INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL)

RESOLUCIÓN No. 021-16

QUE CONOCE LA SOLICITUD DE RECONOCIMIENTO DE CERTIFICADOS DIGITALES PRESENTADA POR LA ENTIDAD DE CERTIFICACIÓN AVANSI, S.R.L., Y LA SOCIEDAD ANF AUTORIDAD DE CERTIFICACIÓN DE CONFORMIDAD A LA LEY NO. 126-02 DE COMERCIO ELECTRÓNICO, DOCUMENTOS Y FIRMAS DIGITALES

El **Instituto Dominicano de las Telecomunicaciones (INDOTEL)**, por órgano de su Consejo Directivo, en ejercicio de las facultades conferidas por la Ley General de Telecomunicaciones, No. 153-98, por la Ley de Comercio Electrónico, Documentos y Firmas Digitales, No. 126-02 y por el Decreto No. 335-03, que aprueba el Reglamento de Aplicación de esta última, reunido válidamente previa convocatoria, dicta la presente **RESOLUCIÓN:**

Con motivo de la solicitud de **RECONOCIMIENTO RECÍPROCO DE CERTIFICADOS DIGITALES,** presentada por la entidad de certificación **AVANSI, S.R.L.**

Antecedentes.-

1. En fecha 4 de marzo de 2016 la Entidad de Certificación **AVANSI, S.R.L.** (en lo adelante "**AVANSI**") depositó la comunicación No. 150871, mediante la cual remitió al **INDOTEL** copia del Convenio de Reconocimiento Internacional de Certificados de Firma Electrónica suscrito con la sociedad **ANF AUTORIDAD DE CERTIFICACIÓN** y su filial **ANF AUTHORITY OF CERTIFICATION ECUADOR**, a fin de iniciar el procedimiento de reconocimiento de los mismos de conformidad con el artículo 59 de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales.

2. Dicha solicitud vino acompañada, de conformidad con el citado numeral 1.1.1.1 del Artículo 24 de la Norma sobre Procedimientos de Autorización y Acreditación, por la siguiente documentación:

1. Declaración de las Prácticas de Certificación (DPC);
2. Declaración de Prácticas de Certificación de ANF AC Autoridad de Sellado de Tiempo (DPC TSA);
3. Certificados de Clase 2 de Persona Física;
4. Clase 2 de Persona Jurídica y Entidad sin Personalidad Jurídica;
5. Representante Legal de Persona Jurídica, y Representante Legal de Entidad sin personalidad jurídica;
6. Certificados de Empleado Público;
7. Política de Certificación para Certificados Time Stamping Unit;
8. Política de Certificación para ANF Basic CA;
9. Política de Certificación para Certificados OSCP Clase 1 Responder;
10. Operador AR;
11. Responsables de Dictámenes de Emisión y Operadores Autorizados de la PKI;
12. Certificados de Sello Electrónico, y Sello Electrónico AAPP;
13. Política de Certificación de Certificados de Aplicación, Firma de Código y Cifrado;
14. Política de Certificación de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (SSL EV);
15. Política de Certificación de Sede Electrónica y Sede Electrónica con Validación Extendida (Sede EV); y

16. Política de Validación de Certificados.

3. En fecha 18 de octubre de 2016, fue emitido el Informe No. PR-I-000017-16, que contiene los resultados del proceso de evaluación al cual fue sometido la solicitud de reconocimiento de Certificados Digitales presentada por la Entidad de Certificación **AVANSI** y por vía del cual los técnicos del **INDOTEL** que estuvieron a cargo del indicado proceso concluyen que: *en el caso que nos ocupa no existen impedimentos para aprobar la Certificación Recíproca entre las Entidades de Certificación AVANSI, SRL., y ANF AUTORIDAD DE CERTIFICACIÓN…"*

EL CONSEJO DIRECTIVO DEL INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL), DESPUÉS DE HABER ESTUDIADO Y DELIBERADO SOBRE EL CASO:

CONSIDERANDO: Que de conformidad con el artículo 56 de la Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales, corresponde al **INDOTEL** ejercer *la función de vigilancia y control de las actividades desarrolladas por las entidades de certificación*;

CONSIDERANDO: Que en virtud de la citada función, al **INDOTEL** le corresponde *velar por el adecuado funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación y el cabal cumplimiento de las disposiciones legales y reglamentarias de la actividad,* así como *evaluar las actividades desarrolladas por las entidades de certificación autorizadas conforme a los requerimientos definidos en los reglamentos técnicos*;

CONSIDERANDO: Que el Reglamento de Aplicación de la Ley No. 126-02, sobre Comercio Electrónico, Documentos y Firmas Digitales, establece en su artículo 43 que es función del **INDOTEL** *aprobar las políticas de certificación, el manual de procedimientos, el plan de seguridad, el plan de cese de actividades y el plan de contingencia, presentados por las Entidades de Certificación que requieren autorización*;

CONSIDERANDO: Que, en ese mismo sentido, dicho Reglamento de Aplicación en su artículo 3.2 dispone que *el **INDOTEL** constituye la única institución del Estado con calidad legal para autorizar la instalación y operación de servicios públicos y privados de certificación digital en el territorio nacional, no pudiendo ser sustituida esta facultad por ninguna otra autoridad centralizada, autónoma o descentralizada del Estado*;

CONSIDERANDO: Que el Consejo Directivo del **INDOTEL** aprobó, mediante su Resolución No. 010-04 de fecha 30 de enero de 2004, las Normas Complementarias a la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales y a su Reglamento de Aplicación;

CONSIDERANDO: Que dentro de las referidas Normas Complementarias de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, fueron aprobadas la Norma sobre Procedimientos de Autorización y Acreditación y la Norma sobre Políticas y Procedimientos de Certificación;

CONSIDERANDO: Que la aplicación de criterios diferentes a los aplicables en otros países en cuanto a los efectos legales de la firma digital o cualquier diferencia en los aspectos técnicos en virtud de los cuales las firmas digitales son consideradas seguras, resultaría perjudicial para el desarrollo futuro del comercio electrónico nacional seguro; y por consiguiente, para el crecimiento económico del país y su incorporación a los mercados internacionales, cada vez más globalizados. Es importante, por ello, que exista un alto grado de homogeneidad normativa para fomentar la comunicación y la actividad empresarial por redes abiertas con los demás países del mundo;

CONSIDERANDO: Que la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales y su Reglamento de Aplicación, no ajenos a las dificultades en aplicación de criterios diferentes a los aplicables en otros países en cuanto a los efectos legales de la firma digital o cualquier diferencia en los aspectos técnicos en virtud de los cuales las firmas digitales son consideradas seguras, prevén una serie de artículos que se expresan de la siguiente manera:

> ***Certificaciones Recíprocas.*** *Los certificados digitales emitidos por entidades de certificación extranjeras podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre que tales certificados sean reconocidos por una entidad de certificación autorizada que garantice, en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia*[1]*.*
>
> ***Reconocimiento de Certificados Extranjeros.-***
>
> *38.1. Las Entidades de Certificación podrán reconocer los certificados digitales emitidos por Entidades de Certificación extranjeras, bajo su responsabilidad.*
>
> *38.2. Para ello la Entidad de Certificación demostrará al INDOTEL que los certificados a ser reconocidos por ella, han sido emitidos por un prestador de servicios de certificación no establecido en República Dominicana que cumple con normas técnicas y de procedimientos equivalentes a las establecidas en la Ley, este Reglamento, sus normas complementarias y modificaciones, para el desarrollo de la actividad. En particular, deberá acreditar que los certificados a ser reconocidos por ella, cumplen las disposiciones referentes a contenidos mínimos de los certificados, establecidas en la Ley, este Reglamento y las normas emitidas por el INDOTEL.*
>
> *38.3. El INDOTEL verificará el cumplimiento de las disposiciones legales y reglamentarias, y publicará la información sobre el reconocimiento en el Registro de Entidades de Certificación. En caso de que la Entidad de Certificación no acredite el cumplimiento de los recaudos legales y reglamentarios para el reconocimiento de certificados extranjeros, el INDOTEL mediante resolución motivada, rechazará la solicitud de reconocimiento.*
>
> *38.4. Una vez practicado el reconocimiento la Entidad de Certificación, en un plazo de TRES (3) días hábiles, comunicará tal situación al INDOTEL y la publicará, inmediatamente en un plazo máximo de VEINTICUATRO (24) horas, en el Registro de acceso público contemplado en el Artículo 51 de la Ley.*
>
> *38.5. El reconocimiento de certificados deberá estar declarado en las Prácticas de Certificación*[2]*.*

