documento digital o un mensaje de datos, si éste ha sido firmado digitalmente y la firma digital cumple con los requisitos de validez establecidos en la ley.

Los documentos digitales y mensajes de datos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los actos bajo firma privada en el Código Civil y en el Código de Procedimiento Civil.

En las actuaciones administrativas o judiciales no se negará eficacia, validez o fuerza obligatoria y probatoria a ningún tipo de información en forma de documento digital o mensaje de datos, por el solo hecho de que se trate de un documento digital o un mensaje de datos o en razón de no haber sido presentado en su forma original.

Al valorar la fuerza probatoria de un documento digital o mensaje de datos se tendrá presente la confiabilidad de la forma en la que se haya generado, archivado o comunicado el documento digital o mensaje, la confiabilidad de la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su creador o iniciador y cualquier otro factor pertinente.

En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un documento digital, un mensaje de datos, o un mensaje de datos portador de un documento digital, como fuere el caso. No se negará validez o fuerza obligatoria a un

contrato por la sola razón de haberse utilizado en su formación uno o más documentos digitales o mensajes de datos. En las relaciones entre el iniciador y el destinatario de un mensaje de datos, o entre las partes firmantes de un documento digital, cuando las hubiere, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de documento digital o mensaje de datos.

Entonces la pregunta seria: ¿Cómo firmo un contrato electrónicamente?

La firma digital es la tecnología más frecuente para firmar electrónicamente. Permite que los receptores identifiquen a los firmantes con la intervención de una tercera parte fiable, conocida como autoridad certificadora (AC).

La AC crea un certificado de identificación digital que establece un vínculo entre la persona firmante y su par de claves ("privada" y "pública), de manera que ésta no puede desconocer su firma después.

La "firma" consiste en un mensaje cifrado del tipo que normalmente se usa en las firmas "reales", que se adjunta al mensaje principal. La intervención de una tercera parte es indispensable para establecer la fiabilidad y la seguridad en los intercambios electrónicos, puesto que las partes contratantes nunca se presentan en persona a firmar sus contratos.

Conclusión I

La investigación y estudios de aplicación de la ley de comercio electrónico nos arroja luz en un área del derecho en nuestro país que todavía podríamos decir esta en pañales, como todos sabemos el comercio en nuestro país es amplio pero con la nueva tecnología y los avances de la misma se ha visto que el comercio ha tenido que adaptarse a los tiempos modernos, la ley de comercio electrónico en el país como hemos visto en esta investigación esta avanzada a nuestra actualidad comercial en el área de las tecnologías, existen muchas figuras que están comprendida en la misma que no se aplican o son de muy poca aplicación, una de esas figuras que están en comprendida en la ley son las firmas digitales, en la actualidad en nuestro país es inexistente , nos preguntaríamos ¿cual es la razón ? y nos hemos dado cuenta durante toda la investigación que la ley contiene figuras avanzadas a la actualidad comercial del país pero su razón lógica tiene porque si hablamos de comercio internacional no podemos estar rezagados enguanto a ley se refiere, por lo tanto aunque en la actualidad lo veamos como algo del futuro ese futuro no se encuentra lejos.

Conclusión II

Esta exhaustiva investigación del derecho y del comercio hacia la expansión de la informática o del comercio electrónico en nuestro país ha surgido la actual ley que abarca una serie de figuras desconocidas para el comercio podríamos decir que la aplicación de la ley se encuentra en panales como a sido mencionado a lo largo de la investigación mas que un mal es beneficiosos para nuestra actualidad comercial una ley con miras futuristas por que insta al comercio a expandirse y formar parte de la revolución informática. En la podemos encontrar una serie de figuras desconocidas para las relaciones comerciales en el país pero de una importancia significativa como lo son las firmas digitales los contratos electrónicos y estos como figuras individualizadas dentro de la ley.

Recomendación

Toda Compañía, asociación, sociedad, industria, es decir toda entidad que se dedica al comercio y mas si utilizan los servicios electrónicos y en especifico la entidades bancarias que son los pioneros en el uso electrónico y digital en sus operaciones y transacciones deben incorporar , utilizar las firmas Digitales. Ya sea teniendo su propia firma digital y dotando al usuario de una, sea con aporte económico de la entidad comerciante, del usuario o de ambas.

Pero como dice la frase "No se puede caminar, sin primero gatear", antes de esto necesitamos de entidades de certificación de firmas digitales, que durante la presentación hemos desarrollado. Todavía en Republica Dominicana no tienes. Las compañías privadas no han encontrado la forma de canalizar en el mercado dominicano la obtención de beneficios con una entidad de certificación.

Somos de opinión que el Estado tiene que motivar, crear una entidad de certificación o incluirla dentro de la funciones del Instituto Dominicano de telecomunicaciones (INDOTEL)para incentivar a los comerciantes y la población dominicana o como en otros países de Latinoamérica que el gobierno fue que estableció entidades de certificación como es el caso de Argentina.

Bibliografía

Cruz Campillo, José "La Firma Digital"

Diario Libre, sección Tecnología y Telecomunicación del nueve (9)de septiembre del dos mil cuatro(2004).

Decreto No. 335-03.Reglamento General de Aplicación de la ley No. 126-02 sobre Comercio Electrónico Documentos y firmas Digitales.

