MODELO DE CONFIANZA PARA FIRMA ELECTRÓNICA CERTIFICADA

(Versión 2)

OID: 2.16.558.0.4.0

Managua, Julio 2020

MINISTERIO DE HACIENDA Y CREDITO PUBLICO
DIRECCION GENERAL DE TECNOLOGIA

CUADRO DE REVISIONES

No. Revisión	Fecha	Elaborado/ Entrevistado	Revisado	Autorizado	Aprobado
0	Diciembre / 2013	Hans Espinoza Acuña Responsable Dirección Acreditación de Firma Electrónica	Yuri Dompe Responsable Departamento Supervisión e Inspección Daysi Romero Responsable Departamento de Acreditación y Registro	Ana Patricia Aguilera Responsable Dirección de Normas y Planes Tecnológicos	Esperanza Meza Responsable Dirección General de Tecnología
1	Julio / 2016	Hans Espinoza Acuña Responsable Dirección Acreditación de Firma Electrónica	Yuri Dompe Responsable Departamento Supervisión e Inspección Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Acuña Responsable Dirección Acreditación de Firma Electrónica	Esperanza Meza Responsable Dirección General de Tecnología
2	Julio / 2020	Daysi Romero Responsable Departamento de Acreditación y Registro	Hans Espinoza Acuña Responsable Dirección Acreditación de Firma Electrónica Yuri Dompe Responsable Departamento Supervisión e Inspección	Hans Espinoza Acuña Responsable Dirección Acreditación de Firma Electrónica	Elba Mercedes García Responsable Dirección General de Tecnología(a.i)

CONTENIDO

I. INTRODUCCIÓN

La Dirección General de Tecnología - DGTEC del Ministerio de Hacienda y Crédito Público a través de la Dirección de Acreditación de Firma Electrónica ha elaborado el documento "Modelo de Confianza para Firma Electrónica Certificada".

El presente documento es una norma técnica que regula el modelo de confianza que regirá en la Infraestructura Nicaragüense de Clave Pública a la cual se someten los Proveedores de Servicios de Certificación - PSC autorizados por la DGTEC y servirá de base y consulta para la población usuaria interesada en conocer el modelo de confianza de firma electrónica certificada en territorio nicaragüense.

II. JUSTIFICACIÓN

Sección a actualizar	**Justificación**	**Servidor Público/Cargo que solicitó la actualización**
Todo el documento	Se realizó ajustes en la numeración de la estructura.	Daysi Romero - Resp. Departamento de Acreditación y Registro.
Capítulo IV: Referencia Normativas.	Se trasladó al Capítulo III. Base Legal el Capítulo IV. Referencias Normativas. Se eliminó algunas referencias de estándares. Se agregó alguna referencia nueva a estándares.	Hans Espinoza - Resp. Dirección Acreditación de Firma Electrónica. Daysi Romero - Resp. Departamento de Acreditación y Registro. Yuri Dompe - Resp. Dpto. de supervisión e Inspección.
Capítulo V: Siglas y Glosario	Se agregó este nuevo Capítulo	
Capítulo VI: Modelo de Confianza Con Firma Electrónica Certificada.	Se actualizó nombres de algunos títulos, el contenido y representación gráficas.	
VII. Anexos	Se eliminó este Capítulo.	

III. OBJETIVO

Establecer la regulación del Modelo de Confianza para Firma Electrónica Certificada que regirá en la Infraestructura Nicaragüense de Clave Pública.

IV. BASE LEGAL

- Ley No.729 Ley de Firma Electrónica, publicada en la Gaceta Diario Oficial No. 165 el 30 de agosto del 2010:

  - Art.15 Entidad Rectora de Acreditación de Firma Electrónica: Se designa a la Dirección General de Tecnología, conocida en adelante como DGTEC, dependencia del Ministerio de Hacienda y Crédito Público, como Ente Rector del proceso de acreditación de firma electrónica.

- Reglamento de Ley 729, Decreto Presidencial 57-2011 publicado en la Gaceta Diario Oficial No. 211 el 8 de noviembre del 2011:

  - Artículo 9, inciso 1: "Definir a través de normas técnicas el modelo de confianza y aspectos relacionados para la emisión de Firmas Electrónicas Certificadas en territorio nicaragüense".

- Art. 14, establece que “Las normas técnicas que dicte la entidad rectora, para la aplicación e implementación del presente reglamento son de obligatorio cumplimiento para los Proveedores de Servicios de Certificación (PSC) y los usuarios de los mismos”.

V. ACRONIMOS Y GLOSARIO

Los siguientes acrónimos son definidos o complementados en esta normativa:

ACRN: Autoridad de Certificación Raíz Nicaragüense.

ETSI: Instituto Europeo de Estándares de Telecomunicaciones.

INCP: Infraestructura Nicaragüense de Clave Pública.

ISO: Organización Internacional de Estandarización.

OID: Identificadores de Objeto.

UIT: Unión Internacional de Telecomunicaciones.