CONSIDERANDO: Que en la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, y también en otras legislaciones internacionales sobre las firmas digitales en el comercio mundial, existen disposiciones no discriminatorias similares a las del artículo 59 de la citada Ley No.

[1] Artículo 59 de la Ley de Comercio Electrónico.

[2] Artículo 38 del Reglamento de Aplicación de la Ley de Comercio Electrónico.

126-02[3]. Dichas disposiciones reconocen que la efectividad jurídica de un certificado o una firma digital deben depender de su fiabilidad técnica[4];

CONSIDERANDO: Que, en consecuencia, si el certificado digital extranjero expedido presenta *"un grado de fiabilidad sustancialmente equivalente"* al de un certificado expedido en el Estado promulgante, tendrá *"los mismos efectos jurídicos"*. De igual modo, una firma digital creada o utilizada fuera del país *"producirá los mismos efectos jurídicos"* que una firma digital creada o utilizada en el país *"si presenta un grado de fiabilidad sustancialmente equivalente"*[5];

CONSIDERANDO: Que la equivalencia entre los grados de fiabilidad presentados por los certificados y firmas nacionales y extranjeros ha de ser determinada en conformidad con normas internacionales reconocidas y cualquier otro factor pertinente, en particular un acuerdo entre las partes para utilizar ciertos tipos de firmas o certificados digitales, a no ser que el acuerdo carezca de validez o efectividad con arreglo al derecho aplicable;

CONSIDERANDO: Que en el estudio realizado por el Grupo de Trabajo de la Organización de Cooperación y Desarrollo Económicos (OCDE) sobre la seguridad de la información y la protección de la vida privada se determinó que, en la mayoría de los marcos legislativos, como mínimo no se discriminaba en principio los métodos de firma y autenticación electrónicas de origen extranjero –siempre que se cumplieran requisitos nacionales o sus equivalentes, en el sentido de que no restaran eficacia jurídica a las firmas relacionadas con servicios originarios de los países– y que esas firmas se hubieran creado en las mismas condiciones que las reconocidas con arreglo al derecho interno[6];

CONSIDERANDO: Que el reconocimiento de los certificados digitales extranjeros se realiza a menudo mediante un método llamado "Certificación Recíproca". En tal caso, es necesario que Entidades de Certificación fundamentalmente equivalentes (o Entidades de Certificación dispuestas a asumir ciertos riesgos con respecto a los certificados expedidos por otras entidades de certificación) reconozcan los servicios prestados por cada cual, de manera que sus usuarios respectivos puedan comunicarse entre sí con mayor eficacia y más confianza en la fiabilidad del certificado que se expida;

CONSIDERANDO: Que la Certificación Recíproca es la práctica de reconocer la Infraestructura de Claves Pública de otro prestador de servicios de certificación por referencia a un nivel convenido de confianza, habitualmente en virtud de un contrato. Esta supone la interoperabilidad técnica y la armonización de las prácticas y políticas de certificación. Esta armonización resulta necesaria para asegurar que los dominios de la Infraestructura de Claves Públicas sean compatibles tanto en términos de sus operaciones de gestión de certificados (o sea, su expedición, suspensión y revocación) como en su observancia de prescripciones operativas y de seguridad análogas;

