DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS E INFORMÁTICA

"MANUAL DE POLÍTICAS, NORMAS Y PROCEDIMIENTOS DE UNA PKI BASADO EN SMART GRID PARA EL SISTEMA NACIONAL DE EDUCACIÓN SUPERIOR DEL ECUADOR"

AUTOR: PONCE DÍAZ JOHANNA ELIZABETH

VILLAGÓMEZ CABRERA SANDRA STEFANY

DIRECTOR: ING. GALÁRRAGA FERNANDO

CODIRECTOR: ING.CAMPAÑA MAURICIO

SANGOLQUÍ

2016

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

DECLARACIÓN DE RESPONSABILIDAD

Nosotras, Johanna Elizabeth Ponce Díaz y Sandra Stefany Villagómez Cabrera

DECLARAMOS QUE:

El proyecto de grado denominado "MANUAL DE NORMAS POLÍTICAS Y PROCEDIMIENTOS DE UNA PKI BASADO EN SMARTGRID PARA EL SISTEMA NACIONAL DE EDUCACIÓN SUPERIOR DEL ECUADOR", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 26 enero de 2016

Johanna Elizabeth Ponce Díaz
C.C. 1721025144

Sandra Stefany Villagómez Cabrera
C.C. 171965968-0

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICADO

Ing. Fernando Galarraga

CERTIFICA

Que el presente trabajo titulado "MANUAL DE NORMAS POLÍTICAS Y PROCEDIMIENTOS DE UNA PKI BASADO EN SMARTGRID PARA EL SISTEMA NACIONAL DE EDUCACIÓN SUPERIOR DEL ECUADOR" fue realizado en su totalidad por la Srta. Johanna Elizabeth Ponce Díaz y la Srta. Sandra Stefany Villagómez Cabrera como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA

Sangolquí 26 enero de 2016

ING. FERNANDO GALARRAGA
DIRECTOR DE TESIS

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN DE PUBLICACIÓN

Nosotras, Johanna Elizabeth Ponce Díaz y Sandra Stefany Villagómez Cabrera, autorizamos a la UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE, la publicación, en la biblioteca virtual de la Institución del proyecto de tesis "MANUAL DE NORMAS POLÍTICAS Y PROCEDIMIENTOS DE UNA PKI BASADO EN SMARTGRID PARA EL SISTEMA NACIONAL DE EDUCACIÓN SUPERIOR DEL ECUADOR", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 26 enero de 2016

Johanna Elizabeth Ponce Díaz
C.C. 1721025144

Sandra Stefany Villagómez Cabrera
C.C. 171965968-0

DEDICATORIA

La presente tesis me gustaría dedicar a mis padres quienes han sido mi fortaleza y el pilar más grande en mi vida, por permitirme realizar y cumplir mis sueños, por regalarme su apoyo, confianza y amor incondicional, además de dotarme de todos los valores necesarios para ser la persona quien soy, enseñándome a perseverar ante cualquier adversidad y luchar por mis ideales.

A mis hermanos, María José y Rafael quienes me han dado aliento con sus palabras de apoyo, brindándome una mano siempre que fuera necesario para seguir adelante.

A mi pequeño milagro que el señor me regalo mi hija Doménica y a mi compañero de vida, la bendición más grande y mi eterna inspiración.

A toda mi familia por regalarme un granito de arena durante mi formación académica y personal.

A mi compañera de tesis y amiga incondicional Sandrita que ha compartido durante varios años el cansancio y desvelos para cumplir nuestras metas, así como su magnífica amistad, sin ella todo este trabajo en conjunto no hubiera sido posible, ya que me ha brindado sus conocimientos, responsabilidad y un profundo sentido de determinación.

A todos mis queridos compañeros con quienes formamos un gran lazo de amistad durante varios años.

A todos ellos, muchas gracias de todo corazón.

AGRADECIMIENTOS

Agradezco a Dios por estar conmigo en cada paso que doy en mi vida, por fortalecerme como persona, iluminando mi mente y mi corazón para cada decisión que he tomado, por ayudarme a seguir un buen camino y por sobretodo poner a personas que han trabajado como soporte y aliento durante todo mi periodo estudiantil.

Agradezco profundamente a mi padre Clemente Ponce, a pesar de que ya no estás conmigo en la tierra sé que en el cielo podrás ver todos mis logros, que gracias a ti se están cosechando ahora, siempre contribuiste con tus palabras que permitieron engrandecer mis metas.

Te extraño mucho, Dios te guarde en su gloria, nos veremos en la eternidad….

A mi madre Yolanda Díaz por siempre haber estado en las buenas y en las malas apoyándome incondicionalmente en mis propósitos, por siempre estar pendiente y preocupada por mi bienestar, alentándome con sus palabras para seguir adelante hasta lograr el éxito. A mis hermanos por haberme dado la fortaleza necesaria y apoyo inigualable día a día.

Mis más sinceros y profundos agradecimientos al Ing. Fernando Galarraga y al Ing. Mauricio Campaña ya que con su guía y conocimientos se ha podido realizar esta tesis.

Por último quisiera agradecer a cada una de las personas que han vivido conmigo la realización de este trabajo,

Para ellos, Muchas gracias por todo

DEDICATORIA

A mis amados hijos David, Matías y Samantha, regalos de Dios que día a día llenan mi corazón y vida con sus sonrisas, travesuras, locuras e inocencia, para quienes dedico todo mi esfuerzo diario.

A mis padres Carlos y Nelly, ejemplos de decisión, valor, constancia y trabajo, de quienes he recibido apoyo incondicional en toda etapa de mi vida

Sandra

AGRADECIMIENTOS

A mi ñaño por estar siempre pendiente de mi bienestar, gracias a sus consejos, inteligencia y visión he podido crecer y entregar al mundo siempre mi mejor esfuerzo.

A mis queridas hermanas Andrea y Erika que han sido parte del crecimiento y formación de mis hijos al igual que mi madre.

A mi amado esposo, compañero de vida y cabeza de mi hogar, Joao, por su apoyo, paciencia y sincero amor.

A mis maestros y compañeros con los que hemos compartido momentos de risas y estudio durante la vida universitaria, en especial Joha, amiga con quien hemos vivido no solo largas malas noches de estudio y sacrificios, sino también gratos momentos de amistad, a todos muchas gracias.

Sandra

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El intercambio de información utilizando tecnología de certificación digital es necesaria para garantizar que la comunicación se realice de forma segura, evitando pérdida o alteración de información en una institución. Para ello, se establece una PKI basada en SmartGrid y es eminente implantar normas, y políticas que creen hábitos para una comunicación exitosa y segura, al igual que convenir los procedimientos que indiquen como se debe llevar a cabo el ciclo de vida de un certificado digital, a la vez homogenizar procesos dentro de las instituciones que sean parte de la red de SmartGrid, quienes deben respetar los lineamientos y estándares que se definan en el manual.

PALABRAS CLAVE:

SMARTGRID

PKI

NORMAS

POLÍTICAS

PROCEDIMIENTOS.

ABSTRACT

The exchange of information using technology of digital certification it is necessary to guarantee that the communication realizes of sure form, avoiding loss or alteration of information in an institution. For it, a PKI based on SmartGrid is established and is eminent to implant procedure and policies that believe habits for a successful and sure communication, as are convenient the procedures that they indicate like it is necessary to carry out and homogenize processes inside the institutions that are a part of Smart Grid's network, who must respect the limits and standards that are defined in manual.

KEY WORDS:.

SMARTGRID

PKI

NORMAS

POLÍTICAS

PROCEDIMIENTOS

CAPÍTULO I

INTRODUCCIÓN GENERAL

El intercambio de información día a día está relacionada más con la realidad de cualquier institución, de esta manera es importante poseer un certificado digital que acredite la veracidad de una manera irrefutable, de esta manera permita garantizar tramites seguros y mucho más rápidos, contando con los elementos principales de la autenticidad, integridad, confidencialidad y no repudio.

El Sistema Nacional de Información de la Educación Superior del Ecuador (SNIESE) permite la planificación institucional, que incluye el diseño del desarrollo de ciertas políticas y el monitoreo de los objetivos del Plan Nacional mediante la gestión de datos y la difusión de información.

Los avances de la tecnología, reemplazan los costos y el tiempo que involucra realizar un trámite presencial, gracias a la velocidad de una comunicación electrónica dotada de validez legal.

1.1 Planteamiento del Problema

Hoy en día el Sistema Nacional de Educación Superior no cuenta con una infraestructura tecnológica que garantice la validez jurídica de los documentos electrónicos, esta realidad ocasiona la no confiabilidad de dichos documentos y desorientación en los procesos por falta de una fuente de conocimiento que defina las normas y los procedimientos esenciales para la certificación digital.

Los resultados de los procedimientos en una PKI y la optimización de recursos informáticos se ven notablemente afectados debido a que no se dispone de un manual de normas, políticas y procedimientos que nos muestre el cómo implementar los servicios de certificación digital basados en una PKI.

Actualmente, las Instituciones de Educación Superior brindan servicios educativos tales como las solicitudes académicas, emisión de certificados, entre otros; de manera autónoma y manual, por este motivo existe pérdida de tiempo ya que dichos procedimientos retardan la eficacia en la generación de documentos necesarios para los trámites dentro de las instituciones.

La repetición de procesos es un severo problema por lo que se puede generar doble documentación, lo que crea confusión y errores al momento de actualizar la información de los estudiantes, docentes y personal administrativo, porque no son claramente definidos por la falta de coherencia en los procedimientos.

La seguridad y veracidad de dichos documentos se ven perjudicados considerablemente porque están en riesgo de no ser calificados como válidos al final del proceso dentro de las Instituciones de Educación Superior.

1.2 Justificación

El manual de normas, políticas y procedimientos ayuda a eliminar la repetición de procesos y evitar la generación de documentación innecesaria, de esta manera la actualización de la información será precisa y válida.

Se considera importante tomar en cuenta la seguridad y veracidad de la documentación, por este motivo este proyecto permite que los riesgos sean mínimos al ofrecer este tipo de servicio.

Es preciso crear una fuente de conocimiento donde estén establecidos las normas, políticas y procedimientos que sean utilizados como herramienta de orientación para certificar documentos y reducir la tasa de errores de procesos realizados en forma manual.

Dentro de las Instituciones de Educación Superior se puede optimizar el tiempo y recursos informáticos al momento de generar documentos, permitiendo que estos sean entregados con mayor rapidez al tener un manual que nos respalde con normas que garanticen los procesos involucrados en la emisión de certificados.

Es necesario desarrollar un manual de políticas, normas y procedimientos para servicios de certificación digital en una PKI basados en tecnología SmartGrid aplicada al Sistema Nacional de Educación Superior del Ecuador, ya que es base fundamental para establecer la manera de realizar los proyectos de desarrollo de una infraestructura de servicios de certificación digital y a su vez la implementación dentro de un ambiente SmartGrid que contenga una autoridad certificadora y lograr la interacción entre Instituciones de Educación Superior.

1.3 Objetivos

1.3.1 Objetivo General

Desarrollar un manual de políticas, normas y procedimientos para ofertar servicios de certificación digital en las Instituciones que pertenecen el Sistema Nacional de Educación Superior del Ecuador a través de una PKI basado en SmartGrid.

1.3.2 Objetivos Específicos

- Analizar el marco legal Ecuatoriano necesario para establecer las políticas de Certificación digital basadas en un modelo de terceras partes confianza
- Definir un modelo de gestión basado en la norma PKIx para implementar servicios de certificación digital.
- Elaborar los procedimientos que describan el ciclo de vida de los certificados y firmas digitales emitidos por las Universidades del Ecuador.

1.4 Alcance

Los conceptos de seguridad informática, integridad, confidencialidad y autenticación son básicos dentro de una infraestructura PKI, y de hecho, la implementación de una PKI en un entorno de SmartGrid requiere componentes tales como la AC (Autoridad Certificadora) y una AR (Autoridad de Registro), basados en el marco legal del Ecuador y los estándares Internacionales para los servicios de certificación digital.

El modelo de gestión PKI basado en SmartGrid se compone del manual de:

- Normas basadas en los estándares Internacionales para servicios de certificación digital.
- Políticas basadas en el marco legal Ecuatoriano para servicios de certificación digital.
- Procedimientos para emitir, revocar, extinguir y suspender los certificados y firmas digitales en las Instituciones de Educación Superior que pertenecen al Sistema Nacional de Educación Superior.

CAPÍTULO 2

MARCO TEÓRICO

En este capítulo se definen conceptos fundamentales tales como, Smart Grid y PKI las cuales se consideran junto con la estructura del SENESCYT y el modelo de terceras partes de confianza, para establecer las normas, políticas y procedimientos de la PKI basado en Smart Grid para el Sistema Nacional de Educación Superior.

2.1 Smart Grid

Smart Grid, también llamado Grid Computing o computación Grid, es un conjunto de sistemas paralelos y distribuidos que permiten utilizar coordinadamente todo tipo de recursos, como puede ser de cómputo, almacenamiento o aplicaciones, los cuales no están sujetos a un control centralizado, es decir su funcionamiento es independiente de los otros sistemas y además son distribuidos geográficamente. Un sistema para ser llamado Grid debe:

- Coordinar los recursos que no son sujetos al control centralizado.
- Utilizar estándares, protocolos de propósito general e interfaces.
- Entregar calidades no triviales de servicio. (Foster, 2002)

La computación Grid promueve que los recursos puedan ser compartidos, por lo que este proceso debe ser flexible de tal forma que la comunicación entre sistemas pueda establecerse fácilmente, permitiendo a nuevos participantes de la Grid integrarse, a pesar de ser desarrollados en diferentes plataformas.