El siguiente término es definido o complementado en esta normativa:

Esquema: Término genérico aplicado a cualquier proceso organizado de supervisión, monitoreo, aprobación o prácticas, que tengan la intención de aplicar la supervisión con el objetivo de garantizar el cumplimiento de criterios específicos para mantener la confianza en los servicios bajo el alcance del Esquema.

Los siguientes términos se encuentran definidos en la Ley No.729 Ley de Firma Electrónica:

Certificado: Certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de esta.

Firma Electrónica: Son datos electrónicos integrados en un mensaje de datos o lógicamente asociados a otros datos electrónicos que puedan ser utilizados para identificar al titular en relación con el mensaje de datos e indicar que el titular aprueba la información contenida en el mensaje de datos.

Firma Electrónica Certificada: Es la que permite identificar al titular y ha sido creada por medios que este mantiene bajo su exclusivo control de manera que vinculada al mismo y a los datos a los que se refiere permite que sea detectable cualquier modificación ulterior a estos.

Proveedor de Servicios de Certificación - PSC: Entidades que otorgan, registran, mantienen y publican los Certificados de Firma Electrónica, para lo cual generan, reconocen y revocan claves en forma expedita y segura, siendo personas jurídicas que pueden prestar otros servicios relacionados con la firma electrónica.

Los siguientes términos se encuentran definidos en el Reglamento de la Ley No. 729 Ley de firma electrónica, Decreto No. 57-2011:

Autoridad de Certificación (AC): Son aquellas a las cuales uno o más usuarios han confiado la creación y asignación de Certificados de firma electrónica certificada.

Los siguientes términos se encuentran definidos en la Recomendación UIT-T X.509 | Estándar Internacional ISO/IEC 9594-8[1]:

Ancla de Confianza: Una entidad en la que confía una Parte que Confía y se utiliza para validar Certificados de Clave Pública.

Autoridad de Certificación - AC: Una autoridad en la que confían una o más entidades para crear y firmar digitalmente Certificados de Clave Pública.

Autoridad de Registro - AR: Aquellos aspectos de las responsabilidades de una Autoridad de Certificación que están relacionados con la identificación y autenticación del sujeto de un Certificado de Clave Pública que emitirá dicha Autoridad De Certificación. Una AR puede ser una entidad separada o ser una parte integrada de la Autoridad de Certificación.

Certificado o Certificado de Clave Pública: La Clave Pública de una entidad, junto con otra información, hecha infalsificable mediante la firma digital con la Clave Privada de la Autoridad de Certificación que la emitió.

Certificado de Entidad Final o Certificado de Clave Pública de Entidad Final: Es un Certificado de Clave Pública emitido a una entidad, que luego actúa como una Entidad Final dentro de una Infraestructura de Clave Pública.

Clave Pública: Es la clave, de un par de claves de una entidad, que es conocida públicamente.

Clave Privada: Es la clave, de un par de claves de una entidad, que solo es conocida por esa entidad.

Confianza: Es la firme creencia en la fiabilidad y la veracidad de la información o en la capacidad y disposición de una entidad para actuar de manera apropiada, dentro de un contexto específico.

Confianza en una AC: Creencia de que la Autoridad De Certificación actuará con fiabilidad y veracidad en la gestión de sus Certificados de Clave Pública y cumplirá con su declaración de práctica de certificación publicada y la legislación pertinente.

Confianza en un Certificado de Clave Pública: Creencia de que el Certificado de Clave Pública pertenece al sujeto identificado en el Certificado de Clave Pública.

Declaración de Practicas de Certificación - DPC: Es una declaración de las prácticas que una Autoridad de Certificación emplea en la emisión de Certificados.

Entidad Final: Es un titular o sujeto de Certificado de Clave Pública que utiliza su Clave Privada para fines distintos a la firma de Certificados de Clave Pública.

Infraestructura de Clave Pública - ICP: Una infraestructura capaz de soportar la gestión de Claves Públicas capaces de soportar servicios de autenticación, cifrado, integridad o no repudio.

Parte que Confía: Una entidad que se basa en los datos de un Certificado de Clave Pública para tomar decisiones.

Política de Certificado - PC: Un conjunto de reglas con nombre que indica la aplicabilidad de un Certificado de Clave Pública a una comunidad y / o clase de aplicación en particular con requisitos de seguridad comunes.

1 Recomendación UIT-T X.509 | Estándar Internacional ISO/IEC 9594-8:2017, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks.

VI. MODELO DE CONFIANZA CON FIRMA ELECTRÓNICA CERTIFICADA

1. Consideraciones Generalidades

1.1. Infraestructura de Clave Pública - ICP

La Dirección General de Tecnología como Ente Rector de Firma Electrónica designa la infraestructura tecnológica para la gestión de firmas electrónicas certificadas a la Infraestructura de Claves Públicas.

La ICP es la combinación de **tecnología** (hardware y software), **procesos** (políticas, prácticas y procedimientos) y **componentes legales** (acuerdos, convenios, leyes) que vinculan la identidad del titular de la clave privada con su clave pública correspondiente, utilizando la tecnología de criptografía asimétrica.