CONSIDERANDO: Que de la lectura de los artículos 59 de la Ley No. 126-02 y 38 del Reglamento de Aplicación precitados podemos establecer las siguientes previsiones para los casos en los cuales una Entidad de Certificación desee reconocer los Certificados Digitales emitidos por Entidades de Certificación extranjeras:

---

[3] Ver el Código de los Estados Unidos, título 15, capítulo 96, artículo 7031 (Principios que rigen la utilización de las firmas electrónicas en las operaciones internacionales), el Artículo 16 de la Ley 25.506 de Firma Digital de Argentina, el artículo 13 de la Ley No. 8454 de Certificados, Firmas Digitales y Documentos Electrónicos de Costa Rica y el artículo 11 de la Ley No. 27269 de Firmas y Certificados Digitales del Perú, entre otros.

[4] *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas*..., segunda parte, párr. 83.

[5] Ibíd. párr. 83.

[6] Organización de Cooperación y Desarrollo Económicos, Grupo de Trabajo sobre la seguridad de la información y la protección de la vida privada, "*The Use of Authentication across Borders in OECD Countries*" (DSTI/ICCP/REG(2005)4/FINAL), disponible en http://www.oecd.org/internet/ieconomy/35809749.pdf

1. Los Certificados Digitales extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos para Certificados Digitales nacionales, siempre que se garantice la regularidad de los detalles del certificado, así como su validez y vigencia;

2. En el caso que nos ocupa **AVANSI** debe demostrar al **INDOTEL** que los certificados a ser reconocidos por ella cumplen con las normas técnicas y de procedimientos equivalentes a las establecidas en la Ley, el Reglamento y sus normas complementarias; y

3. El **INDOTEL** verificará el cumplimiento de las disposiciones legales y reglamentarias y mediante resolución motivada aprobará o rechazará la solicitud de reconocimiento.

CONSIDERANDO: Que en lo que concierne la demostración del cumplimiento de la normativa legal y reglamentaria de los certificados extranjeros, el Artículo 24 de la Norma de Autorización y Acreditación establece en su numeral 1.1.1.1 que al momento de una Entidad de Certificación solicitar autorización para reconocer certificados digitales emitidos por Entidades de Certificación Extranjeras deberá someter la **INDOTEL** la siguiente información:

a) Políticas de Certificación de la Entidad de Certificación Extranjera;

b) Manual de Procedimientos de la Entidad de Certificación Extranjera;

c) Plan de Cese de Actividades de la Entidad de Certificación Extranjera;

d) Plan de Contingencia de la Entidad de Certificación Extranjera;

e) Política de Protección de Datos Personales de la Entidad de Certificación Extranjera;

f) Toda otra documentación que permita demostrar que la Entidad de Certificación Extranjera cumple con normas técnicas y de procedimientos equivalentes a las establecidas por la Ley, el Reglamento, sus normas complementarias y sus modificaciones;

g) Datos de información general de la Entidad de Certificación Extranjera: nombre, domicilio, números de teléfono, de facsímil y dirección de correo electrónico; y

h) Datos de la personería de la Entidad de Certificación Extranjera.