En un entorno Grid, el acceso a la información es limitada bajo la autorización del reconocimiento de identidades para garantizar la seguridad e integridad de información, por ello es importante definir como los sistemas deben comportarse y como debe ser la estructura bajo la cual intercambian información. Los cimientos de Smart Grid son fundamentalmente tres:

1. Distribución de recursos a gran escala: Compartir varios recursos entre diferentes usuarios, cuyo objetivo sea ingresar a la Grid. El acceso a la infraestructura global de la Grid debe ser igual de sencilla que el ingreso a la infraestructura local.
2. Regulación de los recursos distribuidos en las Instituciones: Las instituciones que tengan una Grid deben implantar normas, políticas y procedimientos para que los integrantes que pertenezcan a dicha Grid, trabajen bajo regulaciones para que los recursos puedan ser distribuidos y aprovechados de una manera eficaz e eficiente.
3. Múltiples recursos: Los recursos que comparten los participantes de la Grid son variados y al ejecutarse en sistemas distribuidos la comunicación se establece en distintos estándares, por tanto la Grid está encargada de que estos recursos puedan interactuar y se ejecuten de la mejor manera.

Las ventajas que Smart Grid ofrece son:

- Compartir recursos que se encuentran distribuidos geográficamente.

- Permitir la integración y el uso colectivo de ordenadores de alto rendimiento, redes y bases de datos que son propiedad y están administrados por diferentes instituciones.
- Comunicación bidireccional exitosa entre la red y los usuarios finales.
- Implementación de la seguridad cibernética en todo el sistema de protección.
- Todos los actores del Grid pueden tomar decisiones y comunicarse con el resto de actores.
- Smart Grid aprovecha el rendimiento y la infraestructura mejorando sus recursos computacionales.

2.1.1 Aplicaciones Smart Grid

Smart Grid es utilizada en diversas áreas como, gobiernos, las Fuerzas Armadas, Instituciones de educación y negocios. Existen proyectos internacionales, nacionales, de campos específicos y voluntarios que se han llevado a cabo con muy buenos resultados:

- Grid Internacionales: cruzan las fronteras de los países, expandiendo las culturas, las lenguas, las tecnologías y más, para crear recursos internacionales y darle poder a la ciencia global, empleando computación global. (GRID CAFÉ, s.f.)
- Sistemas distribuidos en tiempo real: Aplicaciones cuyo flujo de datos a alta velocidad son analizados y procesados en tiempo real.
- Proceso intensivo de datos: Son aplicaciones que hacen uso de gran espacio de almacenamiento, desbordando la capacidad de almacenamiento de un úni-

co nodo y los datos son distribuidos por todo el Grid. Además de los beneficios por el incremento de espacio, la distribución de los datos a lo largo del Grid permite el acceso a los mismos de forma distribuida.

- Entornos virtuales de colaboración: Se utilizan los enormes recursos computacionales del Grid y su naturaleza distribuida para generar entornos virtuales 3D distribuidos.
- Existen aplicaciones reales que hacen uso de mini-Grids, las cuales están centradas en el campo de la investigación en el terreno de las ciencias físicas, médicas y del tratamiento de la información. Además existen diversas aplicaciones en el campo de la seguridad vial. (GRID CAFÉ, s.f.)

2.2 PKI

PKI es una infraestructura de clave pública, pertenece a varios servicios los cuales permiten trabajar con criptografía asimétrica usando dos claves para el envío de mensajes, siendo esta una estructura ideal para prestar servicios de autentificación de usuarios y para dar seguridad al usuario, garantizando su acceso a servicios distribuidos en una red y evitar la suplantación de identidad.

PKI al utilizar criptografía asimétrica permite que se desarrolle servicios de seguridad con sus claves, pública y la privada y crea un nivel de confianza dentro de los procesos realizados en base de la administración de certificados digitales, de esta manera corrobora la autentificación, integridad y no repudio de la información.

Este estándar describe procesos necesarios para realizar la gestión de certificados digitales de claves públicas y realizar el intercambio seguro de la información, permite que se realice documentos electrónicos que incluyen firmas digitales sean estas en un email, el código del programa o transacciones bancarias.

PKI tiene usos como el reconocimiento de la identificación a una empresa o persona en internet y a su vez la autorización del acceso a servicios restringidos. Las ventajas presentes en una PKI son las siguientes:

- Optimiza los procesos garantizando la seguridad de los datos.
- Es uno de los servicios más comunes para autentificación de usuarios ya que utiliza la criptografía de clave pública.
- Asegura la identidad del usuario, sea como autor de documentos o identificando a los usuarios que acceden a servicios en la red sean estos distribuidos o no, ya que solo se puede conocer su clave privada evitando la suplantación.
- Vela por la integridad de información, evitando la modificación de los datos firmados.
- Ofrece mejores medios para que se pueda identificar al usuario, ya que los certificados contienen información verificable relacionada con la identidad del usuario.
- Solo el usuario conoce la forma de acceder a su clave privada porque los certificados basados en tecnologías de clave pública proveen un mecanismo de autentificación fuerte.

2.2.1 Aplicaciones PKI

Los sistemas de PKI, de distintos tipos y proveedores, tienen muchos usos, incluyendo la asociación de una llave pública con una identidad para:

- Cifrado y/o autenticación de mensajes de correo electrónico
- Autenticación de servidores web utilizando SSL.
- IPSec Certificación
- Time Stamping
- DNI
- Single Sing On

2.3 SENESCYT

La Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) es el área que garantiza el cumplimiento de la gratuidad para que la ciudadanía tenga el acceso a la educación superior, de esta manera identifica carreras y programas de interés público y es priorizado junto al Plan del Buen Vivir.

Senescyt siendo un ente regulador permite diseñar coordinar, administrar e implementar junto al Sistema Nacional de Información de la Educación Superior del Ecuador (SNIESE) y el Sistema Nacional de Nivelación y Admisión (SNNA).

2.3.1 Historia del SENESCYT

El CONESUP (Consejo Nacional de Enseñanza Superior Universitaria Privada) fue un órgano cuyas funciones eran autorizar la creación de universidades, así como

la creación de carreras. Además realizaba la inspección para garantizar que se cumplan las condiciones básicas aprobadas refiriéndose a las universidades privadas.

El Gobierno actual promovió la gratuidad de la educación superior, borrando de esta manera al CONESUP y dividiendo las funciones que este organismo no acreditador en los tres siguientes organismos:

- CES (Consejo de Educación Superior),
- SENESCYT (Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación)
- CEAACES (Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior).

Bajo esta nueva organización, se controla el desorden absoluto que se presentaban dentro de esta entidad ya que tampoco permitía un manejo adecuado del talento humano, existía un desorden en cuanto al personal que trabajaba y en muchas ocasiones se encontró afectado los salarios siendo estos duplicados y hasta triplicados con respecto a lo que establece la escala del Ministerio de Relaciones Laborales.

2.3.2 Funciones

La Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), es el órgano que regula la política pública de educación superior y permite la coordinación de acciones entre las instituciones de sistema de educación superior y la función ejecutiva.

Las funciones de la SENESCYT son las siguientes:

- Establecer los mecanismos de coordinación entre la Función Ejecutiva y el Sistema de Educación Superior.
- Ejercer la rectoría de las políticas públicas en el ámbito de su competencia;
- Garantizar el efectivo cumplimiento de la gratuidad en la educación superior.
- Identificar carreras y programas considerados de interés público y priorizarlas de acuerdo con el plan nacional de desarrollo.
- Diseñar, implementar, administrar y coordinar el Sistema Nacional de Información de la Educación Superior del Ecuador, y el Sistema de Nivelación y Admisión.
- Diseñar, administrar e instrumentar la política de becas del gobierno para la educación superior ecuatoriana; para lo cual coordinará, en lo que corresponda, con el Instituto Ecuatoriano de Crédito Educativo y Becas.
- Establecer desde el gobierno nacional, políticas de investigación científica y tecnológica de acuerdo con las necesidades del desarrollo del país y crear los incentivos para que las universidades y escuelas politécnicas puedan desarrollarlas, sin menoscabo de sus políticas internas.
- Elaborar informes técnicos para conocimiento y resolución del Consejo de Educación Superior en todos los casos que tienen que ver con los objetivos del Plan Nacional de Desarrollo.
- Elaborar los informes técnicos que sustenten las resoluciones del Consejo de Educación Superior.

- Ejercer las demás atribuciones que le confiera la Función Ejecutiva y la LOES. (EcuadorUniversitario, 2012)

2.3.3 Estructura del SENESCYT

Las universidades y escuelas politécnicas a nivel nacional según la Secretaria Nacional de Educación Superior, Ciencia, Tecnología e Innovación son 74, las cuales se agrupan en cuatro regiones. A continuación se detalla en la Tabla 1, las instituciones correspondientes a la Región Sierra Norte, en la Tabla 2, instituciones de la región Sierra Sur, en la Tabla 3 instituciones de la región Costa y en la Tabla 4 instituciones de la Región Galápagos-Oriente:

Tabla 1. Universidades y Escuelas Politécnicas Región Sierra Norte

NOMBRE	ID	FINANCIAMIENTO	CALF. CONEA	PROVINCIA	CANTÓN
ESCUELA POLITÉCNICA DEL EJÉRCITO	1004	PÚBLICO	A	PICHINCHA	RUMIÑAHUI
ESCUELA POLITÉCNICA NACIONAL	1001	PÚBLICO	A	PICHINCHA	QUITO
ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO	1002	PÚBLICO	A	CHIMBORAZO	RIOBAMBA
FACULTAD LATINOAMERICANA DE CIENCIAS SOCIALES	1026	PÚBLICO	A	PICHINCHA	QUITO
INSTITUTO DE ALTOS ESTUDIOS NACIONALES	1057	PÚBLICO	A	PICHINCHA	QUITO
PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR	1027	COFINANCIADO	A	PICHINCHA	QUITO
UNIVERSIDAD ALFREDO PÉREZ GUERRERO	1055	AUTOFINANCIADO	E	PICHINCHA	QUITO
UNIVERSIDAD ANDINA SIMÓN BOLIVAR	1022	PÚBLICO	A	PICHINCHA	QUITO
UNIVERSIDAD AUTÓNOMA DE QUITO	1048	AUTOFINANCIADO	E	PICHINCHA	QUITO
UNIVERSIDAD CENTRAL DEL ECUADOR	1005	PÚBLICO	A	PICHINCHA	QUITO
UNIVERSIDAD CRISTIANA LATINOAMERICANA	1054	AUTOFINANCIADO	E	PICHINCHA	QUITO
UNIVERSIDAD DE ESPECIALIDADES TURÍSTICAS	1053	AUTOFINANCIADO	E	PICHINCHA	QUITO

Continua

UNIVERSIDAD DE LAS AMÉRICAS	1040	AUTOFINANCIADO	B	PICHINCHA	QUITO
UNIVERSIDAD DE LOS HEMISFERIOS	1070	AUTOFINANCIADO	D	PICHINCHA	QUITO
UNIVERSIDAD DE OTAVALO	1059	AUTOFINANCIADO	E	IMBABURA	OTAVALO
UNIVERSIDAD IBEROAMERICANA DEL ECUADOR	1073	AUTOFINANCIADO	E	PICHINCHA	QUITO
UNIVERSIDAD INTERAMERICANA DEL ECUADOR	1076	AUTOFINANCIADO	E	CHIMBORAZO	RIOBAMBA
UNIVERSIDAD INTERCURTURAL DE LAS NACIONALIDADES Y PUEBLOS INDÍGENAS AMAWTAY WASI	1068	AUTOFINANCIADO	E	PICHINCHA	QUITO
UNIVERSIDAD INTERNACIONAL DEL ECUADOR	1041	AUTOFINANCIADO	C	PICHINCHA	QUITO
UNIVERSIDAD INTERNACIONAL SEK	1036	AUTOFINANCIADO	D	PICHINCHA	QUITO
UNIVERSIDAD NACIONAL DE CHIMBORAZO	1019	PÚBLICO	B	CHIMBORAZO	RIOBAMBA
UNIVERSIDAD OG MANDINO	1071	AUTOFINANCIADO	E	PICHINCHA	QUITO
UNIVERSIDAD POLITÉCNICA JAVERIANA	1039	AUTOFINANCIADO	E	PICHINCHA	QUITO
UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES	1042	AUTOFINANCIADO	D	TUNGURAHUA	AMBATO
UNIVERSIDAD SAN FRANCISCO DE QUITO	1038	AUTOFINANCIADO	A	TUNGURAHUA	AMBATO
UNIVERSIDAD TÉCNICA DE AMBATO	1010	PÚBLICO	A	TUNGURAHUA	AMBATO
UNIVERSIDAD TÉCNICA DE COTOPAXI	1020	PÚBLICO	C	COTOPAXI	LATACUNGA
UNIVERSIDAD TÉCNICA DEL NORTE	1015	PÚBLICO	B	IMBABURA	IBARRA
UNIVERSIDAD TECNOLÓGICA AMÉRICA	1043	AUTOFINANCIADO	E	PICHINCHA	QUITO
UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL	1032	COFINANCIADO	C	PICHINCHA	QUITO
UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA	1045	AUTOFINANCIADO	E	TUNGURAHUA	AMBATO
UNIVERSIDAD EQUATORIALIS	1055	AUTOFINANCIADO	E	PICHINCHA	QUITO
UNIVERSIDAD TECNOLÓGICA ISRAEL	1051	AUTOFINANCIADO	E	PICHINCHA	QUITO

(Senescyt, s.f.)

