ARTÍCULO 2.- El presente Decreto entrará en vigencia a partir del día de su publicación en el Diario La Gaceta.

Dado en la ciudad de Tegucigalpa, municipio del Distrito Central, en el Salón de Sesiones del Congreso Nacional, a los veinte días del mes de enero de dos mil catorce.

MAURICIO OLIVA HERRERA
PRESIDENTE, POR LA LEY

GLADIS AURORA LÓPEZ CALDERÓN
SECRETARIA

ÁNGEL DARÍO BANEGAS LEIVA
SECRETARIO

Líbrese al Poder Ejecutivo en fecha 26 de febrero de 2014

Por Tanto: Ejecútese.

Tegucigalpa, M.D.C., 07 de marzo 2014.

JUAN ORLANDO HERNÁNDEZ ALVARADO
PRESIDENTE DE LA REPÚBLICA

EL SECRETARIO DE ESTADO EN LOS DESPACHOS DE RECURSOS NATURALES Y AMBIENTE.

JOSÉ ANTONIO GALDÁMEZ

Poder Ejecutivo

ACUERDO EJECUTIVO NUMERO 41-2014

REGLAMENTO DE LA LEY SOBRE FIRMAS ELECTRÓNICAS

EL PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA,

CONSIDERANDO: Que con fecha treinta de julio del 2013, el Congreso Nacional de la República aprobó la Ley Sobre Firmas Electrónicas mediante Decreto número 149-2013, el que fue publicado en el Diario Oficial "La Gaceta" número 33,301 el once de diciembre del 2013.

CONSIDERANDO: Que dicha ley regula la utilización de la firmas electrónicas otorgándoles la misma validez y eficacia jurídica que la firma manuscrita u otra análoga, estableciendo el proceder o los deberes del firmante o suscriptor; las características, requerimientos actividades y deberes generales de la Autoridad Certificadora y, las funciones y atribuciones de la Autoridad Acreditadora, siendo esta última la Autoridad Administrativa Competente (AAC) encargada de organizar y regular de manera más específica esta materia.

CONSIDERANDO: Que el Artículo 29 de la precitada ley establece, que la Dirección General de Propiedad Intelectual (DIGEPIH) contará con un término de tres (3) meses, contados

a partir de la publicación de la misma ley para organizar la función de inspección, control y vigilancia de las actividades realizadas por la Autoridades Certificadoras y para emitir el reglamento respectivo.

CONSIDERANDO: Que es imperativo la emisión de la reglamentación correspondiente que permita desarrollar, ampliar, esclarecer y complementar los principios, preceptos y objetivos establecidos en la "Ley Sobre Firmas Electrónicas", al igual que establecer los mecanismos y procedimientos que habrán de seguirse para lograr su plena aplicación y cumplimiento.

POR TANTO

En uso de las facultades de que está investido el Presidente de la República y en aplicación de los artículos: 245, numeral 1 y 11, 248 de la Constitución de la República; 116, 118 numeral 2 y 119 numeral 2 de la Ley General de la Administración Pública; 41 y 42 de la Ley de Procedimiento Administrativo; 1, 24 y 29 de la Ley de Firmas Electrónicas.

A C U E R D A:

PRIMERO: Aprobar el siguiente:

"REGLAMENTO DE LA LEY SOBRE FIRMAS ELECTRÓNICAS"

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto y Ámbito de Aplicación.

El presente Reglamento regula la emisión y uso de las firmas electrónicas en mensajes de datos y documentos electrónicos, generadas bajo la "Infraestructura Oficial de la Firma Electrónica", comprendiendo las funciones y atribuciones de la Autoridad Administrativa Competente o Autoridad Acreditadora (AAC), el régimen de acreditación y supervisión de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC); así como la emisión y uso de la firma electrónica por parte de las instituciones de la Administración Pública, los organismos de derecho privado, las personas jurídicas de derecho privado y las personas jurídicas y naturales; establece además, los mecanismos y procedimientos necesarios para el registro, confidencialidad, seguridad, y para lograr la plena aplicación y cumplimiento de la Ley Sobre Firmas Electrónicas.

Artículo 2. Definiciones.

Para la aplicación de este reglamento y bajo la perspectiva de la tecnología de información y sin perjuicio de lo dispuesto en la Ley de Firmas Electrónicas, debe entenderse por:

a. **Autoridad Acreditadora o Autoridad Administrativa Competente (AAC):** Es La Dirección General de Propiedad Intelectual (DIGEPIH) y la Autoridad Acreditadora o Autoridad Administrativa Competente (AAC) de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).
b. **Autoridad Certificadora o Prestador de Servicios de Certificación (PSC):** Es la persona natural o jurídica, nacional o extranjera responsable de emitir y revocar los certificados o prestar otros servicios en relación con la firma electrónica.
c. **Autoridad de Registro:** Es el órgano designado por la Autoridad Administrativa Competente (AAC) para realizar recepción de solicitudes, validación de información y aprobación de emisión de los Certificados Electrónicos.
d. **Autorización:** Es un acto realizado por una autoridad, a través del cual se permite a un sujeto una cierta actuación que, en otro caso, estaría prohibida.
e. **Certificado:** Es el documento firmado que vincula datos para la verificación de una firma con un firmante y que confirma la identidad del emisor. Es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de internet.
f. **Certificado de Autorización**: Es el documento escrito a través del cual la Autoridad Administrativa Competente (AAC), habilita a una Prestadora de Servicio de Certificación (PSC) a prestar los servicios solicitados, después de haber cumplido las disposiciones establecidas por la Ley y el presente Reglamento.
g. **Certificado Electrónico:** Es el documento digital extendido por la Autoridad Acreditadora o Prestador de Servicios de Certificación (PSC) que da fe y garantiza la vinculación entre la identidad de los usuarios con su Firma Electrónica Avanzada.
h. **Certificación Cruzada**: Acto por el cual una certificadora autorizada (PSC-Acreditadora) reconoce la validez de un certificado emitido por otra, sea nacional o extranjera, asumiendo tal certificado con todas las responsabilidades como si fuera de su propia emisión.
i. **Cifrado:** Es el proceso de convertir un texto plano (o en claro) a un texto ilegible, denominado texto cifrado o criptograma.
j. **Clave Comprometida:** Es la contraseña que el usuario emplea de forma constante para diferentes transacciones,

donde ha sido comprometida en casos en que (aun cuando no se tenga la certeza) se supone que dicha clave es conocida por otra persona que no es el propietario de la misma.

k. **Clave Privada o Clave Secreta:** Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la Firma Electrónica.

l. **Clave Pública:** Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un mensaje de datos para verificar la Firma Electrónica puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.

m. **Criptografía:** Es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio confidencial de mensajes de manera segura y que únicamente puedan ser leídos por las personas a quienes van dirigidos.

n. **Firma Electrónica:** Es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

o. **Firma Electrónica Avanzada:** Firma Electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y al mensaje de datos a que se refiere, que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control, basada en un Certificado Electrónico emitido por un Prestador de Servicios de Certificación (PSC) y generada mediante un dispositivo seguro de creación de Firmas Electrónicas.

p. **Infraestructura Oficial de la Firma Electrónica:** Sistema confiable, acreditado, regulado, y supervisado por la Autoridad Administrativa Competente (AAC) constituido por programas, equipos, bases de datos, redes, estándares tecnológicos, políticas, procesos, procedimientos u otros recursos que permiten la generación de Firmas Electrónica y que garantizan la autenticación e integridad de los documentos electrónicos.

q. **Ley:** Decreto No. 149-2013 Ley Sobre Firmas Electrónicas.

r. **Mensaje de Datos:** Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.

s. **Reglamento:** El presente Reglamento de la Ley Sobre Firmas Electrónicas.

Artículo 3. De la validez y eficacia de la Firma Electrónica.

La Firma Electrónica generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un documento electrónico si se utiliza una Firma Electrónica generada en el marco de la Infraestructura Oficial de la Firma Electrónica.

Lo establecido en el presente artículo y las demás disposiciones del presente Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

Artículo 4. De La Autoridad Administrativa Competente (AAC).

La Dirección General de Propiedad Intelectual (DIGEPIH) es la Autoridad Administrativa Competente (AAC) y legalmente facultada para actuar como Autoridad Acreditadora, es decir; para conceder autorización a las Autoridades Certificadoras a operar en el territorio Nacional; para emitir la reglamentación correspondiente; diseñar y desarrollar la Infraestructura Oficial de la Firma Electrónica; organizar la función de inspección, control y vigilancia de las actividades realizadas por las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) e imponer las sanciones que correspondan de conformidad con la ley y su Reglamento

Artículo 5. De la Estructura Orgánica del Operador de la Firma Electrónica

La Dirección General de Propiedad Intelectual (DIGEPIH) como operador de la Ley Sobre Firmas Electrónicas podrá también crear el órgano o unidad/es de apoyo que considere necesarias para desarrollar todas las actividades conducentes a lograr el cumplimiento de las disposiciones de la Ley Sobre Firmas Electrónicas y su Reglamento, y consecuentemente podrá nombrar el personal necesario para el cumplimiento de sus funciones y atribuciones.