CONSIDERANDO: Que el 4 de marzo de 2016 la Entidad de Certificación **AVANSI** depositó la comunicación No. 150871, mediante la cual remitió al **INDOTEL** copia del Convenio de Reconocimiento Internacional de Certificados de Firma Electrónica suscrito con la sociedad **ANF AUTORIDAD DE CERTIFICACIÓN** y su filial **ANF AUTHORITY OF CERTIFICATION ECUADOR**, a fin de iniciar el procedimiento de reconocimiento de los mismos de conformidad con el artículo 59 de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales;

CONSIDERANDO: Que dicha solicitud vino acompañada, de conformidad con el citado numeral 1.1.1.1 del Artículo 24 de la Norma sobre Procedimientos de Autorización y Acreditación, por la siguiente documentación:

1. Declaración de las Prácticas de Certificación (DPC);
2. Declaración de Prácticas de Certificación de ANF AC Autoridad de Sellado de Tiempo (DPC TSA);

3. Certificados de Clase 2 de Persona Física;
4. Clase 2 de Persona Jurídica y Entidad sin Personalidad Jurídica;
5. Representante Legal de Persona Jurídica, y Representante Legal de Entidad sin personalidad jurídica;
6. Certificados de Empleado Público;
7. Política de Certificación para Certificados Time Stamping Unit;
8. Política de Certificación para ANF Basic CA;
9. Política de Certificación para Certificados OSCP Clase 1 Responder;
10. Operador AR;
11. Responsables de Dictámenes de Emisión y Operadores Autorizados de la PKI;
12. Certificados de Sello Electrónico, y Sello Electrónico AAPP;
13. Política de Certificación de Certificados de Aplicación, Firma de Código y Cifrado;
14. Política de Certificación de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (SSL EV), Sede Electrónica, y Sede Electrónica con Validación Extendida (Sede EV); y
15. Política de Validación de Certificados.

CONSIDERANDO: Que con motivo de la solicitud presentada por **AVANSI** a fin de iniciar el procedimiento de reconocimiento de los mismos de conformidad con el artículo 59 de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, este órgano regulador procedió a realizar los análisis de la información, estudios y comprobaciones necesarias, a fin de poder determinar la factibilidad de la solicitud;

CONSIDERANDO: Que en fecha 18 de octubre de 2016 fue emitido el Informe No. PR-I-000017-16, que contiene los resultados del proceso de evaluación al cual fue sometido la solicitud de reconocimiento de Certificados Digitales presentada por la Entidad de Certificación **AVANSI** y por vía del cual los técnicos del **INDOTEL** que estuvieron a cargo del indicado proceso concluyen de la manera siguiente:

> *En virtud de todo cuanto ha sido indicado previamente en este informe, quien suscribe es de criterio de que en el caso que nos ocupa no existen impedimentos para aprobar la Certificación Recíproca entre las Entidades de Certificación AVANSI, SRL., y ANF AUTORIDAD DE CERTIFICACIÓN en cuanto a las siguientes Prácticas y Políticas de Certificación:*
>
> 1. *Declaración de las Prácticas de Certificación (DPC);*
> 2. *Certificados de Clase 2 de Persona Física;*
> 3. *Clase 2 de Persona Jurídica y Entidad sin Personalidad Jurídica;*
> 4. *Representante Legal de Persona Jurídica, y Representante Legal de Entidad sin personalidad jurídica;*
> 5. *Certificados de Empleado Público;*
> 6. *Política de Certificación para ANF Basic CA;*
> 7. *Política de Certificación para Certificados OSCP Clase 1 Responder;*
> 8. *Operador AR; y*
> 9. *Responsables de Dictámenes de Emisión y Operadores Autorizados de la PKI.*
>
> *Por otra, parte en lo que respecta a la Declaración de Prácticas de Certificación de ANF AC Autoridad de Sellado de Tiempo; la Política de Certificación para Certificados Time Stamping Unit; la Política de Certificación de Certificados de Aplicación, Firma de Código y Cifrado; la Política de Certificación de Certificados de Sello Electrónico, y Sello Electrónico AAPP; la Política de Certificación de Certificados de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (SSL EV), Sede Electrónica, y Sede Electrónica con Validación Extendida (Sede EV); y la Política de Validación de*

Certificados actualmente el marco normativo Dominicano no cuenta el soporte necesario para la oferta de dichos servicios. En consecuencia, recomendamos que el reconocimiento de los mismos no sea aprobado hasta tanto no se actualice dicho marco normativo. [7]