Tabla 2. Universidades y Escuelas Politécnicas Región Sierra Sur

NOMBRE	ID	FINANCIAMIENTO	CALF. CONEA	PROVINCIA	CANTÓN
UNIVERSIDAD ESTATAL DE BOLÍVAR	1017	PÚBLICO	B	BOLIVAR	GUARANDA

Continua

ESCUELA SUPERIOR POLITÉCNICA ECOLÓGICA PROFESOR SERVIO TULIO MONTERO LUDEÑA	1064	AUTOFINANCIADO	E	LOJA	CARIAMANGA
UNIVERSIDAD CATÓLICA DE CUENCA	1029	COFINANCIADO	C	AZUAY	CUENCA
UNIVERSIDAD DE CUENCA	1007	PÚBLICO	A	AZUAY	CUENCA
UNIVERSIDAD DEL AZUAY	1033	COFINANCIADO	A	AZUAY	CUENCA
UNIVERSIDAD NACIONAL DEL LOJA	1008	PÚBLICO	B	LOJA	LOJA
UNIVERSIDAD PANAMERICANA DE CUENCA	1069	AUTOFINANCIADO	E	AZUAY	CUENCA
UNIVERSIDAD POLITÉCNICA SALESIANA	1034	COFINANCIADO	B	AZUAY	CUENCA
UNIVERSIDAD TÉCNICA PARTICULAR DE CIENCIAS AMBIENTALES JOSÉ PERALTA	1063	AUTOFINANCIADO	E	CAÑAR	AZOGUES
UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA	1031	COFINANCIADO	A	LOJA	LOJA

(Senescyt, n.d.)

Tabla 3. Universidades y Escuelas Politécnicas Región Costa

NOMBRE	ID	FINANCIAMIENTO	CALF. CONEA	PROVINCIA	CANTÓN
UNIVERSIDAD TÉCNICA LUIS VARGAS TORRES DE ESMERALDAS	1012	PÚBLICO	C	ESMERALDAS	ESMERALDAS
ESCUELA SUPERIOR POLITENICA AGROPECUARIA DE MANABÍ	1003	PÚBLICO	C	MANABÍ	MANTA
ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL	1021	PÚBLICO	A	GUAYAS	GUAYAQUIL
UNIVERSIDAD AGRARIA DEL ECUADOR	1018	PÚBLICO	B	GUAYAS	GUAYAQUIL
UNIVERSIDAD CASA GRANDE	1049	AUTOFINANCIADO	D	GUAYAS	GUAYAQUIL
UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL	1028	COFINANCIADO	C	GUAYAS	GUAYAQUIL
UNIVERSIDAD DE ESPECIALIDADES ESPÍRITU SANTO	1037	AUTOFINANCIADO	B	GUAYAS	SAMBORONDÓN
UNIVERSIDAD DE GUAYAQUIL	1006	PÚBLICO	B	GUAYAS	GUAYAQUIL
UNIVERSIDAD DEL PACÍFICO ESCUELA DE NEGOCIOS	1044	AUTOFINANCIADO	B	GUAYAS	GUAYAQUIL
UNIVERSIDAD ESTATAL DE MILAGRO	1024	PÚBLICO	C	GUAYAS	MILAGRO

Continua

UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ	1025	PÚBLICO	C	MANABÍ	JIPIJAPA
UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA	1023	PÚBLICO	B	SANTA ELENA	LA LIBERTAD
UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ	1016	PÚBLICO	C	MANABÍ	MANTA
UNIVERSIDAD LAICA VICENTE ROCAFUERTE DE GUAYAQUIL	1030	COFINANCIADO	D	GUAYAS	GUAYAQUIL
UNIVERSIDAD METROPOLITANA	1056	AUTOFINANCIADO	B	GUAYAS	GUAYAQUIL
UNIVERSIDAD NAVAL COMANDANTE RAFAEL MORÁN VALVERDE	1072	AUTOFINANCIADO	C	SANTA ELENA	SALINAS
UNIVERSIDAD PARTICULAR SAN GREGORIO DE PORTOVIEJO	1060	AUTOFINANCIADO	E	MANABÍ	PORTOVIEJO
UNIVERSIDAD TÉCNICA DE BABAHOYO	1013	PÚBLICO	D	LOS RÍOS	BABAHOYO
UNIVERSIDAD TÉCNICA DE MACHALA	1011	PÚBLICO	C	EL ORO	MACHALA
UNIVERSIDAD TÉCNICA DE MANABÍ	1009	PÚBLICO	D	MANABÍ	PORTOVIEJO
UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO	1014	PÚBLICO	C	LOS RÍOS	QUEVEDO
UNIVERSIDAD TECNOLÓGICA ECOTEC	1077	AUTOFINANCIADO	D	GUAYAS	GUAYAQUIL
UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL	1050	AUTOFINANCIADO	E	GUAYAS	GUAYAQUIL
UNIVERSIDAD TECNOLÓGICA SAN ANTONIO DE MACHALA	1052	AUTOFINANCIADO	E	EL ORO	MACHALA

(Senescyt, n.d.)

Tabla 4. Universidades y Escuelas Politécnicas Región Galápagos-Oriente

NOMBRE	ID	FINANCIAMIENTO	CALF. CONEA	PROVINCIA	CANTÓN
UNIVERSIDAD ESTATAL AMAZÓNICA	1058	PÚBLICO	D	PASTAZA	PUYO
ESCUELA POLITÉCNICA ECOLÓGICA AMAZÓNICA	1035	COFINANCIADO	E	NAPO	TENA
UNIVERSIDAD INTERNACIONAL DEL ECUADOR	1041	AUTOFINANCIADO	C	Galápagos	SAN CRISTOBAL
UNIVERSIDAD CENTRAL DEL ECUADOR	1005	PÚBLICO	A	Galápagos	SAN CRISTOBAL
UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA	1031	COFINANCIADO	A	Galápagos	SAN CRISTOBAL

(Senescyt, n.d.)

Continua

2.4 Modelo “Trusted Third Party”

Dentro de la comunicación utilizando medios tecnológicos es muy difícil saber con certeza quien es el emisor de un mensaje y cuál es la información que se recibe recibiendo, si dicha información es confiable e integra o si fue alterada durante la transmisión de datos. Por lo tanto, es necesario que los mensajes de datos que se transmiten por la red, sean válidos.

El modelo TTP (Trusted Third Party), conocido en español como TPC (Terceras Partes de Confianza), es una autoridad de seguridad encargada de proporcionar servicios de seguridad, tales como certificados de clave públicos, generación y recuperación de claves, emisión de dinero electrónico, servicios de notaria o registro de evidencias. Para generar estos servicios, la TTP emite pruebas o evidencias para los usuarios que se encuentran en un mismo dominio de seguridad.

La TTP puede estar involucrada en el proceso de intercambio de información entre emisor y receptor, así como puede no operar interactivamente con los elementos de la comunicación, presentando los siguientes casos:

- TTP Fuera de Línea (off-line): Presta servicio únicamente cuando el usuario realiza una petición como se muestra en la Figura 1.

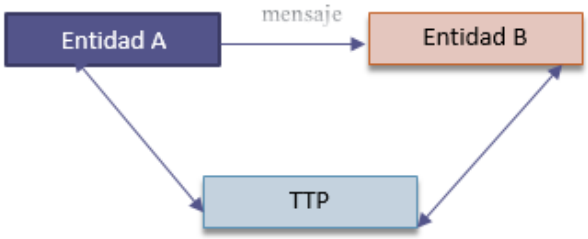

Figura 1. Comunicación usando TTP fuera de línea

- TTP en Línea (on-line): TTC Monitoriza todas las transacciones de la comunicación, sin embargo no está en el camino del emisor hacia el receptor, como se muestra en la Figura 2.

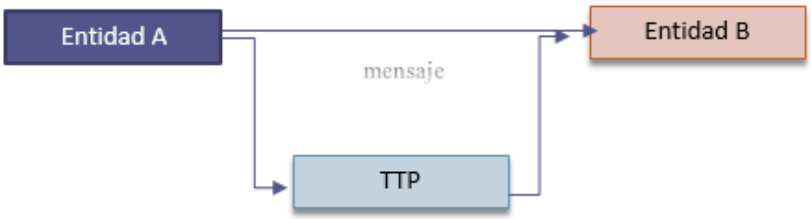

Figura 2. TTP en línea

- TTP dentro de Línea (in-line): TTC está en el camino de intercambio de datos entre el emisor y el receptor del mensaje, como se muestra en la Figura 3.

Figura 3. TTP dentro de línea

Las ventajas al implementar los servicios bajo el modelo TTP (certificación digital, emisión de dinero electrónico, servicios de notaria entre otros) son:

- Comprobar en una comunicación la identidad del emisor del mensaje.
- Asegurarse de que solo obtendrá la información el usuario seleccionado (confidencialidad)

- Asegurarse de que la información no ha sido modificada después de su envío (integridad)
- Asegurarse de que el emisor no puede desdecirse de su propio mensaje (no repudio en origen)

2.5 Normas de Certificación

Las normas son acuerdos documentados que contienen especificaciones técnicas precisas para su uso consecuente como reglas o directrices, para asegurar que productos, procesos y servicios sean correctos. Se debe seguir los siguientes estándares o normas internacionales para prestar servicios de certificación:

2.5.1 Estándar X.509

Es un estándar para infraestructuras de clave pública que especifica los formatos para certificados codificados utilizando ANSI X9, los algoritmos de validación para rutas de certificación y el formato para las listas de revocación de certificados. Los certificados X.509 pueden tener diferentes extensiones entre las que destacan:

- CER- Certificado codificado en CER (mnemónico por certificado), algunas veces es una secuencia de certificados.
- DER- Certificado codificado en DER.
- PEM- Certificado codificado en Base64, encerrado entre -----BEGIN CERTIFICATE----- y -----END CERTIFICATE-----.
- P7C- Estructura PKCS#7, sin datos, solo certificado(s) o CRL(s).

- PFX - Una clave y su correspondiente certificado así como el certificado root y certificados intermedios, pueden ser almacenados en un único archivo .pfx al igual que en un archivo .p12
- P12- PKCS#12, puede contener certificados públicos y claves privadas protegido con clave.

El estándar X.509 desde su primera versión publicada en el año 1988, fue una de las propuestas antiguas de la infraestructura de clave pública PKI. Actualmente se encuentra en la versión 3 cuyos campos se indica en la Figura 4, la misma que permite que los formatos de los certificados y los CRLs sean extensibles, de esta manera los que deseen implementar X.509 podrán definir los contenidos de los certificados. Los campos X.509 son:

- **V:** Denota la versión del certificado
- SN: Representa el número de serie para los CRL
- AL: Identifica el algoritmo de firma que trabaja de forma exclusiva para identificar el algoritmo para firmar el paquete X.509
- CA: Representa la Autoridad Certificadora
- A: Corresponde al propietario de la clave pública que se está firmando
- P: Representa a la clave pública incluida el identificador del algoritmo utilizado y si es necesario los parámetros que sean indispensables.
- Y {I}: Firma digital de Y por l.

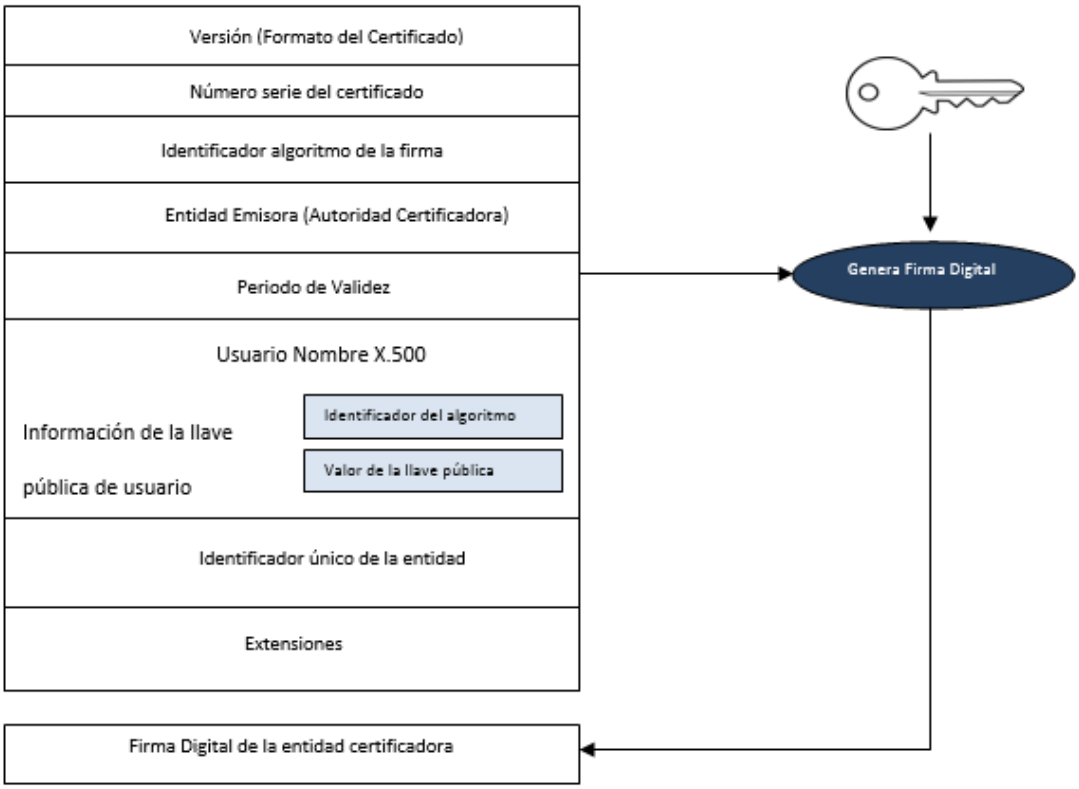

Figura 4. Campos X.509

2.5.2 IETF

El IETF se caracteriza por no ser una organización tradicional, se componen de voluntarios que durante el año realizan reuniones con un límite de tres reuniones anuales para poder cumplir con la misión que se han trazado.