Dicha tecnología, procesos y componentes legales están en correspondencia con la Ley 729 de Firma Electrónica, su Reglamento y las disposiciones dictadas por el Ente Rector de Firma Electrónica.

Una ICP proporciona **Confidencialidad** con el cifrado de las comunicaciones y almacenamiento de datos; **Autenticación** de la identidad de una persona u organización; **Integridad** de mensajes y de datos, y soporte para el **No repudio** de las transacciones o mensajes.

Una representación simple de una Infraestructura de Clave Pública - ICP se resume en la siguiente figura:

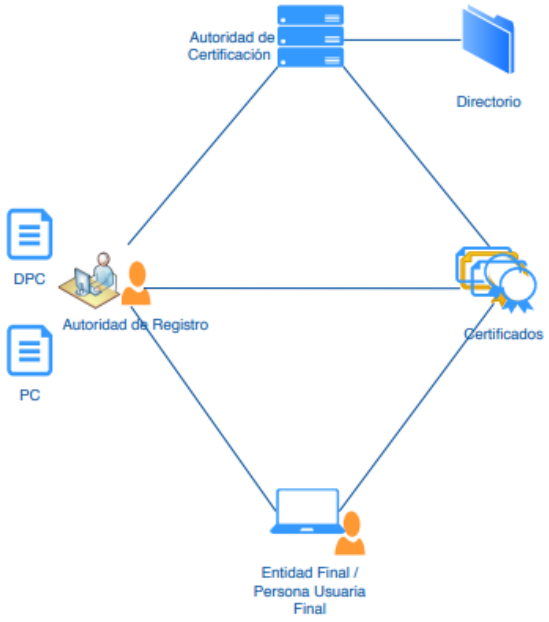

Figura 1: Representación Simple de ICP.

La DPC y PC de cada PSC, describen el funcionamiento entre los elementos mencionados en esta figura.

1.2. Infraestructura de Clave Pública y la Confianza

Desde el punto de vista de la confianza una ICP se describe como un conjunto de **tecnologías**, **procesos** y **componentes legales** para la propagación de la confianza desde donde inicialmente existe, hasta donde sea necesario para la autentificación en entornos en línea. La manera en que se realiza la propagación de la confianza bajo una ICP en específico, depende del **esquema** adoptado por la ICP.

1.3. Bases de la Seguridad y de la Confianza

La confianza resulta de la seguridad de que un Proveedor de Servicios de Certificación - PSC es gestionado correctamente y de que sus servicios se prestan de manera segura es decir que la tecnología y las practicas del PSC han sido certificada y autorizadas por el Ente Rector. Por ello deberá garantizarse que el propio PSC y sus servicios están de acuerdo con las políticas definidas. La política de seguridad especialmente debe abarcar todos los aspectos de la seguridad relacionados con la gestión del PSC y la prestación de los servicios.

La confianza puede establecerse por la evidencia de los aspectos del PSC relacionados con la gestión y el funcionamiento. Deberá evidenciarse que los aspectos de la gestión son los adecuados y suficientes para alcanzar plenamente los objetivos, que el sistema de gestión es eficaz y apropiado para reducir al mínimo los riesgos y contrarrestar los peligros, y que las medidas están documentadas y las conoce el personal, no han quedado obsoletas ni invalidada y se implementan correctamente.

Para ganar confianza en los aspectos relativos a la gestión y el funcionamiento de un PSC deberá sobre todo aportar evidencia en el sentido de que:

- Se ha establecido una política de seguridad adecuada;
- Las soluciones de los problemas de seguridad se han abordado mediante una combinación de procedimientos y mecanismos de seguridad implementados correctamente;
- El funcionamiento se lleva a cabo correctamente y asignando un conjunto claramente definido de objetivos y responsabilidades;
- Las interfaces y procedimientos de comunicación con entidades son adecuados a las funciones que han de realizarse y se utilizan correctamente;
- La gestión y el personal siguen las reglas y regulaciones con un nivel elevado de responsabilidad establecido o fijado como objetivo;
- La calidad de los procesos, las operaciones y las prácticas de trabajo ha sido acreditada adecuadamente;
- El PSC cumple sus obligaciones contractuales de acuerdo con un contrato formal acordado con las personas usuarias;
- Hay un conocimiento y una aceptación clara de los aspectos relativos a la responsabilidad civil;
- Se mantiene y verifica el cumplimiento de las leyes y regulaciones;
- Están claramente identificados los peligros conocidos y las medidas para mitigar dichos peligros;
- Se realiza inicialmente una evaluación de peligros y riesgos, y se revisa y actualiza periódicamente esta evaluación para garantizar que se cumplen los requisitos de confidencialidad, integridad, disponibilidad y fiabilidad;
- Se cumplen las medidas organizativas y de personal;
- Puede contarse con la confianza del PSC y dicha confianza se puede comprobar y verificar; y
- El PSC es supervisado por el Ente Rector que vigila que su funcionamiento se mantiene dentro de las reglas de su acreditación.