Artículo 6. Tecnologías de la Infraestructura Oficial de la Firma Electrónica.

La Infraestructura Oficial de Firma Electrónica se puede basar en las tecnologías de firmas electrónicas siguientes:

a. Tecnologías de Firmas Electrónicas, sobre la cual se basa la Infraestructura Oficial de Firma Electrónica.

b. Otras Tecnologías de Firmas Electrónicas, que sean aprobadas por la Autoridad Administrativa Competente (AAC) de acuerdo con el Principio de Neutralidad Tecnológica.

Artículo 7. Elementos de la Infraestructura Oficial de la Firma Electrónica.

La Infraestructura Oficial de la Firma Electrónica está constituida por:

a. **Personal Competente** para la conducción de los procedimientos de certificación y el mantenimiento de la Infraestructura Oficial de Firma Electrónica.
b. **Procedimientos de Certificación** basados en estándares internacionales o compatibles a los empleados, de acuerdo con lo establecido por la Autoridad Administrativa Competente (AAC).
c. **El Soporte Lógico** o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados a los procedimientos de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b de este artículo.
d. **Sistema de Gestión** que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no discriminación en la prestación de sus servicios.

CAPÍTULO II
VALIDEZ JURÍDICA DE LAS FIRMAS Y DOCUMENTOS ELECTRÓNICOS

Artículo 8. Reconocimiento de la Equivalencia Funcional.

Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico, cualquiera sea su medio de transmisión o de almacenamiento, tendrá la misma validez que aquellos que fueren suscritos mediante el uso de papel y firma autógrafa, siempre y cuando en los mismos se utilice la firma electrónica avanzada.

Artículo 9. Características de la Firma Electrónica Avanzada.

Las características mínimas de la Firma Electrónica Avanzada son las siguientes:

a. Es basada en un certificado electrónico emitido por un Prestador de Servicios de Certificación;
b. Es exclusiva del titular de la firma electrónica y de cada mensaje de datos firmado por éste;
c. Tanto la firma como el mensaje firmado son cifrados, utilizando mecanismos sólidos de criptografía;
d. Es añadida o asociada lógicamente al mensaje de datos de tal manera que es posible detectar si la Firma Electrónica o el mensaje de datos fue alterado;
e. Se genera bajo el control exclusivo del titular de la Firma Electrónica;
f. Es susceptible de ser verificada;
g. Es generada mediante un dispositivo confidencial y seguro de creación de Firma Electrónica; y,
h. Es basada en metodología específica, empleada para crear y verificar la Firma Electrónica del suscriptor impuesta en el mensaje de datos.

Artículo 10. Garantías de la Firma Electrónica.

Dadas las características señaladas en el artículo anterior, técnicamente la Firma Electrónica Avanzada debe garantizar las condiciones siguientes:

a. **Autenticidad**: Identifica al usuario emisor del mensaje y al titular de la Firma Electrónica.
b. **Integridad**: Garantía de que el mensaje de datos no ha sido alterado después que el remitente lo envió.
c. **No Repudio**: Como consecuencia de los dos literales anteriores, el titular de la Firma Electrónica no puede repudiar o desconocer un mensaje de datos que ha sido firmado electrónicamente, dado que ésta se mantiene bajo su control exclusivo; salvo que demuestre ante autoridad competente, que fue utilizada sin su autorización por terceras personas.

Artículo 11. Conservación de Mensajes de Datos o Documentos Electrónicos.

Cuando los documentos, registros o informaciones requieran de una formalidad adicional para la conservación de mensajes de datos o documentos firmados electrónicamente, éstos deberán cumplir con lo siguiente:

a. Accesibilidad para su posterior consulta;
b. Conservación de su formato original de generación, envío, recepción u otro que reproduzca en forma demostrable la exactitud e integridad del contenido electrónico; y,
c. Conservación de todo dato que permita determinar el origen, destino, fecha y hora de envío y recepción.

CAPÍTULO III
CERTIFICADOS ELECTRÓNICOS

Artículo 12. Los Certificados Electrónicos.

Son Certificados Electrónicos los expedidos por una Autoridad Certificadora o Prestador de Servicios de Certificación (PSC)

que cumpla los requisitos establecidos en la Ley y el presente Reglamento, y dentro de la Infraestructura Oficial de la Firma Electrónica, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

Artículo 13. Contenido de los Certificados Electrónicos. Además de los requisitos señalados en la Ley, los Certificados Electrónicos incluirán, al menos, los datos siguientes:

a. La indicación de que se expiden como tales;
b. El código identificativo único del Certificado;
c. La identificación del prestador de servicios de certificación que expide el Certificado y su domicilio;
d. La Firma Electrónica de la Autoridad Certificadora o Prestadora de Servicios de Certificación (PSC) que expide el Certificado;
e. La identificación del firmante, en el supuesto de personas naturales, por su nombre y apellidos y su número de identidad y, en el supuesto de personas jurídicas, por su denominación o razón social y el Registro Tributario Nacional (RTN);
f Los datos de verificación de firma (Clave Pública) que correspondan a los datos de creación de firma (Clave Privada) que se encuentren bajo el control del firmante;
g. El comienzo y el fin del período de validez, suspensión y renovación del certificado;
h. Los límites de uso del certificado, si se establecen; y,
i. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Los Certificados Electrónicos podrán asimismo, contener cualquier otro atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

Artículo 14. Obligaciones Previas a la Expedición de Certificados Electrónicos. Antes de la expedición de un certificado electrónico, la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) deberán cumplir las obligaciones siguientes:

a. Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el Artículo 16 de este reglamento;
b. Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido;
c. Asegurarse de que el firmante está en posesión de los datos de creación de la firma correspondiente, a los de verificación que constan en el certificado; y,
d. Garantizar la complementariedad de los datos de creación y verificación de la firma.

Artículo 15. Requisitos Complementarios y otras circunstancias personales de los solicitantes de Certificados Electrónicos, estos son:

a. La identificación de la persona natural que solicite un Certificado Electrónico, exigirá su comparecencia ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la comparecencia si su firma en la solicitud de expedición de un Certificado Electrónico ha sido legitimada en presencia notarial;
b. En el caso de Certificados Electrónicos de personas jurídicas, las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) y/o Autoridades de Registro o Autoridad Administrativa Competente (AAC) comprobarán, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante, mediante la presentación de copias fotostáticas autenticadas en que constan dichos documentos y certificados originales extendidos por el Registro Mercantil en el que estén inscritos los documentos de constitución y de apoderamiento;
c. Cuando el Certificado Electrónico contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica; y,
d. Los Prestadores de Servicios de Certificación (PSC), podrán realizar las actuaciones de comprobación previstas en este artículo por sí o por medio de otras personas naturales o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación.

Artículo 16. Pueden Solicitar Certificados Electrónicos u Otros Documentos Podrán solicitar certificados electrónicos u otros documentos relacionados:

a. Las Personas Naturales titulares de una firma electrónica, su Representante o Apoderado Legal;
b. Por las Personas Jurídicas, sus administradores, representantes legales o representantes voluntarios con poder bastante a estos efectos; y,

c. Las Autoridades Administrativas y Judiciales competentes.

Artículo 17. Vigencia de Certificados Electrónicos. La Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) y el Firmante, de mutuo acuerdo determinarán la vigencia del certificado reconocido. No obstante lo anterior, este período no podrá ser superior a cinco (5) años.

Artículo 18. Revocación de Certificados Electrónicos. El suscriptor de una Firma Electrónica Certificada, podrá solicitar a la Autoridad Certificadora (PSC) que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los eventos siguientes:

a. Por pérdida de la clave privada; y,
b. Exposición de la clave privada y peligro de uso indebido.

Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe, que confiaron en el contenido del certificado.