IETF desarrollo estándares denominados PKIx, conjunto a las operaciones de in-fraestructuras de Clave Pública que estarán basadas en certificados X.509 que fueron tomados de los distintos países donde se trabajaba con Autoridades de Certificación.

CAPÍTULO 3

MARCO LEGAL

Este capítulo recopila información de los reglamentos y estándares establecidos en nuestro país enfocada a las normas y políticas que se establecerán para el PKI del Sistema Nacional de Educación.

Las leyes proporcionan el marco jurídico que abalara las transacciones a nivel electrónico, de esta forma se permitirá equilibrar la información jurídica entre los documentos físicos y documentos electrónicos.

La ley de comercio electrónico regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas, según el Art. 2 de la Ley de Comercio Electrónico: "Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento".

3.1 Análisis Ley de Comercio Electrónico

La Ley No. 67 correspondiente, al Registro Oficial Suplemento No. 557, de 17 de abril del 2002, se expidió la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, que permite conocer los parámetros legales bajo los cuales se puede ejecutar y establecer las normas, políticas y procedimientos en un PKI basado en un Smart Grid

para el Sistema Nacional de Educación. Los artículos que se consideran propicios para este estudio se definen a continuación.

3.1.1 De las Firmas Electrónicas

En Ecuador se define el término de Firma Electrónica como los datos asignados en un mensaje de datos donde el autor del mensaje se hace responsable de su contenido. La firma electrónica es legamente válida al igual que una firma manuscrita y el autor es responsable de los datos firmados, aplicando al no repudio. Para firmar electrónicamente se debe cumplir requisitos que se mencionan en el Art. 15 de la Ley de Comercio Electrónico.

El uso de la firma electrónica rige obligaciones al autor para evitar la utilización no autorizada de la misma. La duración y validez de la firma electrónica se menciona en los Art.18 y Art. 19 de la Ley de Comercio Electrónico. A continuación, se mencionan los artículos del 13 al 19 correspondientes a la Firma Electrónica.

Art. 13.- Firma electrónica.- "Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos".

Art. 14.- Efectos de la firma electrónica.- "La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en

relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio".

Art. 15.- Requisitos de la firma electrónica.- "Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular;
b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;
c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;
d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, y,
e) Que la firma sea controlada por la persona a quien pertenece".

Art. 16.- La firma electrónica en un mensaje de datos.- "Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas, en dicho mensaje de datos, de acuerdo a lo determinado en la ley".

Art. 17.- Obligaciones del titular de la firma electrónica.- "El titular de la firma electrónica deberá:

- Cumplir con las obligaciones derivadas del uso de la firma electrónica;
- Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;

a) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;
b) Verificar la exactitud de sus declaraciones;
c) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere
d) Obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;
e) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,
f) Las demás señaladas en la ley y sus reglamentos".

Art. 18.- Duración de la firma electrónica.- "Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale".

Art. 19.- Extinción de la firma electrónica.-"La firma electrónica se extinguirá por:

a) Voluntad de su titular;

b) Fallecimiento o incapacidad de su titular;

c) Disolución o liquidación de la persona jurídica, titular de la firma; y,

d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso".

3.1.2 De los Certificados de Firma Electrónica

Los certificados de firma electrónica comprueban la identidad del autor de la firma, para obtenerlos se debe cumplir con requisitos establecidos en el Art. 22 de la Ley de Comercio Electrónico. Los certificados electrónicos tienen tiempo de validez, pueden extinguirse, suspenderse o revocar, los certificados internacionales se los puede reconocer en el Ecuador si cumplen con los artículos establecidos en la ley y el reglamento del Comercio Electrónico. A continuación se mencionan los artículos del 20 al 28 correspondientes a los Certificados de Firma Electrónica.

Art. 20.- Certificado de firma electrónica.- "Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad".

Art. 21.- Uso el certificado de firma electrónica.- "El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta ley y su reglamento".

Art. 22.- Requisitos del certificado de firma electrónica.- "El Certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:

a) Identificación de la entidad de certificación de información;
b) Domicilio legal de la entidad de certificación de información;
c) Los datos del titular del certificado que permitan su ubicación e identificación;
d) El método de verificación de la firma del titular del certificado;
e) Las fechas de emisión y expiración del certificado;
f) El número único de serie que identifica el certificado;
g) La firma electrónica de la entidad de certificación de información;
h) Las limitaciones o restricciones para los usos del certificado; e,
i) Los demás señalados en esta ley y los reglamentos".

Art. 23.- Duración del certificado de firma electrónica.- "Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta ley".

Art. 24.- Extinción del certificado de firma electrónica.- "Los certificados de firma electrónica, se extinguen, por las siguientes causas:

a) Solicitud de su titular;
b) Extinción de la firma electrónica, de conformidad con lo establecido en el artículo 19 de esta ley; y,
c) Expiración del plazo de validez del certificado de firma electrónica.

La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir

de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso".

Art. 25.- Suspensión del certificado de firma electrónica.- "La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:

a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley;
b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,
c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.

La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica".

Art. 26.- Revocatoria del certificado de firma electrónica.- "El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley, cuando:

a) La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,
b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada.

La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado".

Art. 27.- "Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso".

Art. 28.- Reconocimiento internacional de certificados de firma electrónica.- "Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos

en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta ley y su reglamento. Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores".

3.1.3 De las Entidades de Certificación de Información

Las Entidades de Certificación de Información son empresas que emiten certificados de firma electrónica y son responsables del uso que se les dé a dichos certificados, son autorizadas por el Consejo Nacional de Telecomunicaciones y deben cumplir obligaciones mencionadas en el Art. 30 de la Ley de Comercio Electrónico. A continuación se mencionan los artículos del 29 al 35 correspondientes a las Entidades de Certificación de Información.

Art. 29.- Entidades de certificación de información.- "Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República".

Art. 30.- Obligaciones de las entidades de certificación de información acreditadas.- "Son obligaciones de las entidades de certificación de información acreditadas:

a) Encontrarse legalmente constituidas, y estar registradas en Consejo Nacional de Telecomunicaciones;
b) Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios;
c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información,
d) Mantener sistemas de respaldo de la información relativa a los certificados;
e) Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que se especifiquen en esta ley;
f) Mantener una publicación del estado de los certificados electrónicos emitidos;
g) Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido;

h) Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados; e,

i) Las demás establecidas en esta ley y los reglamentos".

Art. 31.- Responsabilidades de las entidades de certificación de información acreditadas.- "Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso.

Cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio".

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- "Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley".

Art. 33.- Prestación de servicios de certificación por parte de terceros.- "Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

El Consejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros".

Art. 34.- Terminación contractual.- "La terminación del contrato entre las entidades de certificación acreditadas y el suscriptor se sujetará a las normas previstas en la Ley Orgánica de Defensa del Consumidor".

Art. 35.- Notificación de cesación de actividades.- "Las entidades de certificación de información acreditadas, deberán notificar al Organismo de Control, por lo menos con noventa días de anticipación, la cesación de sus actividades y se sujetarán a las

normas y procedimientos establecidos en los reglamentos que se dicten para el efecto".

3.1.4 Servicios de Certificación

Los servicios de firma electrónica y la emisión de certificados por parte de Entidades de Certificación de Información Acreditadas iniciaron en Ecuador a partir de la propuesta normalizada en el año 2002 mediante la emisión de la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos.

Las entidades de certificación de información y servicios relacionados son trascendentes para la validez de la firma electrónica al generar, administrar y gestionar los certificados electrónicos, cada firma electrónica está vinculada a un certificado electrónico para garantizar la identidad y autoría del emisor.

Para poder operar como Entidad de Certificación, se debe realizar una solicitud al Consejo Nacional de Telecomunicaciones para obtener un título habilitante, previamente, la empresa debe encontrarse legalmente establecida y representada en el país, además de cumplir con todos los requisitos necesarios que las normativas los exige. (Proasetel, 2003)

Según la legislación ecuatoriana se toma como referencia la ley llamada "Ley Modelo de CNUDMI-UNCITRAL", la cual establece los requisitos legales y técnicos que deben cumplir las empresas para calificarse como autoridad certificadora entre los que se encuentran:

Los requisitos legales requeridos son:

- Identificación y generales de ley del solicitante, socios y representantes con los certificados: nombramientos, contratos de prestación de servicios.
- Certificados de antecedentes penales.
- Certificados profesionales.
- Certificados legales en general de acuerdo al tipo de servicio a prestar.

Los requisitos técnicos necesarios son:

- Diagrama esquemático y descripción técnica detallada del sistema.
- Descripción detallada de cada servicio propuesto y de los recursos e infraestructura disponibles para su prestación.
- Documentos de soporte que confirmen que se disponen de medidas para evitar la falsificación de certificados y, en el caso que el Proveedor de Servicios de Certificación intervenga en la generación de claves criptográficas privadas, se garantice la seguridad y confidencialidad durante el proceso de generación de dichas claves" (Proasetel, 2003)

3.1.5 Organismos de promoción y difusión de los servicios electrónicos y de regulación y control de las entidades de certificación acreditadas

La autorización, registro, regulación de las entidades de certificación acreditadas en el Ecuador, así como sus respectivas funciones se los detalla en los artículos 36 al 43 de la Ley de Comercio Electrónico.

Art. 36.- Organismo de promoción y difusión.-"Para efectos de esta ley, el Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción

y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior".

Art. 37.- Organismo de regulación, autorización y registro de las entidades de certificación acreditadas.- "El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas. En su calidad de organismo de autorización podrá además:

a) Cancelar o suspender la autorización a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones;
b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones; y
c) Las demás atribuidas en la ley y en los reglamentos".

Art. 38.- Organismo de control de las entidades de certificación de información acreditadas.- "Para efectos de esta ley, la Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas".

Art. 39.- Funciones del organismo de control.- "Para el ejercicio de las atribuciones establecidas en esta ley, la Superintendencia de Telecomunicaciones tendrá las siguientes funciones:

a) Nota: Literal derogado por Ley No. 0, publicada en Registro Oficial Suplemento 555 de 13 de Octubre del 2011.
b) Ejercer el control de las entidades de certificación de información acreditadas en el territorio nacional y velar por su eficiente funcionamiento;
c) Realizar auditorías técnicas a las entidades de certificación de información acreditadas;
d) Requerir de las entidades de certificación de información acreditadas, la información pertinente para el ejercicio de sus funciones;
e) Imponer de conformidad con la ley sanciones administrativas a las entidades de certificación de información acreditadas, en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio;
f) Emitir los informes motivados previstos en esta ley;
g) Disponer la suspensión de la prestación de servicios de certificación para impedir el cometimiento de una infracción; y,
h) Las demás atribuidas en la ley y en los reglamentos".

Art. 40.- Infracciones administrativas.- "Para los efectos previstos en la presente ley, las infracciones administrativas se clasifican en leves y graves.

Infracciones leves:

1. La demora en el cumplimiento de una instrucción o en la entrega de información requerida por el organismo de control; y,
2. Cualquier otro incumplimiento de las obligaciones impuestas por esta ley y sus reglamentos a las entidades de certificación acreditadas.

Estas infracciones serán sancionadas, de acuerdo a los literales a) y b) del artículo siguiente.

Infracciones graves:

1. Uso indebido del certificado de firma electrónica por omisiones imputables a la entidad de certificación de información acreditada;
2. Omitir comunicar al organismo de control, de la existencia de actividades presuntamente ilícitas realizada por el destinatario del servicio;
3. Desacatar la petición del organismo de control de suspender la prestación de servicios de certificación para impedir el cometimiento de una infracción;
4. El incumplimiento de las resoluciones dictadas por los Organismos de Autorización Registro y Regulación, y de Control; y,
5. No permitir u obstruir la realización de auditorías técnicas por parte del organismo de control.

Estas infracciones se sancionarán de acuerdo a lo previsto en los literales c) y d) del artículo siguiente.

Las sanciones impuestas al infractor, por las infracciones graves y leves, no le eximen del cumplimiento de sus obligaciones.

Si los infractores fueren empleados de instituciones del sector público, las sanciones podrán extenderse a la suspensión, remoción o cancelación del cargo del infractor, en cuyo caso deberán observarse las normas previstas en la ley.

Para la cuantía de las multas, así como para la gradación de las demás sanciones, se tomará en cuenta:

a) La gravedad de las infracciones cometidas y su reincidencia;
b) El daño causado o el beneficio reportado al infractor; y",

Art. 41.- Sanciones.- "La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

a) Amonestación escrita;
b) Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;
c) Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica; y,
d) Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica".

Art. 42.- Medidas cautelares.- "En los procedimientos instaurados por infracciones graves, se podrá solicitar a los órganos judiciales competentes, la adopción de las medidas cautelares previstas en la ley que se estimen necesarias, para asegurar la eficacia de la resolución que definitivamente se dicte".

Art. 43.- Procedimiento.- "El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones".

3.2 Análisis del Reglamento a la Ley de Comercio Electrónico

El Reglamento a la Ley de Comercio Electrónico complementa y describe cómo aplicar la Ley mencionada.

3.2.1 De las Firmas Electrónicas

Los elementos que respaldan a la firma electrónica se los detalla en el Art. 10 del Reglamento a la Ley de Comercio Electrónico que se mencionan a continuación.

Art. 10.- Elementos de la infraestructura de firma electrónica.- "La firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y este reglamento.