Gaceta Judicial del doce (12) al veintiséis (26) de Agosto del año mil novecientos noventa y nueve (1999) "Derecho en la red, el nuevo régimen virtual".

Gaceta Judicial del cinco (5) al diecinueve (19) de Abril del año dos mil uno (2001) "Seguridad y comercio electrónico".

Gaceta Judicial del veinticinco (25) de Abril al nueve (9) de Mayo del año dos mil tres (2203) "reglamento de la ley de comercio electrónico y exposición de motivos".

Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales

Normas complementarias a la ley No. 126-02 sobre Comercio Electrónico Documentos y firmas Digitales. Sobre estándares tecnológicos.

Normas complementarias a la ley No. 126-02 sobre Comercio Electrónico Documentos y firmas Digitales. Sobre política y procedimiento de certificación.

Normas complementarias a la ley No. 126-02 sobre Comercio Electrónico Documentos y firmas Digitales. Sobre criterios de auditoria de servicio de certificación.

Normas complementarias a la ley No. 126-02 sobre Comercio Electrónico Documentos y firmas Digitales. Sobre procedimiento de autorización y acreditación de los sujetos reguladores por el INDOTEL.

Normas complementarias a la ley No. 126-02 sobre Comercio Electrónico Documentos y firmas Digitales. Sobre procedimiento de seguridad.

Resolución No. 042-03 que aprueba el Reglamento de Aplicación de la ley No. 126-02 sobre Comercio Electrónico Documentos y firmas Digitales

ANEXO

ANEXO

Entrevista a ejecutivos de Indotel

Entrevista I:

A: José Delio Ares Guzmán (Director Ejecutivo)

Buenas tardes. **¿Como se encuentra?**
Muy bien gracias. **¿y ustedes?**
Muy bien!!!

¿Cuales son las funciones del Indotel?

Es la institución reguladora de las telecomunicaciones en el país. Pero todavía en la actualidad no desempeñamos todas las funciones a la que estamos capacitados.

¿A que se debe esto?

Indotel es una institución adelantada a la situación actual de el país en cuanto a las telecomunicaciones podemos decir que Indotel vive en el futuro y el país no ha llegado todavía hay pero lo hará pronto eso esperamos.

¿La actual ley de telecomunicaciones es eficiente?

Es mas que eficiente prevé y abarca una serie de ámbitos inimaginables para la actualidad del país, lo que sucede es que no hay aplicación de la misma ya que como habíamos dicho en el futuro.

¿ El comercio electrónico en el país esta regulado por la ley y por el Indotel?

Claro que si, toda relación comercial o acuerdo que tenga que ver con documentos digitales es comercio electrónico por tanto regulado por la ley No. 126-02 y regulado por el Indotel.

Quiero dejar algo claro Indotel es un regulador es como arbitro, no es la cabeza ni el que gobierna las telecomunicaciones solo nos encargamos de asegurar y garantizar que se cumpla con los acuerdos y se aplique de manera correcta.

¿Qué es una firma digital?

Es un valor numérico que permita identificar un documento específico y que garantiza que ni ha sido alterado antes de llegar a su destino.

¿Se usan las firmas digitales en el país?

Realmente no, las instituciones que necesitan del uso de las firmas digitales en el país no lo han solicitado pero esperamos que pronto empecemos a ver las firmas digitales como algo primordial par los asuntos comerciales.

¿O sea que no hay ejemplo de firmas digitales nos puedan dar?

Bueno de una manera u otra con las tarjetas de crédito y algunos asuntos bancarios podemos decir que ocurre algo que pudiéramos relacionar con las firmas digitales pero no del todo.

Entrevista II:

A las: Lic. Maria Teresa Puigbo (Encargada de Regulación Gerencia Comercio Electrónico, Documentos y Firmas digitales) y a la Ing. Carmen Leda Tejada Cano (Encargada de Auditoria de Firmas Digitales Gerencia Comercio Electrónico, Documentos y Firmas Digitales).

Indotel es una institución encargada de regular todos los asuntos de telecomunicaciones del país y de las firmas digitales y el comercio electrónico.

Pero lamentablemente en el país todavía es una figura nueva, no hay instituciones inscrita el Indotel en relación a esta área.

Han venido jóvenes de otras universidades ha investigar sobre asuntos parecidos haciendo preguntas con relación a las telecomunicaciones pero ustedes son los primeros que preguntan en cuanto a las firmas digitales y el comercio electrónico.

¿Cómo se ve o representa una Firma Digital?

A la vista, una firma digital se representa por una extensa e indescifrable cadena de caracteres, esta cadena representa en realidad un número el cual es el resultado de un procedimiento matemático aplicado al documento.

¿Cuál es la diferencia entre una firma digital y una firma electrónica?

La diferencia entre estas dos radica en que a la firma electrónica carece de alguno de los requisitos legales para ser considerad firma digital como lo son su certificación y autorización en el caso de Republica Dominica del Indotel. Lo cual hace que la firma electrónica no tenga el valor jurídico y probatorio que le confiere la ley No. 126-02 a la firma digital.

Sustentante

Sustentante

Asesor

Presidente del Jurado

Miembro

Miembro

Decano

Calificación: A

Fecha: 18/01/2005