Una Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) revocará un certificado emitido por las razones siguientes:

a. A petición del suscriptor o un tercero en su nombre y representación;
b. Por muerte del suscriptor;
c. Por liquidación del suscriptor en el caso de las personas jurídicas;
d. Por la confirmación de que alguna información o hecho contenido en el certificado es falso;
e. La clave privada de la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado;
f. Por el cese de actividades de la Autoridad;
g. Por orden judicial o de Autoridad Administrativa competente;
h. Por declaración de insolvencia, siempre que en el plazo fijado por ley, no se levante dicho estado; y,
i. Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

Artículo 19. Disposiciones relativas a la Revocación de Certificados Electrónicos.

a. La Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) hará constar inmediatamente, de manera clara e indubitada, la revocación de la vigencia de los certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la revocación de su vigencia;
b. La Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) informará al firmante acerca de esta circunstancia de manera previa o simultánea a la revocación de la vigencia del certificado electrónico, especificando los motivos, la fecha y la hora en que el certificado quedará sin efecto;
c. La revocación de la vigencia de un Certificado Electrónico no tendrá efectos retroactivos; y,
d. La revocación de la vigencia de un Certificado Electrónico se mantendrá accesible en el servicio de consulta sobre la vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

Artículo 20. Certificados Electrónicos Extranjeros. Toda Firma Electrónica creada o utilizada fuera de la República de Honduras producirá los mismos efectos jurídicos que una firma creada o utilizada en Honduras, si presenta un grado de fiabilidad equivalente.

Los Certificados de Firmas Electrónicas emitidos por autoridades o Entidades de Certificación extranjeras, producirán los mismos efectos jurídicos que un certificado expedido por Autoridades Certificadoras Nacionales, siempre y cuando tales certificados presenten un grado de fiabilidad en cuanto a la regularidad de los detalles del mismo, así como su validez y vigencia.

A efectos de determinar si un Certificado de Firmas Electrónicas o una Firma Electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de los párrafos anteriores, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente; ya que lo que se pretende es contrastar su fiabilidad con los requisitos establecidos en el Artículo 8 de la "Ley Sobre Firmas Electrónicas" y este Reglamento. Considerando que el grado de fiabilidad de un certificado extranjero no debe ser exactamente idéntico al grado de fiabilidad de un certificado nacional.

Sin perjuicio de lo dispuesto en los párrafos anteriores, las partes pueden acordar la utilización de determinados tipos de Firma Electrónicas o Certificados. Ese acuerdo será suficiente a

los efectos del reconocimiento transfronterizo, siempre que el mismo sea válido, y eficaz de conformidad con la Ley.

Tanto las Firmas Electrónicas como los Certificados Electrónicos extranjeros, serán en todo caso válidos, siempre que exista convenio de reciprocidad entre Honduras y el país de origen del firmante o autoridad certificadora; sin que esas firmas o esos certificados se sometan al criterio de la equivalencia sustancial expresado en los párrafos anteriores.

CAPÍTULO IV
SISTEMAS DE FIRMA ELECTRÓNICA AVANZADA

Artículo 21. Sistema Seguro de Creación de Firma Electrónica Avanzada.

Un sistema seguro de creación de Firma Electrónica es un programa o dispositivo informático que sirve para aplicar los datos de creación de firma, ofreciendo, al menos las siguientes garantías:

a. Que los datos utilizados para la generación de una Firma Electrónica pueden producirse sólo una vez y asegura razonablemente su secreto;
b. Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la Firma Electrónica está protegida contra la falsificación con la tecnología existente en cada momento;
c. Que los datos de creación de Firma Electrónica pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros; y,
d. Que el sistema utilizado no altere los datos del documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Artículo 22. Sistema Seguro de Verificación de Firma Electrónica Avanzada.

Un Sistema Seguro de Verificación de Firma Electrónica Avanzada, son los dispositivos informáticos para la identificación y autenticación del ejercicio de la competencia en la actuación administrativa automatizada y que garantizará el proceso de verificación de las firmas registradas, bajo el cumplimiento al menos de los requisitos siguientes:

a. Que los datos utilizados para verificar la Firma Electrónica Avanzada correspondan a los datos mostrados a la persona que verifica la firma;
b. Que la Firma Electrónica Avanzada se verifique de forma fiable y el resultado de esa verificación se presente correctamente;
c. Que la persona que verifica la Firma Electrónica Avanzada pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados;
d. Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación;
e. Que se verifiquen de forma fiable la autenticidad y la validez del Certificado Electrónico correspondiente; y
f. Que deba detectarse cualquier cambio relativo a su seguridad.

CAPÍTULO V
AUTORIDADES CERTIFICADORAS O PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)

Artículo 23. Requerimientos de las Autoridades de Certificación o Prestadores de Servicios de Certificación (PSC).

Podrán actuar como Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), las personas naturales, y las personas jurídicas, tanto públicas como privadas, que sean autorizadas por la Autoridad Administrativa Competente (AAC), para operar como tales y que cumplan con los requerimientos establecidos en la Ley, el presente Reglamento, la Infraestructura Oficial de la Firma Electrónica y por la misma Autoridad Administrativa Competente (AAC); y conforme las condiciones siguientes:

a. Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como autoridad certificadora, así como con el recurso humano y la de ontología jurídica, que demanda su condición de tal;
b. Contar con la capacidad y elementos técnicos (equipos y programas informáticos) necesarios para la generación de Firmas Electrónicas, garantizando la autenticidad de las mismas, para la emisión y trámite de certificados, y la conservación de mensajes de datos y consulta de los registros, en los términos establecidos en la Ley y el presente Reglamento; y,
c. Disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste.

Los representantes legales y administrativos no podrán ser personas que hayan sido condenadas a pena privativa de la

libertad, o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética. Esta inhabilidad, estará vigente por el mismo período que la Ley Penal o Administrativa señale para el efecto.

Los Notarios que reúnan las condiciones expresadas, serán automáticamente autorizados para actuar como autoridad certificadora. Lo dispuesto en el párrafo anterior les será en su caso aplicable.

Para verificar que las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) cumplan con los requerimientos antes establecidos y para determinar el grado de fiabilidad de dichos prestadores se tomarán los factores siguientes:

a. Recursos y capacidad financiera para asumir la responsabilidad por el riesgo de pérdida;
b. Garantías y representaciones;
c. Seguros;
d. Descripción detallada de las políticas, procedimientos y mecanismos que el prestador de servicios de certificación se obliga a cumplir;
e. Disponer de personal suficiente de reconocida honorabilidad, el cual deberá ser competente para las funciones que realiza, incluyendo la emisión de opiniones técnicas que se requieran, la formulación de políticas y su implementación;
f. Experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados;
g. Contar con el equipo y los programas informáticos necesarios;
h. Mantenimiento de un registro de auditoría y realización de auditorías por una Autoridad independiente;
i. Existencia de un plan para casos de emergencia (por ejemplo, "programas de recuperación en casos de desastre" o depósitos de claves);
j. Disposiciones para proteger su propia clave privada;
k. Seguridad interna;
l. Disposiciones para suspender las operaciones, incluida la notificación a los usuarios;
m. Declaración de limitación de la responsabilidad; y,
n. Contar con procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado en entredicho).

Artículo 24. Procedimiento de Acreditación de las Autoridades de Certificación o Prestadores de Servicios de Certificación (PSC).

Se iniciará por medio de una solicitud presentada a la Autoridad Administrativa Competente (AAC), acompañada del comprobante de pago de los costos de la acreditación y de los antecedentes que permitan verificar el cumplimiento de lo dispuesto en la Ley y este Reglamento.

En la solicitud que se presente, el interesado deberá especificar su nombre completo, denominación o razón social, su RTN, el nombre completo y RTN del Representante Legal, su domicilio social y dirección de correo electrónico, aceptando expresamente dicho medio electrónico como forma de comunicación. Recibida la solicitud, la Autoridad Administrativa Competente (AAC) procederá a verificar la admisibilidad de la misma mediante la verificación de la información requerida.

Artículo 25. Facultades del Representante del Solicitante.

Las facultades de la persona natural que actúa en representación del solicitante se acreditarán de la manera siguiente:

a. **En el caso de personas jurídicas constituidas en el país**: En el poder o mandato que acredite la representación deberán constar las facultades conferidas al representante, bastando para tales efectos la presentación de la copia autenticada o cotejada del poder respectivo.
b. **En el caso de personas jurídicas constituidas en el extranjero**: Los correspondientes poderes o mandatos, deberán ser apostillados o en su caso, legalizados por un Funcionario Consular de Honduras; y de encontrarse redactados en idioma extranjero, será necesario su traducción al idioma oficial, debiendo el responsable de la traducción suscribir el correspondiente documento.
c. **En el caso de instituciones del Estado**: Deberá acreditarse el acuerdo de nombramiento de la persona encargada de dirigir la oficina, gerencia o dependencia interna encargada de la prestación del servicio de certificación digital. Asimismo se debe acreditar las competencias y facultades de este funcionario.

Artículo 26. De la Admisión, Requerimiento o Rechazo de la Solicitud.

