12 de diciembre de 2019

INSTITUCIONES SUPERVISADAS
Toda la República

CIRCULAR CNBS No.017/2019

Señores:

La infrascrita Secretaria General de la Comisión Nacional de Bancos y Seguros transcribe para los efectos legales que corresponda la parte conducente del Acta de la Sesión No.1362 celebrada en Tegucigalpa, Municipio del Distrito Central el diez de diciembre de dos mil diecinueve, con la asistencia de los Comisionados ETHEL DERAS ENAMORADO, Presidenta; JOSÉ ADONIS LAVAIRE FUENTES, Comisionado Propietario; EVASIO A. ASENCIO, Comisionado Propietario; MAURA JAQUELINE PORTILLO G., Secretaria General; que dice:

"... **7. Asuntos de la Gerencia de Tecnología de Información y Comunicación:** ... literal **a)** ... **RESOLUCIÓN GTI No.977/10-12-2019.-** La Comisión Nacional de Bancos y Seguros,

CONSIDERANDO (1): Que de conformidad a lo dispuesto en el Artículo 13, numerales 1), 2), 4) y 24) de la Ley de la Comisión Nacional de Bancos y Seguros, corresponde a este Ente Supervisor dictar las normas prudenciales que se requieran para la revisión, verificación, control, vigilancia y fiscalización de las Instituciones Supervisadas, para lo cual se basará en la legislación vigente y en acuerdos y prácticas internacionales; cumplir y hacer cumplir la Constitución de la República, las leyes generales y especiales, los reglamentos y resoluciones a que están sujetas las instituciones supervisadas y emitir los reglamentos y demás normas necesarias para el funcionamiento de la Comisión.

CONSIDERANDO (2): Que la Comisión Nacional de Bancos y Seguros mediante Resolución GE No.316/27-02-2012 aprobó las "NORMAS REGULADORAS DE FIRMAS ELECTRÓNICAS ADMINISTRADAS POR LA COMISIÓN NACIONAL DE BANCOS Y SEGUROS", las cuales tienen por objeto regular las firmas generadas bajo la denominada "Infraestructura de Firma Electrónica" (IFE), cuya propiedad y administración le corresponde a la Comisión Nacional de Bancos y Seguros (CNBS), utilizada por las Instituciones Usuarias del Sistema de Interconexión Financiera. Esta Resolución se fundamentó en el Artículo 51 del Decreto Legislativo No.129-2004 LEY DEL SISTEMA FINANCIERO publicado en el Diario Oficial La Gaceta con fecha 24 de septiembre del 2004.

CONSIDERANDO (3): Que mediante Decreto Legislativo No.160-2016 se reformó el Artículo 51 de la LEY DEL SISTEMA FINANCIERO, el cual establece que: "La Comisión seleccionará la infraestructura que soportará la firma en formato electrónico que debe utilizarse para el intercambio de información segura entre la Comisión y las instituciones del sistema financiero, así como para los demás fines que el Ente Regulador estime necesarios en cumplimiento de sus atribuciones y deberes, pudiendo para tales efectos, contratar servicios especializados para su implementación y/o revisiones, garantizando en todo momento la aplicación de los más altos estándares en materia de seguridad de la información. La infraestructura señalada en el párrafo anterior debe cumplir con las siguientes condiciones: 1) Identificar de manera única al firmante; 2) Que haya sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control; 3) Que haya sido realizada por un dispositivo seguro de creación de firma; y, 4) Que permita detectar cualquier cambio posterior de los datos firmados. La firma generada a través de medios electrónicos, utilizada para los propósitos establecidos en el primer párrafo del presente Artículo, tendrá respecto de los datos consignados en

COMISIÓN NACIONAL DE BANCOS Y SEGUROS SECRETARÍA GENERAL HONDURAS

forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y debe ser admisible como prueba en juicio, debiendo valorarse como instrumento público. Los servicios de la infraestructura que soporta la firma en formato electrónico administrados por la Comisión, no están sujetos a la inspección, vigilancia y control de otra entidad pública o privada. Lo anterior, a efecto de asegurar su independencia y capacidad técnica, administrativa y financiera, en el cumplimiento a lo señalado en el presente Artículo".

CONSIDERANDO (4): Que la Comisión Nacional de Bancos y Seguros considera necesario reformar las normas vigentes en materia de firmas en formato electrónico para el intercambio de información segura entre la Comisión Nacional de Bancos y Seguros y las instituciones del sistema financiero, así como demás personas naturales o jurídicas que realicen cualquier trámite o gestión administrativa; a efecto de adecuarlas a los mejores prácticas y estándares internacionales y a las condiciones actuales del mercado.