1.4. Aspectos legales para la Confianza

Un PSC heredará amplias responsabilidades derivadas de las expectativas de sus personas usuarias. Estas responsabilidades incluirán disposiciones sin fisuras con relación a la confidencialidad, integridad, disponibilidad, control de acceso, rendición de cuentas; autenticidad, fiabilidad, privacidad, aspectos éticos (como el uso legítimo), aspectos legales (esto es, leyes y reglamentos), técnicas y mecanismos, y aspectos financieros. El no cumplimiento accidental o deliberada de estas responsabilidades por parte de un PSC puede ocasionar pérdidas substanciales a sus personas usuarias, los cuales tratarán de recuperarlas del PSC.

Para gestionar las expectativas de sus personas usuarias y limitar su responsabilidad civil, debe establecerse un contrato claramente definido y legalmente vinculante entre el PSC y sus personas usuarias.

Este contrato debe recoger como mínimo los aspectos legales relativos a los siguientes temas:

- Responsabilidad civil;
- Privacidad, sobre todo en relación con la ley de protección de datos;
- Marcas registradas y propiedad intelectual;
- Uso de la criptografía;
- Legalidad de un servicio vinculante, tal como las Firmas Electrónicas Certificadas;
- Derecho de investigar, por ejemplo, la cedula de identidad u otra información proporcionada por el solicitante de servicio;
- Requisitos legislativos y reglamentarios aplicables a la jurisdicción y la industria;
- Los tipos de servicio que han de prestarse;
- Disposiciones de acceso, incluidos los métodos de acceso permitidos y los procedimientos de autorización de personas usuarias (y de cambio de personas usuarias autorizadas);
- Procedimientos de resolución de problemas (incluidos los puntos de contacto autorizados);
- Responsabilidades concernientes a los requisitos de soporte físico y soporte lógico, la gestión y el control de los cambios;
- Disposiciones sobre la ejecución de informes, la notificación y la investigación de los incidentes relacionados con la seguridad.
- Longevidad o posterior consulta, los PSC pueden tener que presentar pruebas de certificaciones muchos años después de se hayan emitido;
- Disposiciones para proteger su propia Clave Privada;
- Disposiciones para suspender sus actividades, incluida la notificación a los usuarios;
- Capacidad de revocación de claves en caso de riesgos de seguridad;
- Experiencia en tecnologías de Clave Pública y familiaridad con procedimientos de seguridad apropiados.

1.5. Modelo de Confianza Generalizado

1.5.1. Componentes del Modelo de Confianza

Se facilita a las personas usuarias comparar y aceptar a Proveedores de Servicios de Certificación y sus servicios (como por ejemplo los certificados de Firma Electrónica) cuando estos se rigen por los componentes (Ver Figura 2) que permiten construir la confianza como son:

- Un conjunto de requisitos publicados para cualquiera que pretenda operar como PSC.
- Los criterios de aprobación del PSC aplicados por evaluadores/auditores.
- Medios para proporcionar información sobre el estado del PSC.

Los requisitos para operar como PSC son definidos, elaborados y actualizados por el Ente Rector en su marco normativo y publicados en La Gaceta Diario Oficial, sin perjuicio de su publicación en el portal electrónico de la Entidad Rectora de conformidad a lo establecido en el Reglamento de la Ley 729.

Los criterios que se den por parte de Evaluadores/Auditores para la aprobación de un PSC, estarán apegados a las normativas, procedimientos y estándares de operación que establezca la Ley y el Ente Rector. Los resultados de las evaluaciones serán la base principal para la elaboración de las resoluciones que emita el Ente Rector, las cuales se publicarán tanto en el portal electrónico del Ente Rector como en el sitio web del PSC; de igual manera los PSC deberán publicar las certificaciones ISO, Webtrust[2],u otra reconocida por el Ente Rector. La autorización otorgada por el Ente Rector únicamente contendrá la resolución que lo autoriza a operar como PSC en Nicaragua, el cual deberá ser publicada en La Gaceta, Diario Oficial, así como en el portal electrónico de la Entidad Rectora.

La información sobre el estado de los PSC será visible a través del portal electrónico del Ente Rector u otro servicio propio del esquema.

En la Figura 2, se muestra la utilización de manera general de los componentes mencionados, tomando en consideración que la confianza es una relación direccional entre dos partes, que pueden ser llamadas la “parte que confía” y la “parte a la que se confía” (Sujeto).

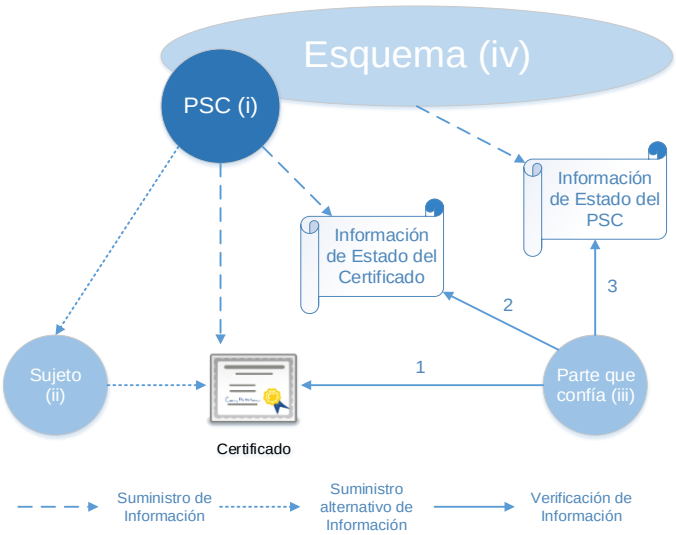

Figura 2: Modelo de Confianza Generalizado.