Recibida la solicitud, la Autoridad Administrativa Competente (AAC) procederá a verificar la admisibilidad de la misma mediante la verificación de la información requerida. De no acompañar la solicitud todos los requisitos establecidos en la "Ley Sobre Firmas Electrónicas" y este Reglamento, se notificará al interesado de tal situación dentro de los tres (3) días hábiles siguientes a la recepción de la solicitud, para que proceda a completar la información requerida, dentro del plazo de treinta (30) días hábiles,

bajo apercibimiento de ser rechazada la solicitud mediante simple providencia y se archivará sin más trámite.

Artículo 27. Evaluación de los Requisitos y de la Competencia Técnica.

Admitida la solicitud, la Autoridad Administrativa Competente (AAC) procederá a verificar el cumplimiento de los requisitos, la competencia técnica, y demás requerimientos exigidos por la Ley y este Reglamento para obtener la acreditación, la que deberá ser emitida mediante resolución dentro de un plazo no mayor de noventa (90) días hábiles, contados desde la fecha de notificación.

En caso que no cumpla con los requisitos fijados para el desarrollo de la actividad, señalará si los incumplimientos son subsanables en un término de ciento veinte (120) días hábiles improrrogables para que presente y ejecute un plan de medidas correctivas; en caso que los incumplimientos no sean subsanables, se procederá a dictar una resolución denegando la solicitud de acreditación. Si dentro del término para la ejecución del plan de medidas correctivas, se cumple a satisfacción con el mismo, se emitirá la resolución otorgando la autorización para operar como Autoridad Certificadora o Prestador de Servicios de Certificación (PSC); de no ejecutarlo o no cumplirlo a satisfacción, se emitirá resolución denegatoria.

Artículo 28. Recurso de Reposición y Subsidiaria Apelación.

Contra la resolución definitiva procede el Recurso de Reposición, que deberá interponerse ante la Autoridad Administrativa Competente (AAC), dentro de los diez (10) días siguientes a la última notificación, ésta resolverá dentro de los veinte (20) días hábiles siguientes al auto de admisión de la reposición. La resolución que recaiga es apelable conforme a lo dispuesto en los artículos 21 y 22 de la Ley de Propiedad.

Artículo 29. Reconocimiento de Evaluaciones Técnicas de Terceros o Realizadas en el Extranjero.

La evaluación de los requisitos de competencia técnica de la entidad de certificación solicitante, podrá ser realizada directamente por la Autoridad Administrativa Competente (AAC) o a través de terceros o reconociendo aquellas realizadas en el extranjero por otras autoridades extranjeras que cumplan funciones equivalentes a las de la autoridad administrativa competente, siempre que los requisitos evaluados por ellas sean equivalentes a los requisitos comprendidos en el presente Reglamento.

En todo caso, se podrá reconocer las evaluaciones sobre los requisitos de competencia técnica de la entidad de certificación solicitante realizadas en el extranjero siempre y cuando se cumpla con las normas establecidas por la Autoridad Administrativa Competente (AAC) en el marco del presente Reglamento.

Artículo 30. Costos de la Acreditación y Otros.

Las entidades solicitantes asumirán los costos por el trámite de acreditación, y aquellos otros por la evaluación de la competencia técnica, supervisión, inspecciones, auditorías y demás previstos por la Autoridad Administrativa Competente (AAC).

Cuando la evaluación de la competencia técnica sea realizada por la propia Autoridad Administrativa Competente (AAC), se aplicará, en caso de traslado el reglamento de viáticos y transporte interno de la institución; y cuando sea realizada por terceros, se ejecutará a través de técnicos debidamente acreditados, los que serán seleccionados y calificados por la Autoridad Administrativa Competente (AAC) y todos los costos deberán ser cubiertos por el solicitante.

CAPÍTULO VI
OTRAS DISPOSICIONES RESPECTO DE LAS AUTORIDADES CERTIFICADORAS O PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (PSC)

Artículo 31. Actividades de las Autoridades de Certificación o Prestadores de Servicios de Certificación (PSC).

La Autoridad Certificadora o Prestador de Servicios de Certificación (PSC), autorizados por la Autoridad Administrativa Competente (AAC), podrán realizar, entre otras, las actividades siguientes:

a. Emitir certificados en relación con las Firmas Electrónicas certificadas de personas naturales o jurídicas;
b. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos;
c. Ofrecer o facilitar los servicios de creación de Firmas Electrónicas certificadas;
d. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos; y,
e. Ofrecer los servicios de archivo y conservación de mensajes de datos.

Artículo 32. Declaración de las Prácticas de Certificación.

Es obligación de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) contar con reglas sobre

prácticas de certificación consistentes en una descripción detallada de las políticas, procedimientos y mecanismos que el prestador de servicios de certificación se obliga a cumplir en la prestación de sus servicios de certificación y homologación.

Las Prácticas de Certificación deben declarar el cumplimiento de los requisitos señalados en el Artículo 13 de la Ley Sobre Firmas Electrónicas; y el artículo 23 del presente Reglamento.

Las prácticas de certificación deben ser objetivas y no discriminatorias, y se deben comunicar a los usuarios de manera sencilla y en idioma español. Dichas prácticas deberán contener al menos:

a. Una introducción, que deberá contener un resumen de las prácticas de certificación, mencionando tanto la Autoridad que suscribe el documento, como el tipo de usuarios a los que son aplicables;
b. Consideraciones generales, debiendo contener información sobre obligaciones, responsabilidades, cumplimiento de auditorías, confidencialidad, y derechos de Propiedad Intelectual, con relación a todas las partes involucradas;
c. Identificación y autenticación, debiendo describirse tanto los procesos de autenticación aplicados a los solicitantes de Firma Electrónica Avanzada;
d. Requerimientos operacionales, debiendo contener información operacional para los procesos de trámite de las solicitudes de Firma Electrónica Avanzada, emisión de certificados, revocación de certificados, procesos de control, seguridad, almacenamiento de información relevante, cambio de datos de creación de Firma Electrónica Avanzada, superación de situaciones críticas, contingencias (casos de fuerza mayor o casos fortuitos), y procedimientos de término del servicio de certificación;
e. Administración de los recursos humanos, procesos, procedimientos, materiales, físicos y operativos; debiendo describir los controles de seguridad no técnicos utilizados por la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) para asegurar las funciones de generación de datos de creación de la Firma Electrónica, autenticación de usuarios, emisión de certificados, revocación de certificados, auditoría y almacenamiento de información relevante;
f. Controles de seguridad técnica; debiendo señalar las medidas de seguridad adoptadas por la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) para proteger los datos de creación de su propia Firma Electrónica;
g. Perfiles de certificados y del registro de acceso público, debiendo especificar el formato del certificado y del registro de acceso público; y,
h. Especificaciones de administración de la política de certificación, debiendo señalar la forma en que la misma está contenida en la práctica, los procedimientos para cambiar, publicar y notificar la política.

La declaración de prácticas de certificación de cada Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) deberá estar disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

Artículo 33. Obligaciones de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).

La autoridad certificadora tendrá, entre otros los deberes siguientes:

1. Emitir certificados conforme a lo solicitado o acordado con el suscriptor;
2. Adoptar las medidas razonables para determinar con exactitud la identidad del titular de la firma y de cualquier otro hecho y acto que certifique;
3. Implementar los sistemas de seguridad para garantizar la emisión y creación de Firmas Electrónicas, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;
4. Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;
5. Garantizar que todas las declaraciones y manifestaciones materiales, sean exactas y completas;
6. Atender oportunamente las solicitudes y reclamaciones materiales, cuidando que sean exactas y completas;
7. Proporcionar a los titulares de firmas, un medio para dar aviso que la Firma Electrónica refrendada está en entredicho;
8. Suministrar la información que le requieran las entidades administrativas competentes o judiciales con relación a las Firmas Electrónicas y certificados emitidos, y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;
9. Permitir y facilitar la realización de las auditorías por parte de la Autoridad Administrativa Competente (AAC) con autorización de la Dirección General de Propiedad Intelectual (DIGEPIH);
10. Llevar un registro electrónico de los certificados emitidos y cancelados;

11. Informar a los firmantes de las condiciones de emisión, uso y cancelación de los certificados de Firmas Electrónicas reconocidas;
12. Proporcionar a la parte que confía en el certificado, medios razonablemente accesibles que permitan a ésta determinar mediante el certificado, la información siguiente:
    a. La identidad del prestador de servicios de certificación;
    b. Que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;
    c. Que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;
    d. El método utilizado para comprobar la identidad del firmante;
    e. Cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;
    f Si los datos de creación de la firma son válidos y no están en entredicho;
    g. Cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;
    h Si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el Artículo 8 de la Ley; y,
    i. Si se ofrece un servicio para revocar oportunamente el certificado;
13. Revocar de forma inmediata los certificados emitidos e implementar medidas necesarias, cuando la clave privada de la autoridad de certificación sea comprometida;
14. Mantener un registro que garantice se pueda determinar con precisión la fecha y la hora en las que se expidió un certificado o se revocó; y,
15. Cumplir los términos bajo los cuales obtuvo la acreditación conforme a lo establecido en este Reglamento.