POR TANTO: Con fundamento en los Artículos 6, 8 y 13 numerales 1), 2), 4), 24) y 25) de la Ley de la Comisión Nacional de Bancos y Seguros; 51 reformado de la Ley del Sistema Financiero;

RESUELVE:

1. Reformar las "Normas Reguladoras de Firmas Electrónicas administradas por la Comisión Nacional de Bancos y Seguros", las cuales se leerán así:

NORMAS PARA REGULAR LA FIRMA EN FORMATO ELECTRÓNICO DE LA COMISIÓN NACIONAL DE BANCOS Y SEGUROS

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto
Las presentes Normas tienen por objeto regular el uso de la firma en formato electrónico soportada por la infraestructura tecnológica de la Comisión Nacional de Bancos y Seguros, de conformidad a lo dispuesto en el Artículo 51 reformado de la Ley del Sistema Financiero.

Artículo 2. Alcance
Estarán sujetas a las disposiciones contenidas en las presentes Normas las instituciones supervisadas y demás personas naturales o jurídicas, que utilicen la firma en formato electrónico soportada por la infraestructura tecnológica de la Comisión Nacional de Bancos y Seguros.

Artículo 3. Definiciones
Para efectos de las presentes Normas, se entiende por:
1. Autoridad Certificadora: Entidad de confianza, responsable de emitir y recovar certificados digitales.
2. Autoridad Certificadora Raíz: En una Infraestructura de Llave Pública (PKI), es la autoridad certificadora de confianza por todas las personas que utilizarán los certificados digitales de la PKI.
3. Autoridad Certificadora Subordinada: En una Infraestructura de Llave Pública (PKI), es una autoridad certificadora que ha sido debidamente certificada por la Autoridad Certificadora Raíz u otra Autoridad Certificadora Subordinada a la Autoridad Certificadora Raíz.

COMISION NACIONAL DE BANCOS Y SEGUROS SECRETARIA GENERAL HONDURAS, C.A.

4. Certificado Digital: Documento electrónico firmado digitalmente utilizado para demostrar la propiedad de una llave pública. Este documento incluye una llave pública e información del dueño de la llave pública, y la firma digital de la Autoridad Certificadora.
5. Cifrar: Transcribir en letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger.
6. Comisión: Comisión Nacional de Bancos y Seguros.
7. Criptografía: El cifrado (y descifrado) de información, que tiene como objetivo garantizar la confidencialidad, integridad, el no repudio y la autenticación de la información. (i) confidencialidad: que la información no sea entendida por personas a las cuales la información no fue destinada; (ii) integridad: que la información no pueda ser alterada en almacenamiento o en tránsito entre el remitente y el destinatario sin que la alteración sea detectada; (iii) no repudio: el creador/remitente de la información no puede negar en un momento futuro su intención en la creación o transmisión de la información; (iv) autenticación: el remitente y destinatario pueden confirmar la identidad del otro y el origen/destino de la información.
8. Criptografía Asimétrica: Clave basada en el uso de claves públicas y privadas para cifrar y descifrar. Las claves simplemente son números grandes que se han emparejado, pero no son idénticas (son asimétricas). Una clave del par puede ser compartida con cualquier persona; a esta se conoce como llave pública. La otra clave del par se mantiene secreta; a esta se conoce como llave privada. Cualquiera de las llaves puede ser utilizada para cifrar la información; la llave contraria de la utilizada para cifrar se utiliza para descifrar. (Para brindar confidencialidad, integridad, no repudio, y autenticación, las personas necesitan estar seguras que la llave pública es auténtica, que pertenece a la persona que reclama ser el dueño de la misma, y que no ha sido alterada. Para lograr esto, se utiliza una Infraestructura de Llave Pública).
9. Firma en Formato Electrónico: Los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos y para indicar la voluntad que tiene tal parte respecto de la información consignada en el mensaje de datos.
10. Firma Digital: Firma en formato electrónico, equivalente digital a una firma manuscrita o sello estampado, que permite autenticar y garantizar la integridad de un documento electrónico. Esta firma está basada en criptografía asimétrica. La firma digital se crea mediante el uso de un programa de computadora, el cual genera un hash de la información electrónica que se desea firmar. La llave privada del firmante es utilizada para cifrar el hash, resultando en un valor que es único a la información electrónica original. El hash cifrado (con otra información adicional como el algoritmo utilizado para generar el hash) es la firma digital. Cualquier cambio en la información, aunque sea un solo bit, resultara en un hash diferente. Este atributo permite a otros validar la integridad de la información al utilizar la llave pública del firmante para descifrar el hash. Si el hash descifrado es igual a un segundo hash generado de la misma información, prueba que la data no ha sido modificada desde que fue firmada. Si los dos hashes no son iguales, la información ha sido alterada en alguna manera (indicando un error de integridad) o la firma digital fue creada con una llave privada que no corresponde a la llave pública del firmante (indicando un error de autenticación). La firma digital también hace difícil que el firmante niegue haber firmado el documento (la propiedad de no repudio).
11. Hash: El resultado de transformar por medio de algoritmos una cadena de caracteres en una clave o valor usualmente de tamaño fijo menor a la cadena de caracteres original que representa.
12. IFE: Infraestructura de Firma Electrónica de la CNBS, implementada por la Comisión para generar la firma electrónica, regulada mediante Resolución GE No.316/27-02-2012,