[2] Es un sello de confianza, calidad y seguridad reconocido internacionalmente por evaluar específicamente la aplicación de la ICP.

Las entidades involucradas en la Figura 2 son:

- El Proveedor de Servicios de Certificación-PSC;
- El Sujeto al que el PSC le ha emitido un Certificado;
- Una parte que confía y
- Un esquema.

Las fuentes de información son:

- El certificado emitido por el PSC;
- El estatus del certificado emitido por el PSC y
- La información acerca del PSC (y el esquema) emitido por el esquema.

Estos son los elementos mínimos que debería contener un Modelo de Confianza, este documento especifica el Modelo de Confianza de la Firma Electrónica Certificada para Nicaragua.

1.5.2. Verificación de la Información

La Figura 2 muestra los tres medios disponibles para la verificación y aceptación que pueden ser utilizados por la parte que confía durante una transacción para asegurarse la confianza entre las partes. Los números "1" y "2" se explican en los incisos 1.5.2.1 y 1.5.2.2 a continuación como referencia, mientras que el número "3" es detallado en este documento desde el inciso 1.5.2.3. Los medios son:

1.5.2.1. Verificación del Servicio de Identidad y Política

Indicado en la Figura 2, mediante la ruta de verificación de información "1". El Certificado provee la información acerca de la identidad del titular del par de claves. Además, provee mediante la utilización de un OID, una referencia a la política bajo el cual el certificado fue emitido. Dicha política debe ser elaborada por el PSC cumpliendo lo establecido en el documento "Modelo para la Declaración de Prácticas de Certificación - DPC y Políticas de Certificados – PC de Los PSC" elaborado por el Ente Rector - DGTEC.

1.5.2.2. Verificación del Estado del Certificado

Indicado en la Figura 2, mediante la ruta de verificación de información "2". La parte que confía puede inspeccionar la información de estado del Certificado, que indica si está o no válido en el momento que fue verificado. La manera de validación estará contrastada en la DPC de cada PSC autorizado por el Ente Rector - DGTEC.

1.5.2.3. Verificación de Aprobación y Estado Actual del Servicio (Estado del PSC)

Indicado en la Figura 2, mediante la ruta de verificación de información "3". Representa el valor para el cual el presente documento define sus requerimientos. Todos los PSC autorizados por el Ente Rector - DGTEC, deberán operar bajo el Esquema definido en este documento el cual proveerá de la información acerca del Estado del PSC. La información de Estado del PSC, está contenida en dos partes una estática y una dinámica.

La parte estática es la información de la evaluación inicial y su aprobación para operar como PSC por parte del Ente Rector - DGTEC, así como su reconocimiento bajo el Esquema que especifica este documento.

La parte dinámica es la información basada en los resultados de auditoría regulares y en otros eventos reportados por procesos del Esquema especificado en este documento. Ejemplos de tales eventos pueden ser cambios en la situación financiera del PSC, cambios en la longitud de las claves criptográficas, reportes de incidentes de seguridad, etc.

El resultado positivo de esta verificación asegurará a las partes que confían que el servicio dentro de sus limitaciones según establezca es de hecho de confianza en el momento que se realizó la verificación y cumple con los compromisos que estableció el PSC.

2. Infraestructura Nicaragüense de Clave Pública

2.1. Modelo de la Infraestructura Nicaragüense de Clave Pública

El Modelo de Confianza utilizado en el territorio nicaragüense está organizado en un modelo jerárquico, caracterizado por tener un solo punto de confianza en la ICP, mediante una Autoridad de Certificación Raíz Nacional denominada “Autoridad de Certificación Raíz Nicaragüense” (ACRN).

La ACRN sirve como ancla de confianza para toda la INCP por lo que la ACRN está bajo la responsabilidad de su administración el Ente Rector de Firma Electrónica.

Este modelo de confianza debe ser adoptado por todo PSC que desee solicitar su autorización ante el Ente Rector - DGTEC.

En la siguiente figura (Figura 3) se muestra la relación directa de los certificados en la Infraestructura Nicaragüense de Clave Pública, en esta la participación de las Autoridades de Registro (AR) no se muestran por no tener vinculación con el certificado más que para solicitar emitir o revocar de ser necesario.