Serán de cargo de la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) las consecuencias jurídicas que entrañe el hecho de no haber cumplido con los requisitos enunciados en la ley y el presente reglamento.

Artículo 34. Responsabilidad de las Autoridades de Certificación o Prestadores de Servicios de Certificación (PSC).

La Autoridad Certificadora o Prestadores de Servicios de Certificación (PSC) será responsable de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso corresponderá a las Autoridades Certificadoras (PSC) demostrar que actuó con la debida diligencia.

Artículo 35. Limitaciones de Responsabilidad de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).

Las Autoridades Certificadora o Prestadores de Servicios de Certificación (PSC) no serán responsables de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:

1. No haber proporcionado a la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación;
2. La falta de comunicación sin demora a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) de cualquier modificación de las circunstancias reflejadas en el certificado electrónico;
3. Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación;
4. No solicitar la revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma;
5. Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de certificación le notifique la extinción de su vigencia; y,
6. Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación.

Las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) tampoco serán responsables de los daños y perjuicios ocasionados al firmante o a terceros de buena fe, si el destinatario de los documentos firmados electrónicamente actúa de forma negligente.

Se entenderá, en particular, que el destinatario actúa de forma negligente en los casos siguientes:

1. Cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus

posibles usos y al importe individualizado de las transacciones que puedan realizarse con él; y,

2. Cuando no tenga en cuenta la revocación o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica.

La exención de responsabilidad frente a terceros obliga a la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) a probar que actuó en todo caso con la debida diligencia.

Artículo 36. Remuneración por la Prestación de Servicios de Certificación (PSC).

La remuneración por los servicios de la Autoridad Certificadora o Prestadora de Servicios de Certificación (PSC), será establecida libremente por ésta.

Artículo 37. Terminación unilateral.

La Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) podrá dar por terminado el acuerdo de vinculación con el suscriptor dando un preaviso no menor de treinta (30) días hábiles. Vencido este término, la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) revocará los certificados que se encuentren pendientes de expiración.

Igualmente, el suscriptor podrá dar por terminado el acuerdo de vinculación con la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) dando un preaviso no inferior a treinta (30) días hábiles.

Artículo 38. Cese de actividades del Prestador de Servicios de Certificación (PSC).

La Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) autorizado puede cesar en el ejercicio de actividades por voluntad propia, siempre y cuando haya recibido autorización por parte de la Autoridad Acreditadora Competente (AAC).

Cuando las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) decidan cesar en sus actividades, solicitarán autorización a la Autoridad Acreditadora Competente (AAC) al menos con sesenta (60) días hábiles de anticipación a la fecha de cesación.

Así mismo, deberá advertir al titular que de no existir objeción a la transferencia de los certificados a otro prestador de servicios de certificación, dentro del plazo de quince (15) días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos. En este caso, si el prestador es acreditado, deberá traspasar los certificados, necesariamente, a un certificador acreditado e informará este extremo al titular

Si el cese no es voluntario o revocatorio, la cancelación de la acreditación, deberá comunicarse a través de la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC), inmediatamente a los titulares. En caso que el la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) esté en situación de traspasar los certificados a otro prestador acreditado, deberá informar tal situación en la forma y plazo señalado en el artículo anterior (Art. 37).

Si el titular del certificado se opone a la transferencia, el certificado quedará sin efecto sin más trámite.

Artículo 39. Proceso de Transmisión de los Certificados Electrónicos.

La Autoridad Administrativa Competente (AAC), emitirá el instructivo que contendrá el proceso mediante el cual se llevará a cabo la transmisión de certificados electrónicos entre las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) con la autorización de la Autoridad Certificadora.

CAPÍTULO VII
DURACIÓN DE LA ACREDITACIÓN Y RENOVACIÓN

Artículo 40. De la Duración de la Acreditación.

La duración de la autorización otorgada por la Autoridad Administrativa Competente (AAC) para operar como la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) será de cinco (5) años, a partir de la fecha de la resolución que la conceda; pero podrá renovarse por periodos iguales mediante el pago de la tasa de renovación. Si la Autoridad Administrativa Competente (AAC) considera necesario deberá practicarse inspección o auditoría para constatar el cumplimiento de los requisitos y de la efectiva prestación de servicios de acreditación.

Artículo 41. De la Renovación.

La renovación de la autorización para operar como la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) se efectuará mediante la presentación de la solicitud de renovación, ante la Autoridad Administrativa Competente (AAC) dentro de los tres (3) meses antes de su vencimiento. La renovación también podrá hacerse dentro de un plazo de gracia de tres (3) meses contados desde la fecha de vencimiento de la acreditación o de

la renovación en su caso, debiendo pagarse la sobretasa establecida, además de la tasa de renovación correspondiente.

Durante el plazo de gracia, el registro de la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) mantendrá su vigencia plena.

La solicitud de renovación deberá presentarse en el formato aprobado por la Autoridad Administrativa Competente (AAC) al efecto y contendrá al menos los siguientes datos:

a. Datos generales de la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) de su representante o apoderado;
b. Número y fecha de la resolución de otorgamiento y de su registro;
c. Modificación del registro (en caso cambio de nombre por fusión o transformación);
d. Relación de documentos anexos;
e. Lugar y fecha;
f. Nombre y firma del solicitante; y,
g. Fotocopia del recibo de pago de la tasa de renovación y en su caso, de la sobretasa.

Si la solicitud de renovación se presentare antes de los tres (3) meses para el vencimiento de la acreditación, se le devolverá al peticionario y se tendrá por no presentada, sin perjuicio de que se presente en tiempo y forma.

De no renovarse la acreditación en una de las formas previstas en este artículo, la Autoridad Administrativa Competente (AAC) procederá a revocar definitivamente la autorización para operar como autoridad certificadora, sin perjuicio de resarcir los daños y perjuicios que ocasione a los suscriptores de conformidad con el artículo 25 de la ley.

CAPÍTULO VIII
DE LOS SUSCRIPTORES Y USUARIOS DE LOS SERVICIOS DE CERTIFICACIÓN

Artículo 42. Derechos de los Suscriptores y/o Usuarios de los Servicios de Certificación.

Los usuarios o titulares de certificados o firmas electrónicas reconocidas tendrán los siguientes derechos:

a. A ser informados por los prestadores de servicios de certificación, de las características generales de los procedimientos de creación y de verificación de firma electrónica, así como las reglas sobre prácticas de certificación y los demás que estos se comprometan a seguir en la prestación de servicios, previamente a que se empiece a efectuar;
b. A la confidencialidad en la información cuando los prestadores de servicios de certificación decidan cesar en sus actividades;
c. A ser informados antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, en su caso; de condiciones precisas para la utilización del certificado y sus limitaciones de uso, y de los procedimientos de reclamación y de resolución de litigios previstos en las leyes que se convinieren;
d. A que la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) o quien homologue sus certificados le proporcionen la información sobre sus domicilios en Honduras y sobre todos los medios a los que el usuario pudiera acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar reclamos;
e. A ser informado por la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) del cese de su actividad, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador;
f. A ser informado inmediatamente de la cancelación de la inscripción en el registro de la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) acreditados, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador;
g. A traspasar sus datos a otro prestador de servicios de certificación;
h. A que la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) no proporcione más servicios y de otra calidad de los que haya pactado, y a no recibir publicidad comercial de ningún tipo por intermedio del prestador, salvo autorización expresa del usuario;
i. A acceder, por medios electrónicos al registro de la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) acreditados que mantendrá la Autoridad de Vigilancia y Control (Autoridad Administrativa Competente); y,
j. A ser indemnizado por los daños y perjuicios que la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) le ocasionare, considerando lo establecido en los artículos 35 y 36 del presente reglamento.

Artículo 43. Obligaciones de los Suscriptores o Titulares de los Servicios de Certificación (PSC).