donde la Comisión aprobó las "NORMAS REGULADORAS DE FIRMAS ELECTRÓNICAS ADMINISTRADAS POR LA COMISIÓN NACIONAL DE BANCOS Y SEGUROS".

13. Infraestructura de Llave Pública o PKI por sus siglas en inglés: Infraestructura tecnológica utilizada para soportar la distribución, revocación y verificación de llaves públicas utilizadas en criptografía asimétrica por medio de certificados digitales. La infraestructura de llave pública permite a las personas autenticar a los poseedores de certificados digitales. Estos certificados incluyen la llave pública utilizada para cifrar la información, la información para identificar al poseedor del certificado, la información sobre la PKI que emitió el certificado, y otra información como la vigencia del certificado. (Una PKI está conformada mínimo por: (i) Una autoridad certificadora raíz, la cual debe ser de confianza por todas las personas que utilizarán los certificados digitales de la PKI. Esta autoridad certificadora es la que provee la seguridad de los individuos identificados en los certificados digitales de la PKI; (ii) Una autoridad certificadora subordinada, la cual emite los certificados digitales de la PKI. La autoridad certificadora subordinada es certificada por la autoridad certificadora raíz y es autorizada para emitir certificados digitales).

14. Llave Pública: Clave que se puede compartir con cualquier persona.

15. Llave Privada: En criptografía asimétrica, es la clave que se mantiene secreta.

CAPÍTULO II
DEL AMBITO DE APLICACIÓN Y USO DE LA FIRMA EN FORMATO ELECTRÓNICO DE LA COMISIÓN

Artículo 4. La Firma en Formato Electrónico de la Comisión

Corresponde a la firma en formato electrónico conformada por una firma digital generada a base de un certificado digital emitido por una autoridad certificadora de la infraestructura de llave pública soportada por la infraestructura tecnológica de la Comisión.

Artículo 5. Ámbito de Aplicación de la Firma en Formato Electrónico de la Comisión

La firma en formato electrónico de la Comisión será aplicable para los siguientes ámbitos:

1. El intercambio de información entre la Comisión y las instituciones supervisadas.

2. El intercambio de información entre la Comisión y las personas naturales o jurídicas no supervisadas.

3. La publicación de información por parte de la Comisión al público en general.

4. El intercambio de información entre las diferentes dependencias de la Comisión.

Cualquier clase de solicitud o petición que la Comisión resuelva mediante Resolución u Oficio, de conformidad al marco legal y normativo vigente.

Artículo 6. Uso de la Firma en Formato Electrónico de la Comisión.

La firma en formato electrónico de la Comisión será utilizada exclusivamente para autenticar y garantizar la integridad de la información intercambiada en los ámbitos definidos en el Artículo anterior. Adicionalmente, servirá para garantizar el no repudio de la información intercambiada por el firmante.

Artículo 7. Validez de la Firma en Formato Electrónico de la Comisión.

La firma en formato electrónico de la Comisión utilizada para los ámbitos establecidos en el Artículo 5 de las presentes Normas, tendrá respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y debe ser admisible como prueba en juicio, debiendo valorarse como instrumento público.

CAPÍTULO III
DE LA INFRAESTRUCTURA TECNOLÓGICA QUE SOPORTA LA FIRMA EN FORMATO ELECTRÓNICO DE LA COMISIÓN

Artículo 8. Infraestructura de Llave Pública
La Comisión implementará una infraestructura de llave pública (o PKI por sus siglas en inglés) para soportar la firma en formato electrónico de la Comisión. La PKI de la Comisión estará conformada por una autoridad certificadora raíz, una autoridad certificadora intermedia, la cual estará subordinada a la autoridad certificadora raíz, y dos autoridades certificadoras, subordinadas a la autoridad certificadora intermedia. Todas las autoridades certificadoras mencionadas anteriormente estarán bajo el control exclusivo de la Comisión, creando una cadena de confianza desde la autoridad certificadora raíz hasta los certificados digitales emitidos por la PKI.