Los principios y elementos que respaldan a la firma electrónica son:

a) No discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada;
b) Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente;

c) El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b);

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; y,

d) Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación".

3.2.2 De los Certificados de Firma Electrónica

En el Reglamento a la Ley de Comercio Electrónico se describe la duración, revocación, extinción y suspensión de los certificados de firma electrónica, los artículos que hacen referencia son los siguientes:

Art. 11.- Duración del certificado de firma electrónica.- "La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos

años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en la leyes".

Art. 12.- Listas de revocación.- "Las entidades de certificación de información proporcionarán mecanismos automáticos de acceso a listas de certificados revocados o suspendidos de acuerdo al artículo 26 de la Ley 67. Cuando la verificación de la validez de los certificados de firma electrónica no sea posible de realizar en tiempo real, la entidad de certificación de información comunicará de este hecho tanto al emisor como al receptor del mensaje de datos.

Los períodos de actualización de las listas de certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente".

Art. 13.- Revocación del certificado de firma electrónica.- "Establecidas las circunstancias determinadas en la Ley 67, se producirá la revocación, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado.

En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades.

La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado.

La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la Ley 67 y este reglamento".

Art. 14.- De la notificación por extinción, suspensión o revocación del certificado de firma electrónica.- "La notificación inmediata al titular del certificado de firma electrónica, de acuerdo al artículo 26 de la Ley 67, se hará a la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio, luego de la extinción, suspensión o revocación del certificado".

Art. 15.- Publicación de la extinción, revocación y suspensión de los certificados de firma electrónica y digital.- "La publicación a la que se refiere el artículo 27 de la Ley 67, se deberá hacer por cualquiera de los siguientes medios:

a) Siempre en la página electrónica determinada por el CONATEL en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora; y,
b) Mediante un aviso al acceder al certificado de firma electrónica desde el hi-pervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un directorio electrónico o por cualquier procedimiento por el cual se consulta los datos del certificado de firma electrónica.

Opcionalmente, en caso de que la entidad certificadora o el tercero vinculado relacionada crean conveniente, se podrá hacer la publicación en uno de los medios de comunicación pública".[1]

Art. 16.- "Sin perjuicio de la reglamentación que emita el CONATEL, para la aplicación del artículo 28 de la Ley No. 67, los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en el Ecuador una vez obtenida la revalidación respectiva por una Entidad de Certificación de Información y Servicios Relacionados Acreditada ante el CONATEL, la cual deberá comprobar el grado de fiabilidad de dichos certificados y de quien los emite".[2]

---

[1] Artículo reformado por Decreto Ejecutivo No. 908, publicado en Registro Oficial 168 de 19 de Diciembre del 2005.

Artículo reformado por Decreto Ejecutivo No. 1356, publicado en Registro Oficial 440 de 6 de Octubre del 2008.

[2] Artículo reformado por Decreto Ejecutivo No. 908, publicado en Registro Oficial 168 de 19 de Diciembre del 2005.

Artículo sustituido por Decreto Ejecutivo No. 1356, publicado en Registro Oficial 440 de 6 de Octubre del 2008

3.2.3 De las Entidades de Certificación de Información

En el Reglamento a la Ley de Comercio Electrónico se detallan como obtener la acreditación de entidades de certificación.

Art. 17.- Régimen de acreditación de entidades de certificación de información.- "Para obtener autorización de operar directamente o a través de terceros relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONATEL.

Los certificados de firma electrónica emitidos y revalidados por las Entidades de Certificación de Información y Servicios Relacionados Acreditadas por el CONATEL, tienen carácter probatorio.

Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acrediten en el CONATEL, tendrán la calidad de entidades de certificación de información no acreditadas y están obligadas a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten".[3]

---

[3] Artículo reformado por Decreto Ejecutivo No. 908, publicado en Registro Oficial 168 de 19 de Diciembre del 2005.

Art. ...- Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y terceros vinculados: "Se crea el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y terceros vinculados, a cargo de la Secretaría Nacional de Telecomunicaciones. El CONATEL emitirá la reglamentación que permita su organización y funcionamiento".[4]

3.2.4 Servicios de Certificación

Según el Reglamento a la Ley de Comercio Electrónico se consideran los siguientes artículos relacionados con los servicios de Certificación:

Art. 21.- "De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que

---

Segundo inciso sustituido por Decreto Ejecutivo No. 1356, publicado en Registro Oficial 440 de 6 de Octubre del 2008

4 Artículo agregado por Decreto Ejecutivo No. 1356, publicado en Registro Oficial 440 de 6 de Octubre del 2008

utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades.

Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidas en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones"

Art. 22.- Envío de mensajes de datos no solicitados.- "El envío periódico de información, publicidad o noticias promocionando productos o servicios de cualquier tipo observará las siguientes disposiciones:

a) Todo mensaje de datos periódico deberá incluir mecanismos de suscripción y descripción (sic);
b) Se deberá incluir una nota indicando el derecho del receptor a solicitar se le deje de enviar información no solicitada;
c) Deberá contener información clara del remitente que permita determinar inequívocamente el origen del mensaje de datos;
d) A solicitud del destinatario se deberá eliminar toda información que de él se tenga en bases de datos o en cualquier otra fuente de información empleada para el envío de mensajes de datos periódicos u otros fines no expresamente autorizados por el titular de los datos; y,
e) Inmediatamente de recibido por cualquier medio la solicitud del destinatario para suscribirse del servicio o expresando su deseo de no continuar recibiendo mensajes de datos periódicos, el emisor deberá cesar el envío de los mismos a la dirección electrónica correspondiente.

Las solicitudes de no envío de mensajes de datos periódicos, se harán directamente por parte del titular de la dirección electrónica de destino.

Los proveedores de servicios electrónicos o comunicaciones electrónicas, a solicitud de cualquiera de sus titulares de una dirección electrónica afectado por el envío periódico de mensajes de datos no solicitados, procederán a notificar al remitente de dichos correos sobre el requerimiento del cese de dichos envíos y de comprobarse que el remitente persiste en enviar mensajes de datos periódicos no solicitados podrá bloquear el acceso del remitente a la dirección electrónica afectada".

Art. 23.- Sellado de tiempo.- "Para la prestación de los servicios de sellado de tiempo, el mensaje de datos debe ser enviado a través de la entidad certificadora o un tercero debidamente registrado en el CONATEL para prestar este servicio. El sellado de tiempo únicamente establecerá para los fines legales pertinentes, la hora y fecha exacta en que el mensaje de datos fue recibido por la entidad certificadora o el tercero registrado por el CONATEL; y la fecha y hora exacta en dicho mensaje de datos fue entregado al destinatario.

Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano. La prestación de servicios de sellado de tiempo se realizará en régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios podrán determinar las condiciones que regulan su relación.[5]

Disposición Transitoria.- Los trámites pendientes relacionados con la acreditación como Entidades de Certificación de Información y Servicios Relacionados deberán adecuarse a lo dispuesto en este decreto".[6]

---

[5] Artículo reformado por Decreto Ejecutivo No. 908, publicado en Registro Oficial 168 de 19 de Diciembre del 2005.

[6] Disposición agregada por Decreto Ejecutivo No. 1356, publicado en Registro Oficial 440 de 6 de Octubre del 2008

3.3 Entidades de Certificación Acreditadas y No Acreditadas

En Ecuador el Consejo Nacional de Telecomunicaciones "CONATEL" es el organismo de autorización registro y regulación de las entidades de certificación de información acreditadas, este organismo tiene la autoridad de cancelar o suspender la autorización a las entidades de certificación acreditadas, revocar o suspender los certificados de firma electrónica.

3.3.1 Entidades de Certificación Acreditadas

La acreditación de una entidad certifica el reconocimiento mutuo de los organismos de certificación a nivel internacional. "Los objetivos de la acreditación son:

- Declarar la competencia e imparcialidad de los organismos acreditados;
- Adquirir la aceptación de las prestaciones y el reconocimiento de las competencias a nivel internacional.
- Unifica y simplifica los trámites de reconocimiento de los operadores;
- Evita a las empresas exportadoras los reiterados controles que deben pasar para tener acceso a los mercados internacionales;
- Establece y promueve la confianza a nivel nacional e internacional al comprobar la competencia de los operadores en cuestión." (FAO, n.d.)

Para que una Entidad de Certificación pueda ser operativa directamente o por terceros, debe registrarse directamente en el CONATEL, sin embargo, este organismo regulador no informa sobre los procedimiento que necesita una empresa realizar para prestar servicios para ser autorizada y acreditada. La Superintendencia de Teleco-

municaciones es el organismo encargado del control de las entidades de certificación de información acreditadas.

La Ley de Comercio Electrónico en el Ecuador, exige a las Entidades de Certificación solvencia técnica, logística y financiera para la emisión de certificados sobre la autenticación de las firmas electrónicas.

El Banco Central del Ecuador es la Entidad de Certificación de Información acreditada por el Consejo Nacional de Telecomunicaciones, mediante Resolución 481-20-CONATEL-2008 de 8 de octubre de 2008 y acto administrativo suscrito el 6 de noviembre de 2008.

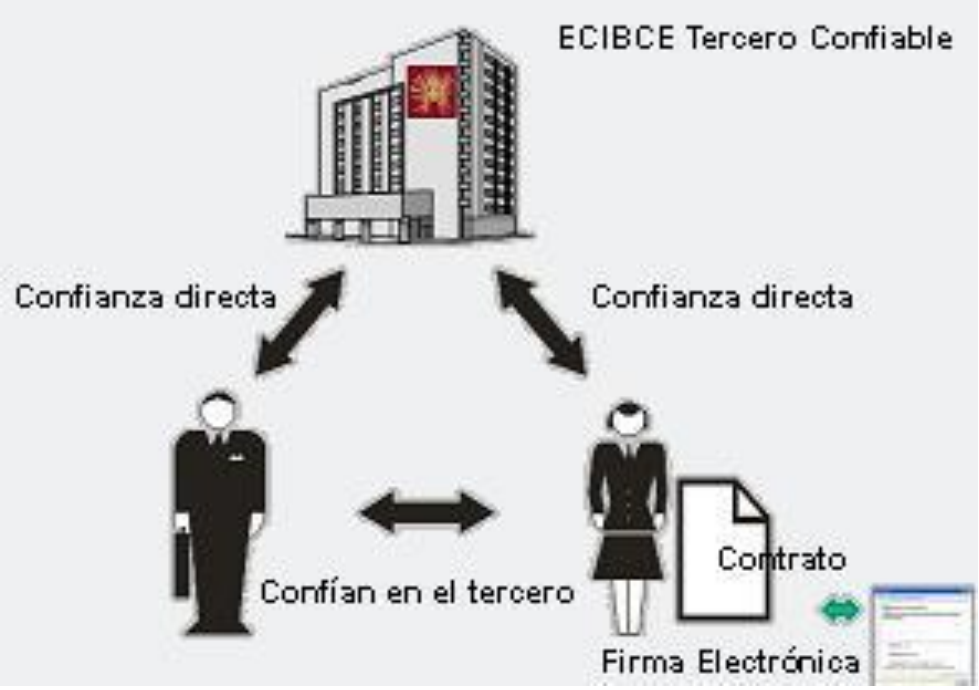

Figura 5. ECIBCE

Fuente: (Certificación Electrónica Banco Central del Ecuador, 2015)

En la siguiente figura muestra la página web de la Certificación Digital del Banco Central del Ecuador:

Figura 6. Página de Certificación Electrónica del Banco Central del Ecuador

Fuente: (Ecuador, www.eci.bce.ec, 2015)

El Consejo de la Judicatura fue acreditado como Entidad de Certificación de Información y Servicios Relacionados ante el estado ecuatoriano por el Consejo Nacional de Telecomunicaciones el 28 de julio del 2014, por tanto alcanza el derecho para instalar, modificar, ampliar y operar la infraestructura requerida para prestar servicios como AC Acreditada y debe cumplir con las disposiciones contenidas en la Ley de Comercio Electrónico y Mensajes de Datos. En la siguiente figura muestra la página web del Consejo de la Judicatura:

Figura 7. Página Web Consejo de la Judicatura

Fuente: (Judicatura, 2015)

ANF es una Autoridad de Certificación ofrece soluciones para la emisión y recepción de factura electrónica cumpliendo con la normativa fiscal y legal. Además, es la primera CA acreditada oficialmente de España y opera en Ecuador desde el año 2010 está equipada con la tecnología necesaria para emitir certificados electrónicos reconocidos, firma electrónica avanzada, sellos digitales de tiempo y verificación en línea del estado del certificado empleado. En la siguiente figura muestra la página web de la Certificación Digital del ANF Autoridad de Certificación:

Figura 8. Página Web ANF Autoridad de Certificación

Fuente: (Certificación, 2015)

Security Data Seguridad en Datos y Firma Digital S.A es una Entidad Certificadora de firma electrónica y servicios relacionados autorizada por el CONATEL según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Los servicios de Certificación de Información y Servicios Relacionados ofrecidos por Security Data Seguridad en Datos y Firma Digital están orientados a Corporaciones Públicas y Privadas y su objetivo es acreditar la identidad digital de las corporaciones y las personas naturales que actúan a través de la red. (Data, 2015). En la siguiente figura muestra la página web de la Certificación Digital de Security Data:

Figura 9. Página Web Security Data

Fuente: (Data, 2015)

3.3.2 Entidades de Certificación No Acreditadas

La Ley de Comercio Electrónico impone a las entidades de certificación un régimen obligatorio de autorización previa y de registro, sin embargo las entidades de certificación No Acreditadas están registradas y tienen autorización para ser operativas en forma directa o por terceros relacionados en Ecuador. Las entidades de certificación No Acreditadas no fueron acreditadas en el CONATEL y tienen la obligación de probar la fiabilidad de los certificados que son emitidos y corroborar la suficiencia técnica adecuada.