Además de las señaladas en el artículo 23 de la Ley, los suscriptores o titulares de certificados o firmas electrónicas reconocidas tendrán las siguientes obligaciones:

a. Entregar información veraz bajo su responsabilidad;
b. Observar las condiciones establecidas para la utilización lógica y física de las firmas electrónicas reconocidas, sus certificados y dispositivos asociados;
c. Generar la clave privada y firma mediante los procedimientos señalados por la Declaración de Prácticas del Prestador de Servicios de Certificación;
d. Mantener el control y la reserva de la clave privada bajo su responsabilidad.
e. Actualizar permanentemente la información brindada al Prestador de Servicios de Certificación, asumiendo responsabilidad por la veracidad y exactitud de ésta;
f. En caso de que la clave privada quede comprometida en su seguridad, el titular debe notificarlo de inmediato a la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) para que revoque el certificado asociado a dicha clave; y,
g. Efectuar los pagos correspondientes por los servicios de certificación.

Artículo 44. Responsabilidad de los Suscriptores o Titulares de los Servicios de Certificación.

Los Suscriptores o titulares serán responsables por la falsedad, error u omisión en la información suministrada al prestador de servicios de certificación y por el incumplimiento de sus obligaciones como suscriptor o titular.

CAPÍTULO IX
UTILIZACIÓN DE LA FIRMA ELECTRÓNICA Y DOCUMENTOS ELECTRÓNICOS POR LOS ÓRGANOS DEL ESTADO

Artículo 45. Autorización para Utilización de las Firmas Electrónicas

Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Supremo Electoral, así como a todas las instituciones públicas descentralizadas y entes públicos no estatales y cualquier dependencia del sector público, para la utilización de las firmas electrónicas en los documentos electrónicos en sus relaciones internas, entre ellos y con los particulares.

Para obtener la aprobación de la autoridad acreditadora, los órganos del Estado deberán someterse al procedimiento establecido en los Artículos del 24 al 29; pero estarán exentos del pago de los costos establecidos en el Artículo 30 y del pago del arancel a que refiere el Artículo 48, en lo demás quedan sujetos a la ley y al presente Reglamento.

CAPÍTULO X
DE LAS FUNCIONES Y ATRIBUCIONES DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE (AAC).

Artículo 46. De las Funciones y Atribuciones de la Autoridad Administrativa Competente (AAC).

La Dirección General de Propiedad Intelectual (DIGEPIH), además de las ya señaladas en la Ley y en este Reglamento, tiene las siguientes funciones y atribuciones:

a. Recibir y resolver las solicitudes de autorización para operar como Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) en el territorio nacional;
b. Llevar el registro físico y digital de las personas naturales y jurídicas que han sido acreditadas para operar como Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), llevando anotación fehaciente de toda actuación derivada de los mismos;
c. Velar por el buen funcionamiento y la eficiente prestación del servicio por parte de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC);
d. Ejercer la función de supervisión, control y vigilancia ordinaria o extraordinaria, o auditorías a las Autoridades Certificadora o Prestadores de Servicios de Certificación (PSC), levantando los informes pertinentes. En caso de imposibilidad administrativa, técnica o financiera para el desarrollo de las funciones antes descritas se podrá auxiliar de consultorías externas, las cuales deberán ser financiadas por la o las PSC involucradas;
e. Instruir, sustanciar y resolver los procedimientos que correspondan para revocar o suspender la autorización para operar como Autoridad Certificadora o Prestadores de Servicios de Certificación (PSC);
f. Iniciar de oficio o a petición de parte, los procedimientos para imponer sanciones a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio;
g. Conocer y resolver la revocación de certificados, cuando las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) los emita sin el cumplimiento de las formalidades legales;
h. Emitir los certificados de Autorización que sean solicitados en relación con las firmas electrónicas de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC);

i. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor en los mercados atendidos por las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC);
j. Impartir las directrices e instrucciones sobre el adecuado cumplimiento de las disposiciones a las cuales deben sujetarse las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC);
k. Llevar el registro de las sanciones impuestas a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC);
l. Llevar la guarda y custodia de todos los documentos físicos y datos electrónicos que correspondan y deriven del ejercicio de sus funciones y atribuciones;
m. Difundir la Ley, promover el uso de la firma electrónica, y ofrecer servicios de consulta a los usuarios;
n. Aprobar el empleo de estándares técnicos internacionales dentro de la Infraestructura Oficial de Firma Electrónica y determinar la compatibilidad de otros;
o. Definir los criterios para evaluar la suficiencia del respaldo financiero con el que deben contar las entidades de certificación;
p. Suscribir acuerdos de reconocimiento mutuo con autoridades administrativas extranjeras que cumplan funciones similares a las de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC);
q. Delegar en el personal bajo sus órdenes y responsabilidad, las funciones que de conformidad a ley y el presente reglamento correspondan;
r. Conocer de los reclamos que se presenten contra o entre Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), los suscriptores de Firmas Electrónicas, las partes que confían y de las demás personas sujetas a la Ley de Firmas Electrónicas y el presente Reglamento; y,
s. Las demás que resulten necesarios para el cumplimiento de las obligaciones que le impone la Ley y este Reglamento.

Artículo 47. La Unidad Técnica de Servicios de Informática dependiente de la Dirección General de Propiedad Intelectual (DIGEPIH).

Como área especializada en tecnologías de la información y comunicaciones, será la encargada de implementar y administrar la infraestructura tecnológica necesaria para el registro y control de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), así mismo para brindar información y capacitación que requieran sobre el sistema de registro y certificación.

Artículo 48. Obligaciones de la Unidad Técnica de Servicios de Informática.

La Unidad de Servicios Técnicos Informáticos tendrá las obligaciones siguientes:

a. Establecer y operar los esquemas de monitoreo para las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), para garantizar la disponibilidad de la infraestructura tecnológica que soporta los procesos operativos asociados a la Firma Electrónica Avanzada;
b. En el ámbito de sus atribuciones, preservar la confidencialidad, integridad y seguridad de los datos personales e institucionales de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) en términos del reglamento;
c. Habilitar los mecanismos de consulta en línea de los certificados digitales de Acreditación, las listas de revocación, así como la habilitación de servicios de verificación en línea para obtener el estado de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) acreditados por las Autoridades Administrativas Competentes (AAC);
d. Implementar los lineamientos de control de acceso a los mecanismos de consulta en línea respecto de los certificados digitales expedidos por la Autoridad Administrativa Competente (AAC), en torno a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC);
e. Conocer los controles tecnológicos y/o protocolos de seguridad que al efecto deberán llevar las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) para proteger las llaves públicas y privadas de las mismas durante todo su ciclo de vida (generación de las llaves, uso y activación de las llaves, desactivación y borrado de las llaves);
f. Establecer observancia sobre los esquemas de auditorías internas y externas que las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) deberán llevar en materia de seguridad informática que permitan identificar riesgos y vulnerabilidades potenciales en la infraestructura que soporta los procesos operativos asociados al Sistema de Registro y Certificación, así como ejecutar los procesos de corrección que se consideren adecuados, y las demás que se deriven de las disposiciones del presente Reglamento y que le designe la Autoridad Administrativa Competente (AAC).
g. Preparar los parámetros e instructivos mínimos para la trasmisión de los certificados y documentos digitales de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) a otro, haciendo las previsiones correspondientes para el registro administrativo.

Artículo 49. Ingresos de la Autoridad Administrativa Competente (AAC).

Serán ingresos de la Autoridad Administrativa Competente (AAC), los siguientes:

a. Los recursos que le sean asignados por el Instituto de la Propiedad en el presupuesto Anual de conformidad con las exigencias del servicio que presta.
b. Los provenientes de su gestión en aplicación de los costos de acreditación, renovación y el arancel de auditoría.

Artículo 50. Aranceles de la Autoridad Administrativa Competente (AAC).

Los costos de acreditación serán pagados por la Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) que solicite acreditarse, los cuales no serán restituidos en el evento de que la acreditación no se conceda por incumplimiento de los requisitos y obligaciones legales y reglamentarias exigidas para el desarrollo de la actividad de certificación como acreditado.

La Autoridad Administrativa Competente (AAC) a través de la Dirección General de Propiedad Intelectual (DIGEPIH) de conformidad con lo establecido en el Artículo 10, numeral 12 de la LEY DE PROPIEDAD (Decreto 82-2004 de fecha 29 de Junio de 2004); propondrá ante el CONSEJO DIRECTIVO del INSTITUTO DE LA PROPIEDAD las tasas por la acreditación, renovación, cancelación, supervisión, vigilancia y auditoría.

El arancel deberá ser pagado por las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) acreditados dentro de los treinta (30) días siguientes a la fecha de la providencia o resolución que lo ordene.

Artículo 51. De la Función de Supervisión, Control y Vigilancia.