Artículo 9. Autoridad Certificadora Raíz
La autoridad certificadora raíz tendrá la función de garantizar la cadena de confianza de la PKI de la Comisión.

Todas las instituciones supervisadas, y demás personas naturales o jurídicas, que utilizarán la firma en formato electrónico de la Comisión, deberán confiar en esta autoridad certificadora raíz. Para tal fin, la Comisión publicará en su página web el certificado digital de la autoridad certificadora raíz.

Artículo 10. Autoridad Certificadora Intermedia
La autoridad certificadora intermedia de la Comisión estará subordinada a la autoridad certificadora raíz, su función es servir de intermediadora entre la autoridad certificadora raíz, y las diferentes autoridades certificadoras subordinadas que estarán emitiendo certificados digitales.

Artículo 11. Autoridad Certificadora Interna
Existirá una autoridad certificadora interna de la Comisión, subordinada a la autoridad certificadora intermedia. Esta autoridad certificadora será responsable de emitir certificados digitales de uso exclusivo de la Comisión.

Los certificados digitales emitidos por esta autoridad certificadora interna serán los únicos válidos para ser utilizados por los empleados y funcionarios de la Comisión al momento de generar una firma en formato electrónico para ser utilizada de acuerdo a lo estipulado en el Artículo 5 de las presentes Normas.

Artículo 12. Autoridad Certificadora para las Instituciones del Sistema Supervisado y de Terceros
Existirá una autoridad certificadora para el Sistema Supervisado, subordinada a la autoridad certificadora intermedia. Esta autoridad certificadora será utilizada para emitir certificados digitales de las instituciones supervisadas; así como demás personas naturales o jurídicas, no supervisadas.

Los certificados digitales emitidos por esta autoridad certificadora serán utilizados exclusivamente por las instituciones supervisadas, y demás personas naturales o jurídicas,

no supervisadas; para generar una firma en formato electrónico a ser utilizada de acuerdo a lo estipulado en el Artículo 5 de las presentes Normas.

Artículo 13. Oficial de Registro
Las autoridades certificadoras subordinadas a la Autoridad Certificadora Intermedia deberán contar con un Oficial de Registro, el cual se encargará de recibir y gestionar las solicitudes de emisión de certificados digitales.

Todas las instituciones que forman parte del Sistema Supervisado por la Comisión, están en la obligación de contar con un Oficial de Registro. La institución deberá gestionar el acceso del Oficial de Registro a la Autoridad Certificadora para las Instituciones del Sistema Supervisado y de Terceros, a través de la Gerencia de Tecnología de Información y Comunicación de la Comisión.

La Comisión deberá contar con un Oficial de Registro que atenderá a las demás personas naturales o jurídicas no supervisadas.

CAPÍTULO IV
DE LOS CERTIFICADOS DIGITALES UTILIZADOS PARA LA FIRMA EN FORMATO ELECTRÓNICO DE LA COMISIÓN

Artículo 14. Certificados Digitales Utilizados para la Firma en Formato Electrónico de la Comisión
Se conocerán como certificados digitales utilizados para la firma en formato electrónico de la Comisión a los certificados digitales emitidos por la PKI de la Comisión, creados con el fin de generar una firma en formato electrónico a ser utilizada de acuerdo a lo estipulado en el Artículo 5 de las presentes Normas.

Artículo 15. Emisión de un Certificado Digital
El Oficial de Registro deberá implementar los controles necesarios para identificar plenamente al solicitante de un certificado digital utilizado para la firma en formato electrónico de la Comisión. En dicho proceso de identificación deberá confirmar la siguiente información:
1. En caso de ser persona natural, sus nombres y apellidos, número de identidad, si es extranjero carnet de residencia o pasaporte; en caso de ser persona jurídica, su razón social, registro tributario nacional (RTN).
2. En caso de ser empleado o funcionario de una institución supervisada, la razón social de la institución.
3. La ciudad y departamento.
4. En caso de ser persona natural, empleado o funcionario de una institución supervisada, el correo electrónico institucional; para persona jurídica, el correo electrónico de la sociedad o de su representante; y persona natural individual, el correo electrónico personal.