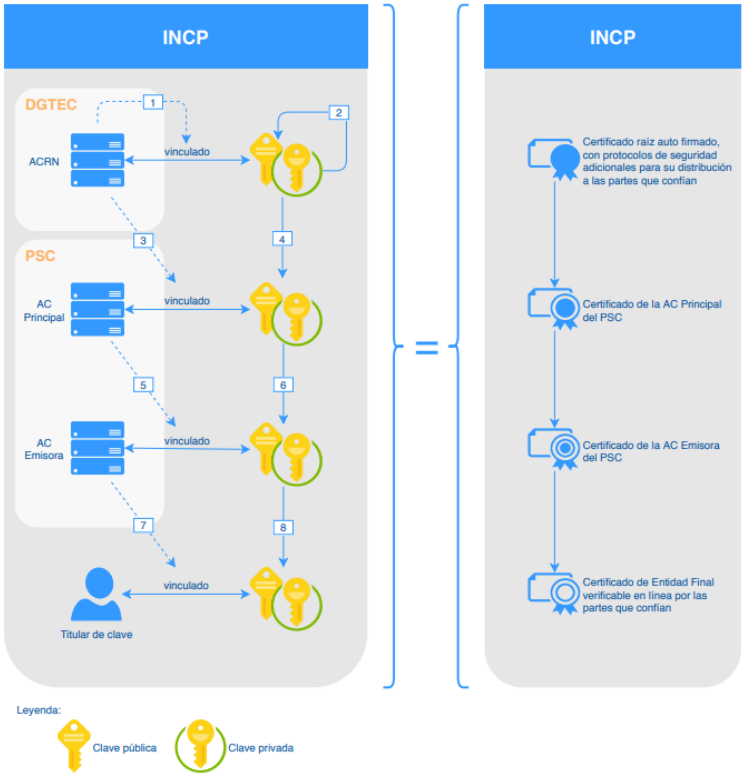

Figura 3: Detalle de la Jerarquía de Certificación.

La figura anterior (Figura 3) muestra la estructura típica de confianza interna de una INCP.

El lado izquierdo, muestra cómo la confianza se realiza mediante los índices, el cual indican el orden en el cual la relación de confianza y las Firmas Electrónicas Certificadas se forman.

En lado derecho se muestra la representación gráfica correspondiente de los certificados involucrados para dar confianza a una persona en la INCP.

En esta figura (Figura 3):

- La ACRN, las AC´s principales, las AC´s Emisoras y las Personas Usuarias, tienen completa confianza en la autenticidad del par de claves del ancla de confianza (En este caso es la ACRN) (Índice 1).
- La ACRN genera un certificado auto firmado (Índice 2) el cual se distribuye a través de cualquier medio seguro adecuado a las partes que confían.
- Cuando la ACRN ha confirmado la identidad de la AC Principal del PSC y la autenticidad de su clave pública es aquí cuando se ha establecido la confianza sobre el vínculo entre la identidad y la clave pública de la AC Principal del PSC (Índice 3).
- La AC Raíz emite un certificado para afirmar lo establecido en el índice 3 de acuerdo con su DPC y PC (Índice 4).
- Cuando la AC Principal del PSC ha confirmado la identidad de la AC Emisora y la autenticidad de su Clave Pública, es aquí cuando se ha establecido la confianza sobre el vínculo entre la identidad y la Clave Pública de la AC Emisora (Índice 5).
- La AC Principal del PSC emite un certificado para afirmar para afirmar lo establecido en el índice 5 de acuerdo con su DPC y PC (Índice 6).
- Cuando la AC Emisora está segura de la identidad de la persona usuaria y la autenticidad de su Clave Pública, es aquí cuando se ha establecido la confianza sobre el vínculo entre la identidad y la Clave Pública de una persona usuaria (Índice 7).
- La AC Emisora emite el certificado de la persona usuaria para afirmar lo establecido en el índice 7 de acuerdo con su DPC y PC de la AC Emisora (Índice 8).

Si cualquiera fuese las circunstancias la ACRN no estuviese disponible para emitir o renovar el certificado de una AC Principal, se permitirá que dicha AC Principal pueda auto firmar su certificado; DGTEC dará validez de la confianza de dicho método y será la única razón por el cual se permita que un PSC tenga una AC Principal auto firmada.

2.2. Verificación del Modelo de Confianza

A nivel técnico la parte que confía verificara la exactitud de la Firma Electrónica en el certificado. Los datos extraídos por un certificado válido, tales como nombre, clave pública y otros atributos serán asumidos auténticos. En la Figura 4 se muestra el proceso de validación y la confianza derivada en la Clave Pública de una persona usuaria.