La Dirección General de Propiedad Intelectual como Autoridad Administrativa Competente (AAC), ejercerá la función de supervisión, control y vigilancia de las actividades de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) con el objeto de verificar que cumplan con todos los requerimientos y exigencias legales, técnicas y reglamentarias para ofrecer un servicio eficaz a sus usuarios. A tal efecto, podrá directamente o a través de expertos, realizar las inspecciones ordinarias, extraordinarias y auditorías que fueren necesarias para comprobar que las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) deben cumplir.

Artículo 52. Supervisión Ordinaria y Extraordinaria.

Para vigilar el correcto desempeño de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), la Autoridad Administrativa Competente (AAC), llevará a cabo al menos una (1) inspección ordinaria anualmente y extraordinariamente, en alguno de los supuestos siguientes:

a. Cambios estructurales u organizacionales de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).
b. Cambios en las políticas, procedimientos o prácticas empleadas en la prestación de los servicios por parte de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).
c. Cuando haya un uso indebido o fuera del alcance de la acreditación obtenida.
d. Cuando el análisis de un reclamo o cualquier otra información que contravenga el cumplimiento de las condiciones de acreditación.

Las visitas de supervisión se realizarán sin previo aviso a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), salvo que la Autoridad Administrativa Competente (AAC) disponga lo contrario en función a la finalidad de la supervisión y los resultados de la misma serán informados a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).

Artículo 53. Auditorías.

Sin perjuicio de las supervisiones, la acreditación se encuentra sujeta a auditorías a partir de la fecha de la resolución de acreditación. Estas auditorías buscan asegurar que las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), han respetado las condiciones establecidas para el otorgamiento de la acreditación y que asimismo cumple con los criterios de acreditación y competencia técnicas correspondientes para la prestación de sus servicios en condiciones habituales.

Los objetivos fundamentales de las evaluaciones de seguimiento son:

a. Comprobar el mantenimiento de los criterios de acreditación por parte de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).
b. Verificar la implementación y eficacia de las acciones correctivas o las no conformidades u observaciones detectadas en evaluaciones previas, de ser el caso.

c. Comprobar que se han respetado las obligaciones de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).
d. Examinar cualquier cambio en la organización, procedimientos y recursos de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) para la realización de las actividades incluidas en el alcance de la acreditación y verificar que los eventuales cambios en las mismas han sido puestos en conocimiento de la Autoridad Administrativa Competente (AAC).
e. Evaluar aspectos que hayan generado reclamos o comunicaciones de usuarios por supuestas irregularidades en los servicios prestados por las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).

En caso de reiterados reclamos o denuncias, o bien por circunstancias especiales no previstas en este artículo, la Autoridad Administrativa Competente (AAC) pueden realizar auditorías extraordinarias. Los resultados de estas auditorías serán informados a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC).

CAPITULO XI
DEL PROCEDIMIENTO PARA LAS SANCIONES ADMINISTRATIVAS

Artículo 54. Actuación de Oficio o por Denuncia.
En cumplimiento de la función de inspección, control y vigilancia la Autoridad Administrativa Competente (AAC) podrá iniciar de oficio o a petición de parte, los procedimientos para imponer sanciones a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio.

El procedimiento de oficio dará inicio con el informe que se levante en ocasión de la visita de supervisión, inspección o auditoría que se practique a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), siempre que en el informe resulte evidenciada la transgresión o falta, y en lo sucesivo el proceso se activara en la forma prevista en el presente capítulo.

Artículo 55. Contenido de la Denuncia.
La denuncia se formulará por escrito y en la misma se expresará y acompañará los datos siguientes:

a. Suma que indique su contenido o trámite de que se trate;
b. La indicación del órgano al que se dirige;
c. El nombre y apellido, estado, profesión u oficio y domicilio del solicitante o de su representante, en cuyo caso deberá presentar el documento que acredite su representación;
d. Los hechos y razones en que se funde y la expresión clara de lo que se solicita; y,
e. Lugar, fecha y firma o huella digital, cuando no pudiese o supiese firmar.

Además con el escrito de la denuncia, se acompañarán los documentos en que el denunciante se fundamenta y los medios de prueba que justifiquen su petición.

Artículo 56. Recepción de la Denuncia.
Recibida la denuncia en los términos del artículo anterior, esta se impulsará de oficio y se procederá a citar al denunciado para ponerle en conocimiento la infracción imputada, dándole el derecho a defenderse presentando sus alegatos por escrito en los mismos términos del artículo anterior (Art.55).

Artículo 57. Citación.
La citación se hará al supuesto infractor dentro de un término de quince (15) días, por medio de cédula que le será entregada personalmente y no hallándose el citado, se hará entrega a cualquiera de sus familiares, dependientes o empleados que se encuentren en el domicilio o centro de trabajo habitual; en su defecto se procederá a citar a través de la dirección de correo electrónico, aceptado expresamente dicho medio como forma de comunicación, al tenor de lo dispuesto en el artículo 24 de este Reglamento.

Artículo 58. Contestación.
Si el citado compareciera, se le hará entrega de la copia de la denuncia o del acta de inspección, así como de las pruebas que se tengan para que en el término de veinte (20) días conteste sus alegatos de descargo, consignando lo actuado en acta.

Artículo 59. Resolución.
La Autoridad Administrativa Competente (AAC), una vez contestada la denuncia y cuando las pruebas presentadas por el denunciante se consideren suficientes; a criterio de la Autoridad Administrativa Competente (AAC) o habiendo el inculpado admitido los cargos formulados, se procederá a dictar la resolución correspondiente.

Artículo 60. Pruebas Insuficientes.
Si las pruebas fueren insuficientes y el inculpado negare los cargos, se abrirá la causa a prueba por el término de veinte (20) días comunes a las partes, prorrogables por una sola vez por el

término de diez (10) días, transcurridos los cuales la Autoridad Administrativa Competente (AAC) dictará la resolución correspondiente, pudiendo declarar procedente o improcedente la acción entablada.

Artículo 61. Recursos.

Contra esta Resolución, proceden el Recurso de Reposición y Subsidiaria Apelación establecidas en el artículo No.28 de este Reglamento.

CAPITULO XII
INFRACCIONES Y SANCIONES

Artículo 62. Infracciones.

Las infracciones de este reglamento se clasifican en leves, graves y muy graves.

Artículo 63. Infracciones Leves.

1. No emitir los certificados conforme a lo solicitado o acordado con el suscriptor;
2. No garantizar que todas las declaraciones y manifestaciones materiales, sean exactas y completas;
3. No atender oportunamente las solicitudes y reclamaciones materiales, cuidando que sean exactas y completas;
4. No proporcionar a los titulares de firmas un medio para dar aviso que la firma electrónica refrendada está en entredicho;

Artículo 64. Infracciones Graves.

Son infracciones graves:

1. La reiteración en faltas leves;
2. La expedición de los certificados electrónicos sin realizar todas las comprobaciones previas.
3. La falta o deficiente presentación de la información solicitada por parte de la Dirección General de Propiedad Intelectual (DIGEPIH) en su función de vigilancia y control.
4. No adoptar las medidas razonables para determinar con exactitud la identidad del titular de la firma y de cualquier otro hecho y acto que certifique;
5. No garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor;
6. No llevar el registro electrónico de los certificados emitidos y cancelados o no Informar a los firmantes de las condiciones de emisión, uso y cancelación de los certificados de firmas electrónicas reconocidas.
7. No declarar o declarar parcialmente las Prácticas de Certificación establecidas en el artículo 32 del presente Reglamento.
8. No proporcionar a la parte que confía en el certificado, medios razonablemente accesibles que le permitan determinar mediante el certificado, la información descrita en el numeral 12 del artículo 33 de este Reglamento;
9. No mantener un registro que garantice se pueda determinar con precisión la fecha y la hora en las que se expidió un certificado o se revocó el mismo.
10. No cumplir o no mantener los términos y condiciones bajo los cuales obtuvo la acreditación conforme a lo establecido en este Reglamento.

Artículo 65. Infracciones Muy Graves.

Son infracciones muy graves:

1. Reincidencia en la comisión de infracciones graves;
2. No suministrar la información que le requieran las entidades administrativas competentes o judiciales con relación a las firmas electrónicas y certificados emitidos, y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración;
3. No permitir o facilitar la realización de las auditorías por parte de la Dirección General de Propiedad Intelectual (DIGEPIH), o la resistencia, obstrucción, excusa o negativa injustificada a la actuación auditora de los órganos facultados para llevarla a cabo con arreglo a este Reglamento;
4. No revocar de forma inmediata los certificados emitidos e implementar medidas necesarias, cuando la clave privada de la autoridad de certificación sea comprometida.
5. El incumplimiento de las resoluciones dictadas por la Dirección General de Propiedad Intelectual (DIGEPIH) para asegurar que el prestador de servicios de certificación se ajuste al presente Reglamento.
6. No Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas electrónicas, la conservación y archivo de certificados y documentos en soporte de mensaje de datos;
7. La expedición de certificados falsos o el fraude en la titularidad de los mismos;
8. La transferencia de certificados electrónicos a otra u otras Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) estén o no acreditados, sin la autorización de la Autoridad Administrativa Competente (ACC).