La Ley de Comercio Electrónico anuncia la posibilidad de que existan entidades inscritas y acreditadas, y otras que, pese a estar inscritas, tengan la calidad de No Acreditadas. En el Art. 9 dispuesto en la Resolución 584 menciona a la acreditación como un requisito opcional.

Art. 9.- "De acuerdo a lo que establece la Ley de Comercio Electrónico y su reglamento, se dispone la implementación de un sistema de acreditación voluntario para las entidades de certificación de información en la emisión de firmas electrónicas y certificados de firma electrónica. Los certificados y firmas electrónicas emitidos por las entidades de certificación de información acreditadas y las entidades de registro relacionadas, se denominarán certificados de firma electrónica acreditados y gozarán de la presunción establecida en el Art. 53 de la Ley de Comercio Electrónico, en tanto que los certificados y firmas electrónicas emitidos por las entidades de certificación de información no acreditadas, directamente o a través de terceros, se denominarán certificados de firma electrónica no acreditados, siendo responsabilidad del usuario probar su validez cuando sea requerido por autoridad competente".

Las entidades de certificación no acreditadas cuentan con menos privilegios que las acreditadas, los organismos extranjeros tienen la obligación de ser acreditados para poder ser registrados en el país, así como para los organismos y entidades del sector público es prohibido utilizar cualquier servicio prestado por entidades No Acreditadas, según el Art. 7 de la resolución 584

Art. 6.- "Las entidades extranjeras de certificación de información para emisión de firmas electrónicas y certificados de firma electrónica, no domiciliadas en Ecua-

dor, podrán solicitar su registro en el país, previo a demostrar la acreditación o reconocimiento legal de los servicios prestados en el extranjero, a través de su apoderado en el Ecuador.

El registro no otorga la calidad de entidad de certificación acreditada en el país, por lo que se deberá hacer constar en el contrato con los usuarios e informar al público en la promoción o publicidad de tal calidad."

Art. 7.- "Al tratarse de servicios de certificación de información empleadas en actos públicos o que involucren a instituciones del sector público, se requerirá a los prestadores de estos servicios estar acreditados en CONATEL de modo obligatorio."

3.4 Estándares y Normas internacionales de servicios de certificación digital.

Los estándares son documentos técnicos legales establecidos por una norma que describe lineamientos a seguir para cumplir procedimientos, son elaboradas por consenso de las partes interesadas como fabricantes, administraciones, usuarios y consumidores, centros de investigación y laboratorios, asociaciones o agentes sociales.

Las normas se basan en los resultados de la experiencia y el desarrollo tecnológico, dan paso a establecer un punto en común de comunicación entre las empresas, la administración y los usuarios, permiten fijar la terminología, atributos, características y prescripciones aplicables de un servicio o producto, para preservar la seguridad y favorecer el efectivo intercambio de información. Las normas y estándares son aprobados por organismos nacional, regional o internacional de normalización reconocidos como:

- IEEE: Institute of Electrical and Electronics Engineers, es la mayor organización profesional dedicada al avance en la innovación de tecnología para el beneficio de la humanidad.
- ISO: International Organization for Standardization, permite la búsqueda de las normas certificadas por esta institución.
- ANSI: American National Standards Institute, organización nacional de normalización norteamericana, permite acceder a su propio catálogo de normas y al de diferentes entidades normativas norteamericanas e internacionales.
- CENELEC: Comité Europeo de Normalización Electrotécnica es el organismo europeo de normalización para la electrónica.
- IEC: International Electrotechnical Commission, organismo que elabora normas internacionales sobre electricidad, electrónica y tecnologías relacionadas.
- NIST: National Institute of Standards and Technology, organismo que depende de U.S. Commerce Department's Technology Administration, su fin es elaborar normas para aumentar la productividad, facilitar el comercio y elevar la calidad de vida.

El cumplimiento de normas internacionales no es de carácter obligatorio, sin embargo es un requisito indispensable para ingresar a ciertos mercados. Para obtener una certificación se divide en 3 pasos básicos:

1. La implementación: Consiste en plasmar las normas técnicas de la certificación dentro de los procesos de la empresa.
2. La inspección: Consiste en la revisión de un técnico enviado por la empresa certificadora que verifica que todas las nomas que incluyen en la certificación estén dentro de la empresa.
3. La certificación: Una vez el técnico emite el informe definitivo con las correcciones implementadas, se envía a la matriz la solicitud de certificado para que posteriormente sea otorgado a la empresa.

Para establecer estándares estos deben apropiados, efectivos, maduros, de ágil disponibilidad, confiables y consistentes con aquellos que se encuentran ampliamente difundidos y que cuentan con aceptación internacional, además tener parámetros de evaluación para futuras modificaciones.

3.5 Análisis del Reglamento PKI

En los artículos del reglamento PKI se indica los lineamientos para los registros de regulación de entidades de certificación habilitantes para prestar el servicio de certificación de información, cumpliendo las normas y requisitos de una entidad certificadora.

3.5.1 Reglamento para la acreditación, registro y regulación de entidades habilitadas para prestar servicios de certificación de información y servicios relacionados.

Las leyes que se presentan a continuación permiten trabajar bajo normas y procedimientos para realizar la prestación de servicios de certificación de información, así como las obligaciones que debe cumplir para la obtención de estos servicios. Estos se detallan en los artículos del 1 al 9.

Artículo 1. "El presente Reglamento tiene por objeto establecer las normas y procedimientos aplicables a la prestación de servicios de certificación de información, emisión de firmas electrónicas y certificados de firma electrónica, registro de datos y sellado de tiempo, y a la operación de una infraestructura de Clave Pública en Ecuador, así como los deberes y derechos de los prestadores de estos servicios y de sus usuarios."

Artículo 2."Las definiciones de los términos técnicos relacionados con el presente reglamento serán las establecidas por la Unión Internacional de Telecomunicaciones – UIT, la Comunidad Andina de Naciones – CAN, la Ley de Comercio Electrónico y su Reglamento así como aquellas que se incorporen en el presente Reglamento."

Artículo 3. "La Infraestructura de Clave Pública la constituyen los programas y equipos, sistemas de información, redes electrónicas de información, políticas y procedimientos cuya finalidad es soportar la operación de los servicios de certificación de información y servicios relacionados."

Son servicios de certificación de información entre otros:

a) Emisión de firmas electrónicas y certificados de firma electrónica.
b) Sellado electrónico de tiempo.
c) Certificación electrónica de documentos a cargo de un notario público o autoridad competente empleando firma electrónica.
d) Conservación de mensajes de datos
e) Otros que empleen la infraestructura de clave pública y sean aprobados por el CONATEL."

Artículo 4." Los dispositivos hardware o software de producción y de verificación de firma electrónica se basarán en la aplicación de algoritmos públicamente conocidos de entre los que sean de general aceptación por la comunidad internacional, tanto en la producción de resúmenes de documento (huella electrónica o hash) como en la de la firma electrónica propiamente dicha.

No serán admisibles dispositivos cuya funcionalidad se base en algoritmos secretos o desconocidos ni los que hayan sido excluidos en los términos del párrafo anterior."

Artículo 5."Es responsabilidad de las entidades acreditadas emitir certificados únicos e induplicables. Cada certificado deberá contener un identificador exclusivo que lo distinga de forma unívoca ante el resto. Solo podrán emitirse certificados vinculados a personas naturales mayores de edad, con plena capacidad de obrar.

Está prohibida por parte de las entidades acreditadas, la emisión de certificados de prueba o demostración. “

Artículo 6.” Las entidades extranjeras de certificación de información para emisión de firmas electrónicas y certificados de firma electrónica, no domiciliadas en Ecuador, podrán solicitar su registro en el País, previo a demostrar la acreditación o reconocimiento legal de los servicios prestados en el extranjero, a través de su apoderado en el Ecuador. El Registro no otorga la calidad de entidad de certificación acreditada en el país, por lo que se deberá hacer constar en el contrato con los usuarios e informar al público en la promoción o publicidad de tal calidad.”

Artículo 7.” Al tratarse de servicios de certificación de información empleadas en actos públicos o que involucren a instituciones del sector público, se requerirá a los prestadores de estos servicios estar acreditados en CONATEL de modo obligatorio.”

Artículo 8.”Una entidad de registro de información es un tercero acreditado en el CONATEL, relacionado contractual y legalmente con una entidad de certificación de información acreditada o con una entidad de certificación extranjera registrada por el CONATEL y que está autorizada para representarla legalmente y prestar servicios de certificación de información y relacionados, a nombre o en representación de la misma. Estos servicios pueden incluir:

a) Recopilación y custodia de información y documentos de soporte requeridos para la emisión de firmas electrónicas y certificados de firma electrónica.
b) Instalación y soporte de aplicaciones relacionadas con el uso y verificación de firmas electrónicas y certificados de firma electrónica.

c) Otros servicios requeridos para la prestación de servicios de certificación de información por parte de la entidad de certificación de información acreditada o entidad de certificación de información extranjera registrada y autorizada por el CONATEL para prestar dichos servicios en el País."

Artículo 9." De acuerdo a lo que establece la Ley de Comercio Electrónico y su Reglamento, se dispone la implementación de un sistema de acreditación voluntario para las entidades de certificación de información en la emisión de firmas electrónicas y certificados de firma electrónica. Los certificados y firmas electrónicas emitidos por las entidades de certificación de información acreditadas y las entidades de registro relacionadas, se denominarán certificados de firma electrónica acreditados y gozarán de la presunción establecida en el Art. 53 de la Ley de Comercio Electrónico, en tanto que los certificados y firmas electrónicas emitidos por las entidades de certificación de información no acreditadas, directamente o a través de terceros, se denominarán certificados de firma electrónica no acreditados, siendo responsabilidad del usuario probar su validez cuando sea requerido por autoridad competente.

En el contrato con los usuarios de estos servicios y en la publicidad y promoción de los mismos por cualquier medio, se hará constar la calidad de acreditado o no acreditado y los derechos y obligaciones que los usuarios tienen en tales calidades.

En los actos públicos o relacionados con instituciones del sector público se estará a lo dispuesto en el artículo 4 del presente Reglamento."

3.5.2 De los Títulos Habilitantes

Estos artículos presentan la información para obtener el cumplimiento por parte del prestador de servicios y que estas se encuentren legalmente establecidas dentro del país, esto permite que se pueda controlar el cumplimiento para poder realizar procesos correspondientes o suspensión de permisos siendo el caso de que existan procedimientos sin cumplir, para que se pueda llevar a cabo el registro. La acreditación es realizada por medio de la obtención de un título habilitante que será entregado por parte de la Secretaría Nacional de Telecomunicaciones con previa autorización del Consejo Nacional de Telecomunicaciones. Toda esta información es detallada en los artículos 10 al 17.

Artículo 10.” El otorgamiento de un permiso o registro, requiere que el prestador de servicios de certificación de información se encuentre legalmente establecido y representado en el País. El órgano de control verificará el cumplimiento de esta condición y podrá solicitar la suspensión del permiso o registro en caso de incumplimiento de este requisito o cese del establecimiento o representación legal en el País. Es obligación del prestador de servicios de certificación de información, el reportar inmediatamente al órgano regulador y al órgano de control para su conocimiento y aprobación todo cambio en el establecimiento o en la representación legal en el País o en las condiciones técnicas, comerciales o legales que fundamentaron el otorgamiento del permiso o registro.”

Artículo 11.” La acreditación para la prestación de servicios de certificación de información y servicios relacionados por parte de las entidades de certificación de

información o entidades de registro de información se obtendrá a través de un título habilitante que será el permiso y registro de operación, otorgado por la Secretaría Nacional de Telecomunicaciones, SENATEL, previa autorización del Consejo Nacional de Telecomunicaciones, CONATEL,

El permiso para la prestación de servicios de certificación de información y servicios relacionados comprende el derecho para la instalación, modificación, ampliación y operación de la infraestructura requerida para proveer tales servicios, de conformidad con las condiciones establecidas en el título habilitante y la normativa vigente.

Todo permisionario para la prestación de servicios de servicios de certificación de información y servicios relacionados deberá cancelar previamente a la Secretaría Nacional de Telecomunicaciones, por concepto de derechos de permiso, el valor que el Consejo Nacional de Telecomunicaciones determine para cada tipo de servicio.

Los costos de administración de contratos, registro, control y gestión serán retribuidos mediante tasas fijadas por los organismos de control y de administración, en función de los costos administrativos que demanden dichas tareas para cada uno de los organismos, como recursos de dichas instituciones."

Artículo 12."La información contenida en la solicitud de un título habilitante será considerada confidencial y los funcionarios a cargo de los trámites o procedimientos, están obligados a resguardarla como tal con las responsabilidades legales que esto implica. No será confidencial la información pública contenida en la solicitud."

Artículo 13. "Para el caso de solicitud de ampliación de los servicios a prestarse o modificaciones de cualquier tipo relacionados con los requisitos exigidos para el otorgamiento del título habilitante, el CONATEL requerirá del solicitante la información y documentos de soporte respectivos y podrá aprobar o rechazar la solicitud de acuerdo a lo establecido en las leyes y reglamentos respectivos."

Artículo 14." El plazo de duración de los títulos habilitantes para la prestación de servicios de certificación de información será de diez (10) años, prorrogables por igual período de tiempo, a solicitud escrita del interesado, presentada con tres meses de anticipación al vencimiento del plazo original, siempre y cuando el prestador haya cumplido con los términos y condiciones del título habilitante."