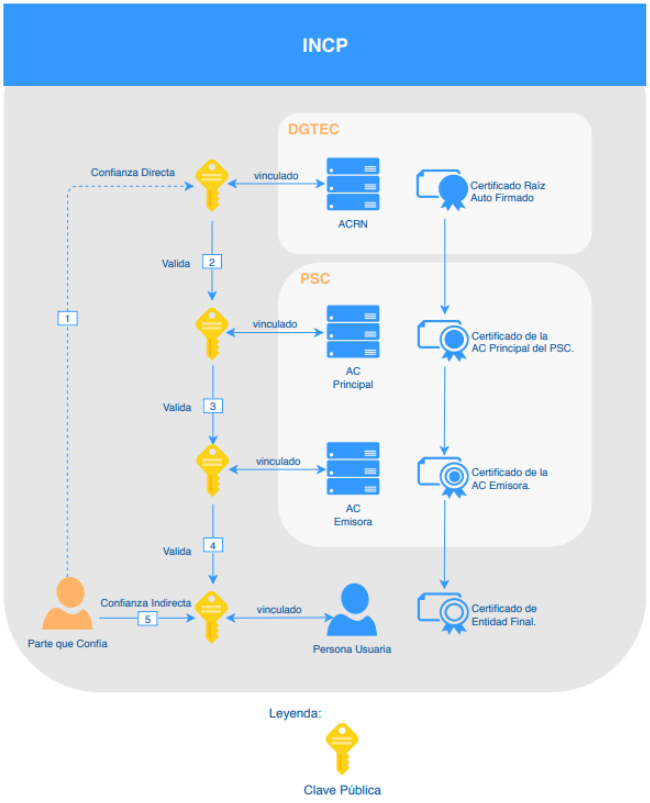

Figura 4: Detalle de la Jerarquía para la Verificación del Certificado.

La parte que confía el cual posee una copia auténtica de la clave pública de la ACRN contenida en el certificado raíz que obtuvo a través de un canal seguro, será capaz de confiar en que la Clave Pública de un Certificado de persona usuaria este realmente vinculado al nombre de una persona usuaria.

Certificado Raíz

El Certificado Raíz auto firmado es generado por una única AC denominada “Autoridad de Certificación Raíz Nicaragüense”, gestionada por el Ente Rector - DGTEC.

Certificado de la AC Principal

El Certificado de la AC Principal es firmado por la “Autoridad de Certificación Raíz Nicaragüense” al PSC, puede ser autofirmado si y solo si no está disponible la ACRN. Dicho certificado es emitido y entregado al cumplir con los requerimientos establecidos en el marco regulatorio de Firma Electrónica. Puede existir “n” cantidad de PSC, por consiguiente “n” cantidad de AC´s Principales.

Certificado de la AC Emisora

El Certificado de la AC Emisora es firmado por la AC Principal. La AC Emisora es quien emite los Certificados a las personas usuarias.

Certificado de Persona Usuaria

El Certificado de persona usuaria es firmado por una AC Emisora del PSC. Dicho Certificado es emitido y entregado en base a la PC y DPC del PSC. Este certificado contará con todo el respaldo legal al ser emitido por un PSC autorizado por el Ente Rector-DGTEC.

2.3. Límites del Modelo

El modelo está limitado de la siguiente manera:

Un máximo de 3 niveles de AC.

- Nivel 1: Una única Autoridad de Certificación Raíz en toda la Infraestructura Nicaragüense de Clave Pública.
- Nivel 2: De 1 a más Autoridades de Certificación Principales conforme autorizaciones emitidas por el Ente Rector. Por cada PSC se tendrán derecho a 1 sola AC Principal.
- Nivel 3: De 1 a más Autoridades de Certificación Emisoras subordinadas a su respectiva AC Principal. Cada PSC según lo requiera o establezca en su solicitud deberá contar con al menos una AC Emisora.
- A partir del Nivel 3 se considera un nivel operativo con las personas usuarias.

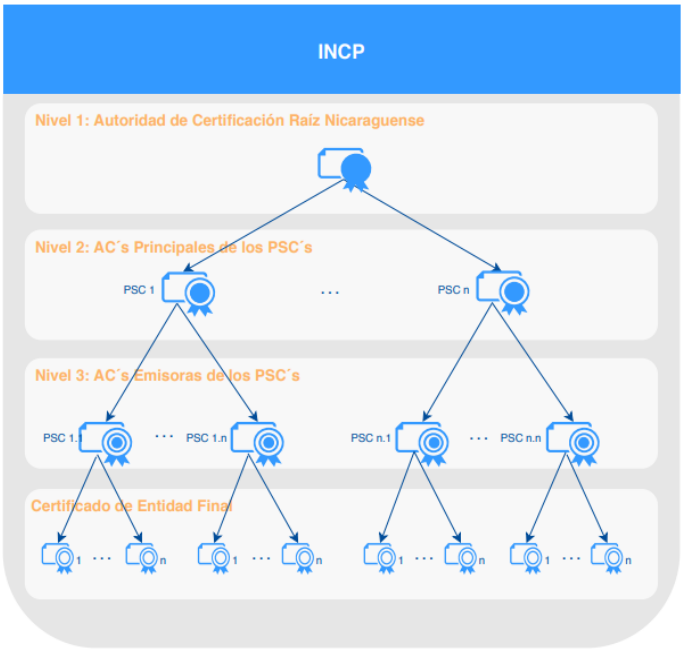

Figura 5: Posibilidades del Modelo de Confianza.