Artículo 66. Sanciones.

La Dirección General de Propiedad Intelectual (DIGEPIH) en observancia del debido proceso y del derecho de defensa, es decir observando el procedimiento establecido en el Capítulo X de este Reglamento, podrá imponer a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC), según la naturaleza y la gravedad de la falta, las sanciones siguientes:

En caso de Faltas Leves: Amonestación privada escrita.
En caso de Faltas Graves:

1. Multas institucionales hasta por el equivalente a dos mil (2,000) salarios mínimos legales mensuales vigentes; y personales a los administradores y representantes legales de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) hasta por trescientos (300) salarios mínimos legales mensuales vigentes, cuando se les compruebe que han autorizado, ejecutado o tolerado una conducta violatoria de la Ley,
2. Suspender de inmediato todas o algunas de las actividades de la autoridad (PSC) infractora;

En caso de Faltas Muy Graves:

1. Prohibir a las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) infractoras prestar directa o indirectamente los servicios de Autoridad Certificadora o Prestador de Servicios de Certificación (PSC) hasta por el término de cinco (5) años; y,
2. Revocar definitivamente la autorización para operar como Autoridad Certificadora o Prestador de Servicios de Certificación (PSC).

Las sanciones señaladas se aplicarán, sin perjuicio de la responsabilidad civil o penal y de las penas que correspondan a los delitos que, en su caso, incurran los infractores.

En caso de la cancelación de la acreditación otorgada, la entidad cuya acreditación haya sido cancelada, sólo podrá obtenerla luego de transcurridos cinco (5) años desde la fecha de la cancelación.

Las sanciones previstas en el presente artículo, serán establecidas e impuestas por la Autoridad Administrativa Competente (AAC) mediante resolución motivada, pudiendo disponer la publicación de la misma, cuando se haya agotado la vía administrativa.

Respecto del fallo que imponga la sanción, se puede interponer los recursos en la forma prevista en el artículo 28 de este Reglamento.

Artículo 67. Criterios para la Imposición de Sanciones
La Autoridad Administrativa Competente (AAC) al hacer el análisis para imponer la sanción, deberá considerar según corresponda en cada caso, los criterios siguientes:

1. Naturaleza y gravedad de la infracción;
2. El daño causado o grado de afectación generado por la infracción en los usuarios;
3. El beneficio obtenido con la infracción, a fin de evitar, en lo posible, que dicho beneficio sea superior al monto de la sanción;
4. La reincidencia en la comisión de una falta;
5. La conducta de la entidad acreditada infractora a lo largo del procedimiento de oposición de la sanción, que comprende la continuación de la práctica materia del procedimiento de infracciones y especialmente la disposición para reparar el daño o mitigar sus efectos;
6. La intencionalidad del infractor;
7. La procuración de reparar los daños causados;
8. Necesidad de dictar medidas cautelares;
9. Cualquier otro que la autoridad administrativa competente deba considerar.

CAPITULO XIII
DISPOSICIONES FINALES Y TRANSITORIAS

Artículo 68. Interpretación Progresiva.
Las regulaciones del presente reglamento serán aplicables a los mensajes de datos y firmas electrónicas independientemente de las características técnicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los mensajes de datos y firmas electrónicas, así como los principios de equivalencia funcional, neutralidad tecnológica y de respeto a la autonomía de las partes.

Artículo 69. Prestadores de Servicios de Certificación Preexistentes.
Aquellas Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) que hayan sido autorizados por una Ley anterior a la publicación de la Ley sobre Firmas Electrónicas y del presente Reglamento que deseen continuar prestando su servicio deberán presentar su solicitud ante la Autoridad Administrativa Competente (AAC) en un plazo no mayor de seis (6) meses, debiendo proceder a ajustar sus estatutos, organización y funcionamiento con las disposiciones de la Ley y el presente Reglamento.

Artículo 70. Incumplimiento por los Prestadores de Servicios de Certificación Preexistentes.
Las entidades que no se hayan regulado como Prestador de Servicio de Certificación (PSC), que continúen operando como

tales y no haya cumplido con el plazo a que se refiere el artículo anterior, la Autoridad Administradora Competente (AAC), le aplicará una multa equivalente a (300) salarios mínimos legales mensuales vigentes, sin perjuicio de las sanciones que corresponda aplicar.

Artículo 71. Uso de Manuales, Instructivos y Formularios.

La Dirección General de Propiedad Intelectual, como Autoridad Administrativa Competente (AAC), emitirá el instructivo al que se sujetará el traspaso de la transmisión de Certificados Electrónicos entre las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) con su previa autorización; también emitirá los formularios de solicitud de acreditación, renovación, fusión, cambio de domicilio, cancelación voluntaria de la acreditación y los demás formularios que resulten necesario; podrá emitir además, los instructivos y manuales que resultaren indispensables para informar y uniformar las actuaciones de las Autoridades Certificadoras o Prestadores de Servicios de Certificación (PSC) y la propia Autoridad Administrativa Competente; esta última deberá mantener toda la información accesible al menos por medio digital.

Artículo 72. Obligatoriedad del presente Reglamento.

Las regulaciones y disposiciones fijadas en el presente Reglamento son de obligatorio cumplimiento para los Prestadores de Servicios de Certificación (PSC) acreditados. La no observancia será sancionada con la multa a que hubiere lugar, según la gravedad de la misma.

Artículo 73. Recursos y Presupuesto

La Dirección General de Propiedad Intelectual (DIGEPIH) como Autoridad Administrativa Competente (AAC), en coordinación con las Autoridades Superiores del Instituto de la Propiedad (IP), deberán presupuestar los recursos necesarios para la implementación, el uso y operación de la Firma Electrónica en forma anual, de conformidad con las disposiciones generales de la Ley de Presupuesto.

Artículo 74. Epígrafes.

Los epígrafes relativos a la identificación del contenido de las normas en el presente Reglamento y que preceden a cada artículo, no tienen valor interpretativo.

SEGUNDO.- El presente reglamento entrará en vigencia a partir de la fecha de su publicación en el Diario Oficial "La Gaceta".

Dado en la ciudad de Tegucigalpa, M.D.C., a los doce (12) días del mes de diciembre del dos mil catorce (2014).

COMUNIQUESE Y PUBLIQUESE.

JUAN ORLANDO HERNÁNDEZ ALVARADO
PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

REINALDO ANTONIO SANCHEZ
SECRETARIO DE ESTADO EN EL DESPACHO DE LA PRESIDENCIA

JUZGADO DE LETRAS CONTENCIOSO ADMINISTRATIVO

A V I S O

El infrascrito, Secretario del Juzgado de Letras de lo Contencioso Administrativo, en aplicación del artículo cincuenta (50) de la Ley de esta jurisdicción y para los efectos legales correspondientes, **HACE SABER:** Que en fecha 12 de agosto del 2014, se interpuso ante este Juzgado, demanda con orden de ingreso **No. 0801-2014-00318,** promovida por el Abogado Cristian Gerardo Medina Sevilla, en su condición de apoderado legal de la señora VILMA HONDURAS RODRÍGUEZ GUZMÁN, contra el Estado de Honduras, a través de la Secretaría de Estado en el Despacho de Seguridad, contraída a pedir: Se declare la nulidad e ilegalidad por no ser conforme a derecho de un acto administrativo de carácter particular emitido por el Poder Judicial a través del Consejo de la Judicatura y de la Carrera Judicial por contener vicios de nulidad y emitido con infracción del ordenamiento jurídico, inclusive el exceso y desviación de poder. Reconocimiento de una situación jurídica individualizada por la ilegal sanción de suspensión de tres meses sin goce de salario y como medida para el pleno restablecimiento del derecho, que se ordene a través de sentencia definitiva el pago de los tres meses de salario que me fue deducido más los derechos laborales de forma proporcional tengo derecho y como pretensión accesoria se reconozca el pago del seis por ciento del interés legal por la cantidad reclamada, se alega prescripción de la acción para imponer la medida disciplinaria.- Se acompañan documentos, costas del juicio, poder.- En relación con las resoluciones de fecha 22 de abril y 7 de mayo del 2014, emitidas por el Consejo de la Judicatura y la Carrera Judicial.

KARINA ELIZABETH GÁLVEZ REYES
SECRETARIA ADJUNTA

21 M. 2015