CONSIDERANDO: Que, en virtud de las consideraciones expuestas previamente, este Consejo Directivo del **INDOTEL** entiende procedente otorgar a **AVANSI** la autorización correspondiente, bajo los términos y condiciones establecidos en la presente resolución, a fin de que ésta pueda reconocer los Certificados Digitales de la Entidad de Certificación **ANF AUTORIDAD DE CERTIFICACIÓN** y su filial **ANF AUTHORITY OF CERTIFICATION ECUADOR**, de conformidad con el artículo 59 de la Ley No. 126-02;

VISTA: La Ley General de Telecomunicaciones, No. 153-98, de fecha 27 de mayo de 1998;

VISTA: La Ley de Comercio Electrónico, Documentos y Firmas Digitales, No. 126-02, de fecha 4 de septiembre de 2002, en sus disposiciones citadas;

VISTO: El Reglamento de Aplicación de la Ley No. 126-02, aprobado por el Decreto No. 335-03, de fecha 8 de abril de 2003;

VISTA: La Resolución No. 042-03, dictada por el Consejo Directivo del **INDOTEL** en fecha 17 de marzo de 2003;

VISTA: La Resolución No. 10-04, dictada por el Consejo Directivo del **INDOTEL** en fecha 30 del mes de enero de 2004, mediante la cual se aprueba la Norma Complementaria de la Ley No. 126-02 sobre Procedimientos de Autorización y Acreditación y la Norma sobre Políticas y Procedimientos de Certificación;

VISTA: La solicitud de fecha 4 de marzo de 2016 de la Entidad de Certificación **AVANSI, S.R.L.**, mediante la cual solicita iniciar el procedimiento de reconocimiento de los mismos de conformidad con el artículo 59 de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales;

VISTOS: Los documentos sobre Declaración de las Prácticas de Certificación (DPC), Declaración de Prácticas de Certificación de ANF AC Autoridad de Sellado de Tiempo (DPC TSA), Políticas de Certificación para Certificados de Clase 2 de Persona Física, Políticas de Certificación Clase 2 de Persona Jurídica y Entidad sin Personalidad Jurídica, Políticas de Certificación para Representante Legal de Persona Jurídica, y Representante Legal de Entidad sin personalidad jurídica, Políticas de Certificación para Certificados de Empleado Público, Políticas de Certificación para Certificados Time Stamping Unit, Política de Certificación para ANF Basic CA, Política de Certificación para Certificados OSCP Clase 1 Responder, Políticas de Certificación para Operador AR, Políticas de Certificación para Responsables de Dictámenes de Emisión y Operadores Autorizados de la PKI, Políticas de Certificación para Certificados de Sello Electrónico, y Sello Electrónico AAPP, Políticas de Certificación de Certificados de Aplicación, Firma de Código y Cifrado, Política de Certificación de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (SSL EV), Política de Certificación de Sede Electrónica y Sede Electrónica con Validación Extendida (Sede EV), y Política de Validación de Certificados;

[7] Al respecto es preciso señalar que en base a la normativa vigente, en particular la Norma Complementaria de la Ley No. 126-02 sobre Políticas y Procedimientos de Certificación, actualmente no se cuenta con la base regulatoria para aprobar dichas prácticas y políticas de certificación.