Artículo 15." El prestador de servicios deberá fijar un domicilio principal de operaciones dentro del territorio ecuatoriano, y podrá establecer oficinas de verificación física de datos en los sitios autorizados. Cada sitio donde el prestador de servicios tenga presencia física deberá ser un sitio seguro; contará con control de acceso, resguardo de documentos y protección contra siniestros."

Artículo 16. "El título habilitante se extinguirá por cualquiera de las siguientes causas:

a) Terminación del plazo para el cual fuera emitido.
b) Incumplimiento de las obligaciones por parte de la entidad de certificación acreditada, debidamente fundamentado por el CONATEL de acuerdo a la Ley y Reglamentos.

c) Modificación no reportada al CONATEL o no aceptada por esta Institución en cualquiera de los requisitos exigidos para la obtención del título habilitante.
d) Por resolución fundamentada del CONATEL por causas técnicas o legales debidamente comprobadas incluyendo pero no limitadas a presentación de información falsa o alteraciones para aparentar cumplir los requisitos exigidos.
e) Cese de actividades de la entidad acreditada por cualquier causa.
f) Cese de la relación contractual en el caso de entidades de registro.

El CONATEL tomará las medidas judiciales y extrajudiciales necesarias para garantizar la protección de la información de los usuarios y el ejercicio de los derechos adquiridos por estos.

Artículo 17." El título habilitante para la prestación de servicios de certificación de información especificará por lo menos lo siguiente:

a) Descripción de los servicios autorizados, duración del título habilitante, y demás características técnicas y legales relativas a la operación de los servicios de certificación de información y servicios relacionados autorizados.
b) Las obligaciones y responsabilidades de las entidades de certificación de información de acuerdo a lo establecido en la Ley de Comercio Electrónico y su reglamento, los límites de responsabilidad de acuerdo al tipo de servicios de que se trate, los procedimientos a seguir para solicitar repara-

ciones o indemnizaciones por daños o perjuicios de acuerdo al tipo de servicio a prestar y a las leyes vigentes y, los procedimientos para garantizar la protección de la información de los usuarios y el ejercicio de los derechos por estos adquiridos aún en el caso de cesación del título habilitante.

c) La capacidad de prestar estos servicios a entidades privadas y/o del sector público.

d) Las causales de extinción del título habilitante."

3.5.3 Del trámite para el otorgamiento de títulos habilitantes y sus aplicaciones.

Estos artículos detallan los procedimientos que se deben cumplir incluyendo la otorgación de permisos para prestaciones de servicios de certificación que se encuentran establecidos en el Reglamento General de la Ley Especial de Telecomunicaciones Reformada. Toda esta información es detallada en los artículos 18 al 27.

Artículo 18. "Todo documento técnico parte de una solicitud deberá estar suscrito por un profesional colegiado y cumplir con los requisitos exigidos en la Ley de Ejercicio profesional de la ingeniería, y su Reglamento."

Artículo 19." El procedimiento y los plazos máximos para el otorgamiento de permisos para la prestación de servicios de certificación de información seguirán lo establecido en el Reglamento General a la Ley Especial de Telecomunicaciones Reformada. "

Artículo 20." Es responsabilidad de los funcionarios a cargo de tramitar la solicitud, el verificar por cualquier medio la veracidad y exactitud de los documentos presentados al trámite para los fines del presente reglamento."

Artículo 21. "La solicitud para la obtención de título habilitante para las entidades de certificación de información, deberán estar acompañadas de los siguientes documentos y requisitos:

a) Identificación y generales de ley del solicitante, socios y representantes con los certificados y documentos que demuestren tal condición y el cumplimiento de los requisitos exigidos en las Leyes y Reglamentos para desempeñarse como tales, incluidos pero no limitados a: Nombramientos, contratos de prestación de servicios, certificados de antecedentes penales, certificados profesionales, y certificados legales en general de acuerdo al tipo de servicio a prestar. El CONATEL podrá requerir la presentación de documentos adicionales cuando considere que es necesario para garantizar la idoneidad de la solicitud.
b) Diagrama esquemático y descripción técnica detallada del sistema cuando sea del caso.
c) Descripción detallada de cada servicio propuesto y de los recursos e infraestructura disponibles para su prestación, cumpliendo con los requisitos de sitio seguro establecidos en el Artículo 15 del presente Reglamento. El CONATEL podrá ordenar inspecciones o verificaciones a las instalaciones del solicitante cuando lo considere necesario.

d) Documentos de soporte que confirmen el cumplimiento de los requisitos establecidos en la Ley de Comercio Electrónico y su reglamento de acuerdo a la autorización solicitada.

e) Documentos de soporte que confirmen que se disponen de medidas para evitar la falsificación de certificados, y, en el caso de que el Proveedor de Servicios de Certificación intervenga en la generación de claves criptográficas privadas, se garantice la seguridad y confidencialidad durante el proceso de generación de dichas claves

f) En caso de solicitud de renovación del permiso o de ampliaciones de cualquier tipo, deberá incluirse adicionalmente la certificación de cumplimiento de obligaciones establecidas en el permiso por parte de la Superintendencia de Telecomunicaciones, además de la información de imposición de sanciones por parte de la Superintendencia."

Artículo 22."La solicitud para la obtención de permiso para las entidades de registro de información, relacionadas con una entidad de certificación acreditada, deberá estar acompañada de los siguientes documentos y requisitos:

a) Documentos que certifiquen la relación contractual y legal de la entidad de registro con la entidad de certificación acreditada.

b) Identificación y generales de ley del solicitante, socios y representantes con los certificados y documentos que demuestren tal condición y el cumplimiento de los requisitos exigidos en las Leyes y Reglamentos para desempeñarse como tales, incluidos pero no limitados a: Nombramientos, contratos de pres-

tación de servicios, certificados de antecedentes penales, certificados profesionales, y certificados legales en general de acuerdo al tipo de servicio a prestar. El CONATEL podrá requerir la presentación de documentos adicionales cuando considere que es necesario para garantizar la idoneidad de la solicitud.

c) Descripción de los servicios a prestar por la entidad de registro.
d) En todos los casos, en el contrato de la entidad de registro de información con la entidad de certificación de información acreditada se deberá establecer claramente las responsabilidades legales de cada una de las partes ante los usuarios y autoridades competentes."

Artículo 23. "La solicitud para la obtención del permiso para las entidades de registro de información, relacionadas con una entidad de certificación extranjera registrada en CONATEL, deberán estar acompañadas de los siguientes documentos y requisitos:

a) Documentos que certifiquen la relación contractual y legal de la entidad de registro con la entidad de certificación de información extranjera.
b) Documentos que demuestren la acreditación o reconocimiento legal de los servicios prestados por la entidad de certificación de información extranjera en su País de origen debidamente notarizados y autenticados por la autoridad nacional respectiva para dicho País.
c) Identificación y generales de ley del solicitante, socios y representantes con los certificados y documentos que demuestren tal condición y el cumplimien-

to de los requisitos exigidos en las Leyes y Reglamentos para desempeñarse como tales, incluidos pero no limitados a: Nombramientos, contratos de prestación de servicios, certificados de antecedentes penales, certificados profesionales, y certificados legales en general de acuerdo al tipo de servicio a prestar. El CONATEL podrá requerir la presentación de documentos adicionales cuando considere que es necesario para garantizar la idoneidad de la solicitud.

d) Descripción de los servicios a prestar por la entidad de registro.
e) Descripción de los servicios que se prestarán por parte de la entidad de certificación de información extranjera y que serán representados en el País por la entidad de registro solicitante.

En todos los casos, la entidad de registro de información acreditada será la responsable legal por los servicios prestados o representados por ella directamente o a través de ella, ante los usuarios y autoridades competentes del País.

La entidad de registro acreditada tiene la obligación legal de informar al órgano de regulación y al órgano de control cualquier cambio en las condiciones contractuales, técnicas o de cualquier tipo que existan en su relación con la entidad de certificación de información extranjera. El CONATEL determinará los efectos legales de estos cambios sobre el permiso otorgado y actuará de conformidad a lo establecido en las Leyes y Reglamentos respectivos.”

Artículo 24."Los servicios de certificación de información prestados por entidades de registro de información acreditadas, se considerarán servicios de certificación de información acreditados. "

Artículo 25."Los solicitantes o permisionarios podrán, en sus relaciones con el CONATEL y la Secretaría Nacional de Telecomunicaciones, acogerse a lo previsto en el Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva."

Artículo 26. "Lo establecido en el artículo anterior no limita el derecho del solicitante a pedir la ampliación, modificación, o aclaración de los actos administrativos emitidos por el Consejo Nacional de Telecomunicaciones o la Secretaría Nacional de Telecomunicaciones. Las solicitudes de ampliación, modificación o aclaración de los actos administrativos expedidos por el CONATEL o la Secretaría Nacional de Telecomunicaciones se resolverán en un término de 15 días laborables. En el caso que no exista pronunciamiento expreso dentro del plazo antes señalado, se entenderá por el silencio administrativo, que la solicitud ha sido resuelta en sentido favorable al peticionario. Los funcionarios responsables de emitir pronunciamiento y que no lo hicieran, serán responsables legal y administrativamente por las consecuencias de sus actos."

Artículo 27. "La modificación de las características de operación de los servicios otorgados o la variación en la modalidad de los mismos, en tanto no se altere el objeto del permiso, requerirá de notificación escrita a la Secretaría Nacional de Telecomunicaciones y de su aprobación. Caso contrario, las modificaciones propuestas

deberán ser sometidas a conocimiento y resolución del Consejo Nacional de Telecomunicaciones."

3.5.4 De las condiciones del título habilitante, normas de operación y limitaciones

En estos artículos se detalla la información de los plazos para poder realizar el proceso por el cual fue requerido, siendo que exista vencimiento del plazo la Superintendencia de Telecomunicaciones informa a la Secretaria Nacional de Telecomunicaciones de dicho permiso incumplido. Esta información se detalla de los artículos 28 al 31.

Artículo 28. "Una vez otorgado el permiso, el permisionario dispondrá del plazo de seis (6) meses para iniciar la operación. Vencido dicho plazo la Superintendencia de Telecomunicaciones informará a la Secretaría Nacional de Telecomunicaciones si el titular del permiso ha incumplido con esta disposición, en cuyo caso se considerará incumplimiento de obligaciones por parte de la entidad y será causa de extinción del permiso.

El permisionario podrá pedir, por una sola vez, la ampliación del plazo para iniciar operaciones mediante solicitud motivada. La ampliación, de concederse, no podrá exceder de 90 días calendario. La Secretaria tendrá el plazo perentorio de 15 días para responder dicha solicitud. Ante el silencio administrativo se entenderá concedida la prórroga.

La Secretaría Nacional de Telecomunicaciones remitirá a la Superintendencia de Telecomunicaciones, copia de los permisos y prórrogas otorgadas, así como de las revocatorias o modificaciones, a fin de que la Superintendencia de Telecomunicaciones pueda verificar en forma inmediata el cumplimiento de la presente disposición.

Artículo 29." El prestador de servicios de certificación de información no podrá ceder o transferir total ni parcialmente el permiso, ni los derechos o deberes derivados del mismo.

Artículo 30." El formato de los contratos que las entidades de certificación de información o las entidades de registro de información suscriban con los consumidores o usuarios deberá ser aprobado por el CONATEL y no podrán modificarse sin su autorización. "

Artículo 31. "Todos los contratos emitidos en Ecuador estarán en idioma castellano, y se someterán a la jurisdicción y leyes ecuatorianas."

3.5.5 Reconocimiento de certificados de firma electrónica emitidos en el extranjero.

En estos artículos se detalla la validez de los certificados tanto en el extranjero como en Ecuador, información detalla en el artículo 32.

Artículo 32." La revalidación en el País de los certificados de firma electrónica emitidos en el extranjero les otorga la misma validez que a los certificados emitidos por entidades de certificación de información acreditadas en Ecuador.

Los certificados de firma electrónica emitidos en el extranjero y no revalidados en Ecuador, tienen el carácter de no acreditados.

Para revalidar un certificado de firma electrónica emitido en el extranjero, se deberá cumplir con los requisitos de acreditación y las exigencias de la Ley y Reglamentos ecuatorianos."

3.5.6 Servicios de sellado de tiempo

En estos artículos se detallan los requisitos para que los solicitantes puedan prestar el servicio. Información detallada en los artículos 33 al 35.

Artículo 33." Los solicitantes que deseen prestar servicios de sellado de tiempo deberán cumplir con los siguientes requisitos:

a) Anteproyecto técnico para demostrar la factibilidad, seguridad e integridad del servicio a prestar.
b) Diagrama esquemático y descripción técnica detallada del sistema a emplear"

Artículo 34." El servicio de sellado de tiempo para los mensajes de datos debe ser posible de prestar independientemente de su contenido o soporte, y de forma que sea imposible alterar de ninguna forma del documento sellado sin que este cambio sea detectado e invalide el sello. El servicio de sellado de tiempo incluye:

a) Recepción del mensaje de datos a sellar electrónicamente.
b) Anotación electrónica de la fecha, hora, lugar en que se produce el sellado de tiempo. Este proceso debe asegurar que sea imposible sellar un documento

con un tiempo y fecha diferente de la actual. Tomando como tiempo de referencia UTC ("Universal Time Coordinated").

c) Firmar Electrónicamente el documento sellado para garantizar su integridad y autenticidad de acuerdo a la Ley.
d) Servicios de encriptación o aseguramiento de confidencialidad cuando sea solicitado.
e) Opcionalmente, y con la autorización expresa de los signatarios, la entidad de certificación de información podrá prestar un servicio de certificación u otorgar nuevas certificaciones mediante la reposición del original firmado. Para ello la entidad de certificación de información podrá realizar la generación de un respaldo del documento sellado para su consulta posterior y verificación de la información de sellado de tiempo.
f) Otros servicios relacionados que deberán solicitarse al CONATEL y constar en el respectivo permiso."