Una vez emitido el certificado digital utilizado para la firma en formato electrónico de la Comisión por el Oficial de Registro, éste le hará entrega del mismo al solicitante, quien pasará a ser el Poseedor del Certificado Digital.

Artículo 16. Poseedor del Certificado Digital
El Poseedor del Certificado Digital implementará los controles necesarios para mantener bajo su control exclusivo y de manera segura la llave privada que corresponde a la llave

pública del certificado digital utilizado para la firma en formato electrónico de la Comisión que recibió del Oficial de Registro.

El Poseedor del Certificado Digital está obligado a solicitar la revocación del certificado digital utilizado para la firma en formato electrónico de la Comisión en los siguientes casos:
1. En caso de pérdida o extravió de la llave privada.
2. En caso de exposición de la llave privada y peligro de uso indebido.
3. Cualquier otro evento que pueda implicar el uso indebido del certificado.

Si el Poseedor del Certificado Digital no solicita la revocación del certificado digital utilizado para la firma en formato electrónico de la Comisión y si ocurriese alguna de las situaciones anteriores descritas, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe, que confiaron en la firma en formato electrónico generada con su certificado digital.

Artículo 17. Vigencia del Certificado Digital
Cada certificado digital utilizado para la firma en formato electrónico de la Comisión tendrá una vigencia y fecha de finalización que se indicará en cada certificado digital.

Artículo 18. Revocación del Certificado Digital
La Comisión se reserva el derecho de revocar cualquier certificado digital utilizado para la firma en formato electrónico de la Comisión, previo a la verificación del uso indebido o por lo expuesto en el segundo párrafo del Artículo 16 de las presentes Normas. Lo anterior sin perjuicio de las firmas en formato electrónico generadas previo a la revocación.

CAPÍTULO V
DISPOSICIONES FINALES

Artículo 19. De la Firma Electrónica de la IFE
Las firmas electrónicas generadas bajo la IFE seguirán manteniendo su validez y eficacia jurídica a partir de la entrada en vigencia de las presentes Normas.

Artículo 20. Transitorios
La Comisión y las instituciones supervisadas podrán seguir utilizando la IFE, mientras realizan la transición al uso de la firma en formato electrónico de la Comisión.

Artículo 21. Infracciones y Sanciones
Las infracciones a lo dispuesto en las presentes Normas, serán sancionadas por la Comisión de conformidad al marco normativo vigente, emitido por esta, en materia de sanciones.

Artículo 22. Casos No Previstos
Lo no previsto en las presentes Normas será resuelto por la Comisión, de acuerdo con las disposiciones legales y normativas vigentes en el país, aplicables y con las mejores prácticas y estándares internacionales.

2. Dejar sin valor y efecto la Resolución GE No.316/27-02-2012, emitida por la Comisión Nacional de Bancos y Seguros el 27 de febrero del 2012, que contiene las Normas Reguladoras de Firmas Electrónicas Administradas por la Comisión Nacional de Bancos y Seguros.

3. Comunicar lo resuelto a la Secretaría General, Dirección de Asesoría Legal, Superintendencia de Bancos y Otras Instituciones Financieras, Superintendencia de Pensiones y Valores, Superintendencia de Seguros, Gerencia de Protección al Usuario Financiero, Gerencia de Estudios, Gerencia de Riesgos, Gerencia de Tecnología de Información y Comunicación, Gerencia Administrativa, Dirección de Planificación y Control de Gestión, Unidad de Inteligencia Financiera, Unidad de Resolución Bancaria, Unidad de Auditoria Interna de la Comisión Nacional de Bancos y Seguros, para los fines legales pertinentes.

4. Instruir a la Secretaría General de esta Comisión para que realice los trámites que correspondan para la publicación de las Normas contenidas en la presente Resolución, en el Diario Oficial La Gaceta.

5. Comunicar a las Instituciones Supervisadas la presente Resolución, para los efectos legales que correspondan.

6. La presente Resolución entrará en vigencia a partir de su publicación en el Diario Oficial La Gaceta. ... Queda aprobado por unanimidad. ... **F) ETHEL DERAS ENAMORADO,** Presidenta; **JOSÉ ADONIS LAVAIRE FUENTES,** Comisionado Propietario; **EVASIO A. ASENCIO,** Comisionado Propietario; **MAURA JAQUELINE PORTILLO G.**, Secretaria General".

COMISION NACIONAL DE BANCOS Y SEGUROS
SECRETARIA GENERAL
HONDURAS, C.A.

MAURA JAQUELINE PORTILLO G.
Secretaria General