VISTO: El Informe No. PR-I-000005-16, sobre la Solicitud de Reconocimiento de Certificados Digitales entre las Entidades de Certificación **AVANSI** y **ANF AUTORIDAD DE CERTIFICACIÓN**;

VISTAS: Las demás piezas que componen el expediente sobre la Solicitud de Reconocimiento de Certificados Digitales entre las Entidades de Certificación **AVANSI** y **ANF AUTORIDAD DE CERTIFICACIÓN**;

EL CONSEJO DIRECTIVO DEL INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL), EN EJERCICIO DE SUS FACULTADES LEGALES Y REGLAMENTARIAS,

RESUELVE:

PRIMERO: AUTORIZAR la Certificación Recíproca entre las Entidades de Certificación **AVANSI, SRL.,** y **ANF AUTORIDAD DE CERTIFICACIÓN,** por haber cumplido con los requisitos legales y reglamentarios establecidos por la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, y su Reglamento de Aplicación y las Normas Complementarias, a fin de que se reconozcan para su uso en República Dominicana los Certificados Digitales que se listan a continuación:

a. Declaración de las Prácticas de Certificación (DPC);
b. Certificados de Clase 2 de Persona Física;
c. Clase 2 de Persona Jurídica y Entidad sin Personalidad Jurídica;
d. Representante Legal de Persona Jurídica, y Representante Legal de Entidad sin personalidad jurídica;
e. Certificados de Empleado Público;
f. Política de Certificación para ANF Basic CA;
g. Política de Certificación para Certificados OSCP Clase 1 Responder;
h. Operador AR; y
i. Responsables de Dictámenes de Emisión y Operadores Autorizados de la PKI.

SEGUNDO: SOBRESEER, hasta tanto no se cuente con el soporte necesario en la normativa nacional, la autorización de la Certificación Recíproca entre las Entidades de Certificación **AVANSI, SRL.,** y **ANF AUTORIDAD DE CERTIFICACIÓN,** las siguientes prácticas y políticas de certificación:

a. Declaración de Prácticas de Certificación de ANF AC Autoridad de Sellado de Tiempo;
b. Política de Certificación para Certificados Time Stamping Unit;
c. Política de Certificación de Certificados de Aplicación, Firma de Código y Cifrado;
d. Política de Certificación de Certificados de Sello Electrónico, y Sello Electrónico AAPP;
e. Política de Certificación de Certificados de Servidor Seguro SSL, Servidor Seguro SSL con Validación Extendida (SSL EV), Sede Electrónica, y Sede Electrónica con Validación Extendida (Sede EV); y
f. Política de Validación de Certificados.

TERCERO: ORDENAR a la Directora Ejecutiva del **INDOTEL,** de conformidad con lo dispuesto por el artículo 46 del Reglamento de Aplicación de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, la actualización del Registro de Entidades de Certificación para que conste la autorización de la certificación recíproca

entre las Entidades de Certificación **AVANSI, SRL.,** y **ANF AUTORIDAD DE CERTIFICACIÓN.**

CUARTO: ORDENAR a **AVANSI, SRL.,** la inclusión en sus Prácticas de Certificación el señalamiento que reconocen los Certificados Digitales de **ANF AUTORIDAD DE CERTIFICACIÓN** de acuerdo a lo dispuesto por el artículo 38.5 del Reglamento de Aplicación de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales.

QUINTO: ORDENAR a la Directora Ejecutiva del **INDOTEL** la notificación de una copia certificada de la presente resolución a la **AVANSI,** así como su publicación en el Boletín Oficial del **INDOTEL** y en la página Web que mantiene esta institución en la red de Internet.

Así ha sido aprobada, adoptada y firmada la presente Resolución a unanimidad de votos por el Consejo Directivo del **Instituto Dominicano de las Telecomunicaciones (INDOTEL)**, en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, hoy día siete (7) del mes de diciembre del año dos mil dieciséis (2016).

Firmados:

José Del Castillo Saviñón
Presidente del Consejo Directivo

Yván L. Rodríguez
En representación del Ministro de Economía Planificación y Desarrollo Miembro ex oficio del Consejo Directivo

Marcos Peña Rodríguez
Miembro del Consejo Directivo

Fabricio Gómez M.
Miembro del Consejo Directivo

Nelson Guillén Bello
Miembro del Consejo Directivo

Katrina Naut
Directora Ejecutiva
Secretaria del Consejo Directivo