3. Consideraciones Específicas

- Para la selección del Modelo de Confianza de la Infraestructura Nicaragüense de Clave Pública se realizó un estudio de los diferentes Modelos de Confianza aplicables a una Infraestructura de Claves Públicas, seleccionándose el Modelo Jerárquico de Confianza con una Autoridad de Certificación Raíz Nacional Única como es la “Autoridad de Certificación Raíz Nicaragüense” de la cual dependen los Proveedores de Servicios de Certificación acreditados.
- Este Modelo de Confianza debe ser adoptado por todo Proveedor de Servicios de Certificación - PSC que desee solicitar su acreditación ante el Ente Rector - DGTEC.
- La Autoridad de Certificación Raíz Nicaragüense es quien emite los Certificados a las AC Principales de los PSC, quienes a su vez pueden emitir y firmar los Certificados a sus AC Emisoras y estas a sus personas usuarias, más no pueden emitir certificados a su AC superior.

- DGTEC es el Ente Rector y Responsable de la Infraestructura Nicaragüense de Clave Pública a través de la Autoridad de Certificación Raíz Nicaragüense.

- En el Modelo de Confianza de la Infraestructura Nicaragüense de Clave Pública se permite que los PSC constituyan hasta dos niveles de AC por debajo de la AC Raíz siendo su AC Principal del PSC y sus AC Emisoras.

- La validez del certificado de la Autoridad de Certificación Raíz Nicaragüense, AC Principal y AC Emisoras, se establece en la correspondiente Declaración de Practicas de Certificación de cada AC. El periodo de validez del resto de certificados vendrá establecido por la política de certificación que corresponda.

- No existe otra AC que pueda firmar el certificado de la AC Raíz. La AC Raíz crea un certificado auto-firmado. Luego ella firma con este certificado, los certificados de las AC Principal de los PSC.

- La AC Principal de un PSC podría auto-firmar su certificado únicamente en caso de que la ACRN no estuviese disponible.

- La AC Raíz no emite certificados de Entidad Final, sólo emite certificados a la AC Principal de los PSC´s.

- La AC Raíz establece las condiciones para los tipos de certificados que pueden emitir las AC de los PSC.

- Cada PSC debe contar con una sola AC Principal, una o varias AC Emisoras y AR´s encargadas de atender a su comunidad de personas usuaria.

- Los PSC son responsables de la gestión (emisión, suspensión y revocación) de los certificados de sus personas usuarias, mas no de los usos posteriores que estos les den a los certificados.

- Las limitaciones de uso de cada tipo de certificado deben estar establecidas en su correspondiente política de certificados.

- El estándar UIT X.509 v3 será el estándar utilizado en todos los aspectos relacionados con el formato, codificación, contenidos e interpretación de los certificados y las listas de certificados revocados.

- Los procedimientos para las solicitudes y emisiones del par de claves se especificarán en la Declaración de Prácticas de Certificación (DPC) del PSC.

- Los procedimientos en caso de pérdida o renovación de algún certificado se establecerán en la DPC del PSC.

- Las personas usuarias de los certificados deben conocer las Políticas de Uso de los Certificados establecidas por el PSC.

- La estructura de OID - Identificadores de Objeto necesaria para la INCP están bajo el nodo joint-iso-itu-t(2) country(16) ni(558) incp(0)[3] .

4. Ciclo de Vida de los Certificados de la INCP

Los ciclos de vida de los certificados de cada nivel de la INCP se regirán de la siguiente manera y deberán de ser tomados en cuenta en las DPC de cada AC:

[3] Ver documento: “Guía De Administración de los Identificadores de Objetos en Nicaragua”

- Para el Nivel 1:

- La ACRN debe ser válida por un periodo de 25 años.

- Faltando 10 años para el vencimiento de la ACRN ésta no emitirá nuevos certificados de AC Principales, los nuevos certificados serán emitidos por una nueva ACRN cuando se requiera.

- La ACRN no podrá emitir certificados de AC Principales que tengan un tiempo de validez que supere el periodo de vigencia de la ACRN.

- Para el Nivel 2:

- Las AC Principales deben ser válidas por un máximo de 10 años y un mínimo de 8 años.

- Faltando 4 años para el vencimiento de una AC Principal ésta no emitirá nuevos certificados de AC Emisoras, y deberá generarse una nueva AC Principal.

- Una AC Principal no podrá emitir certificados de AC Emisoras que tengan un tiempo de validez que supere el periodo de vigencia de la AC Principal.

- Para el Nivel 3:

- Las AC Emisoras deben ser válidas dentro del periodo de vigencia de su AC Principal y no menores a dos veces el periodo máximo de vigencia de los certificados finales que emita.

- Faltando el periodo máximo de validez del certificado final que emita una AC Emisora, previo al vencimiento del periodo de vigencia de la misma, ésta no emitirá nuevos certificados finales y deberá generarse una nueva AC Emisora.

- Una AC Emisora no podrá emitir certificados finales que tengan un tiempo de validez que supere el periodo de vigencia de la AC Emisora.

- Para los Certificados Finales:

- Los certificados finales deben ser válidos hasta por un máximo de 4 años.