Artículo 35." Será responsabilidad de las entidades de certificación de información acreditadas que presten servicios de sellado de tiempo las siguientes:

a) Garantizar la integridad de los documentos sellados y sus respaldos.
b) Garantizar mecanismos automáticos de sellado de tiempo sin posibilidad de cambios en los sistemas de verificación de tiempo y en el sistema de sellado de tiempo.
c) Proporcionar un sistema que garantice la disponibilidad permanente del servicio de sellado de tiempo.

d) Sincronizar sus equipos informáticos de Sellos de Tiempo a través de dispositivos del Sistema Global de Posicionamiento (GPS), protocolo NTP o similares, que permitan trasladar el tiempo UTC con un margen de error no superior a un (1) segundo.

En caso de requerirse cambios en los sistemas de verificación de tiempo o en el sistema de sellado de tiempo, deberá solicitarse autorización a la Superintendencia de Telecomunicaciones, institución que a través de mecanismos técnicos seguros será la única que podrá autorizar el acceso y manipulación o cambios de los sistemas. Deberá adicionalmente proporcionarse un sistema seguro de registro de todas las actividades que genere un reporte automático y encriptado de las mismas que solamente sea accesible por el organismo de control para fines de control y auditorias.

3.5.7 De la regulación y control

Estos artículos presentan información sobre los controles necesarios para los prestadores de servicio de certificación. Se puede observar el detalle en los artículos 36 al 37.

Artículo 36. "La operación de servicios de certificación de información está sujeta a las normas de regulación, control y supervisión, atribuidas al Consejo Nacional de Telecomunicaciones, la Secretaría Nacional de Telecomunicaciones y la Superintendencia de Telecomunicaciones, de conformidad con las potestades de dichos organismos establecidas en las Leyes y Reglamentos.

Artículo 37." La Superintendencia de Telecomunicaciones realizará los controles necesarios a los prestadores de servicios de certificación de información tomando como referencia la Recomendación X.509 de la UIT-T, las recomendaciones del Instituto Europeo de Estándares de Telecomunicaciones (ETSI) y del Comité Europeo de Normalización (CEN), con el objeto de garantizar el cumplimiento de la normativa vigente y de los términos y condiciones bajo los cuales se hayan otorgado los títulos habilitantes, y supervisará e inspeccionará, en cualquier momento, las instalaciones de los prestadores de dichos servicios y eventualmente de sus usuarios, a fin de garantizar que no estén violando lo previsto en el presente Reglamento.

Los prestadores de servicios de certificación de información, deberán prestar todas las facilidades para las visitas de inspección a la Superintendencia y proporcionarles la información indispensable para los fines de control, de no hacerlo estarán sujetos a las sanciones de Ley.

3.6 Legislación Comparada

La ley de Comercio Electrónico, Mensajería de Datos y Firmas Electrónicas se basa en la organización mundial de comercio, con el fin de incrementar relaciones económicas y de comercio de forma regulada y normalizada, mediante servicios electrónicos para que las partes involucradas realicen transacciones electrónicas de forma segura.

En países como Argentina, Colombia y Ecuador, la aceptación de servicios de certificación digital incrementa lentamente por factores como, el desconocimiento de

herramientas informáticas, inseguridad informática frente al fraude electrónico y la inseguridad legislativa, es por eso necesario la certificación de la firma electrónica bajo un marco legal que ampare los mecanismos de autenticación, privacidad y protección de datos, y procedimientos decretados por un Organismo Regulador.

Al comparar las legislaciones de diferentes países en Latinoamérica, se encuentran similitudes ya que se han tomado como referencia la Ley Modelo de la CDUDMI/UNCITRAL para las firmas electrónicas.

La Ley de Comercio Electrónico en Colombia exige requisitos muy similares a Ecuador, en cuanto al cumplimiento de las Entidades Certificadoras de solvencia técnica, logística y financiera.

En Colombia está vigente la Ley de Comercio Electrónico y Firmas Digitales, en la que consta de un capítulo que especifica al comercio electrónico en materia de transporte de mercancías y menciona que todos los documentos de transporte pueden ser remplazados por mensajes de datos debidamente certificados. La ciudad de Bogotá establece "El Sistema de Declaración y Pago de Impuestos Distritales a través de Medios Electrónicos" el que ayuda a los ciudadanos a pagar sus impuestos por medio de servicios electrónicos. En Colombia existen dos clases de entidades de certificación:

- Entidad de certificación cerrada: Ofrecen servicios propios sólo para el intercambio de mensajes entre la entidad y el suscriptor sin exigir remuneración por ello.

- Entidad de certificación abierta: Ofrece servicios propios de la entidad de certificación, tales que su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor o recibe remuneración por la prestación de servicios.

Es así como los certificados digitales de la entidad cerrada, deberán indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor. Mientras que la abierta, lo que pretende es masificar el uso de los certificados digitales para las transacciones en la red.

En cuanto al servicios de certificación digital en la república Argentina, la estructura legal es minuciosamente detallada y clara de tal manera que no permite malas interpretaciones, a diferencia de Ecuador, la legislación argentina pone énfasis en especificar a la firma electrónica y la firma digital. La ley vigente en Argentina se llama Ley de Firma Digital, en la que las funciones de los organismos reguladores y de control son muy detalladas. Además, cuenta con una Comisión Asesora para la Infraestructura de Firma Digital para proveer a los usuarios de esta tecnología un nivel apropiado de seguridad y confianza, la entidad certificadora se asegura que todos los elementos involucrados en el desarrollo y mantenimiento de la Infraestructura de Firma Digital de la Administración Pública Nacional (IFDAPN) exhiban un nivel verificado de seguridad acorde con estándares internacionales vigentes.

La Comisión Asesora para la Infraestructura de Firma Digital es encargada de realizar recomendaciones para establecer estándares tecnológicos, metodologías y requerimientos del resguardo físico de la información, así como analiza el sistema de

registro de toda la información relativa a la emisión de certificados digitales y decreta los requisitos mínimos de información que se debe suministrar a los titulares de certificados digitales de los términos de las políticas certificación.

Es importante analizar varios aspectos de las leyes que regulan la misma materia de servicios de certificación digital para cada país, según las necesidades estas fueron creadas para establecer leyes y normas que ayude a controlar un proceso más real y efectivo. En las siguientes figuras se presenta una comparación de los países latinoamericanos Ecuador, Bolivia, Perú, Venezuela y Colombia, en la Figura 10 la Comparación Firmas Digitales entre países latinoamericanos, la Comparación Certificados Digitales entre países latinoamericanos como lo indica la Figura 11 y la Comparación Firmas Digitales entre países latinoamericanos y la Comparación Entidades/ Autoridades de Certificación y Registro entre países latinoamericanos descrita en la Figura 12:

FIRMAS DIGITALES	ECUADOR	BOLIVIA	PERÚ	VENEZUELA	COLOMBIA
Establecer la regulación de las firmas electrónicas desde un principio.	✓	✓	✓	✓	✗
La firma surtirá los mismos efectos legales que la firma manuscrita.	✓	✓	✓	✓	✓
Información para obtener requisitos y características de la firma electrónica	✓	✗	✓	✓	✓
Duración de la firma electrónica indefinida	✓	✗	✗	✗	✗

Continua →

Tiempo de extinción de la firma electrónica	✓	✗	✗	✗	✗
Invalidez de la firma electrónica o digital	✗	✗	✓	✗	✗
Obligaciones del Titular de una Firma Electrónica y/o Digital	✓	✗	✓	✓	✓

Figura 10. Comparación Firmas Digitales entre países latinoamericanos

CERTIFICADOS DIGITALES	ECUADOR	BOLIVIA	PERÚ	VENEZUELA	COLOMBIA
Requisitos para Obtener un Certificado Digital (Especificaciones Adicionales y Procedimiento).	✗	✗	✓	✗	✗
Contenido de un Certificado de Firma Electrónica.	✓	✗	✓	✓	✓
Atribución Jurídica de un Certificado.	✓	✗	✗	✓	✗
Duración del Certificado de una Firma Electrónica	✓	✗	✓	✓	✗
Suspensión, Revocación o Cancelación y Extinción de un Certificado.	✓	✗	✗	✓	✗

Figura 11. Comparación Certificados Digitales entre países latinoamericanos

ENTIDADES/ AUTORIDADES DE CERTIFICACIÓN Y REGISTRO	ECUADOR	BOLIVIA	PERÚ	VENEZUELA	COLOMBIA
Definición, características y requerimientos de las entidades de certificación.	✓	✗	✓	✓	✓

Figura 12. Comparación Entidades/ Autoridades de Certificación y Registro entre países latinoamericanos

CAPÍTULO 4

INFRAESTRUCTURA CERTIFICADORA EN SMARTGRID

Una PKI está basada en cifrado de clave pública, para cumplir en estándar PKIx se encuentra formada por:

- Certificados Digitales (Estándar X509).
- Estructura o modelo jerárquico.- Conformado por las Autoridades de Certificación (AC) y las Autoridades de Registro (AR), las cuales son utilizadas para generar y verificar la validez de los certificados.
- Directorios de certificados.- Repositorios para el almacenamiento de los certificados.
- Sistema de administración de certificados.- Programa que utiliza la AC o la empresa donde se ha instalado la PKI para que realice el ciclo de vida de los certificados digitales: solicitar, renovar, revocar, suspender y anular.

4.1 Modelo de Certificación

La PKI necesita tener un modelo de certificación para que las Instituciones de Educación Superior del Ecuador formen parte a una estructura de certificación donde cumplan con los procedimientos y las políticas establecidas bajo el marco legal ecuatoriano en la PKI. En un modelo de certificación, las Autoridades Certificadoras están basadas en igualdad de jerarquías donde se pueden presentar dos escenarios:

1. Existe un número reducido de ACs.

2. Existe un número elevado de ACs.

Cuando se muestra el primer caso, siendo este un número reducido de ACs, se puede entender que la determinación de la ruta de certificación puede llegar a ser insignificante ya que la estructura es reconocida con facilidad por parte de todas las universidades participantes dentro de la infraestructura de certificación.

Por otra parte cuando el número de las ACs es elevado, se muestra una gran problemática debido a que esto representa inconsistencia en la ruta de certificación, esto representa dificultad para determinar la compatibilidad con las políticas de certificación.

Es importante trabajar con un modelo de confianza ya que permite tener un marco de referencia para poder administrar las relaciones de confianza, por este motivo se debe determinar qué modelo es el más conveniente a ser utilizado según las necesidades. Existen los siguientes modelos de certificación:

4.1.1 Modelo Jerárquico

La base principal del modelo jerárquico es establecer como ancla de confianza a la Autoridad Certificadora raíz, de esta manera se establece como la mayor parte de confianza de una PKI y su sistema.

Este modelo trabaja bajo relaciones unidireccionales con sus subordinados, por lo tanto no es indispensable comprobar el camino que se forma desde la Autoridad Certificadora que realiza la emisión de un certificado hasta la Autoridad Certificadora de confianza que emitió el certificado, ya que siempre tendrán como punto principal

el certificado de la Autoridad Certificadora raíz, por este motivo es importante que el certificado de la AC raíz sea distribuido a todos los usuarios implicados.

Este modelo tiene como punto de criticidad la Autoridad Certificadora raíz, si su clave privada es comprometida los usuarios se verán totalmente afectados, y se tomara medidas para revocar el certificado y realizar la redistribución de uno nuevo.

A pesar de esto en su gran mayoría, es restringido la emisión de certificados para las autoridades subordinadas, por tal motivo estos casos se presentan muy rara vez, demostrando que este modelo es bastante aceptado para trabajar en las implementaciones de un ambiente PKI dentro de cualquier organización, permite con facilidad determinar un punto de confianza y obtener restricciones implicadas a la subordinación, será inadecuado en organizaciones con ambientes grandes y compuestos debido a que exige establecer su confianza en totalidad por cada participante. En la Figura 13 se representa el Modelo Jerárquico:

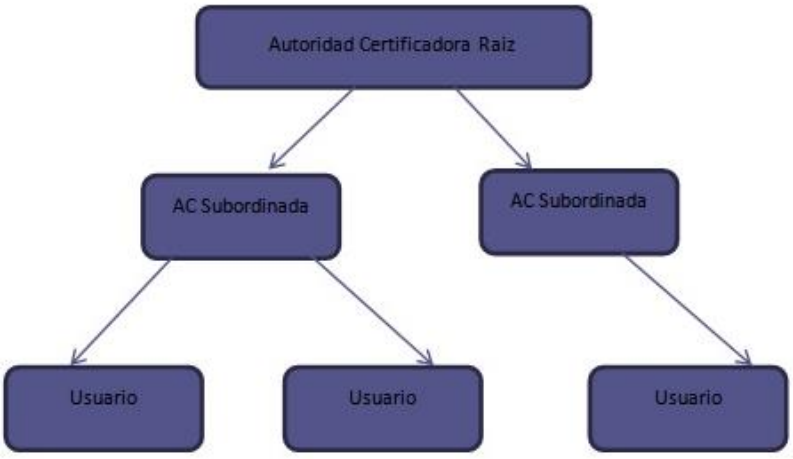

Figura 13. Modelo Jerárquico

4.1.2 Modelo Malla

El modelo en malla es una de las alternativas más accesibles para la PKI jerárquica, en este modelo los servicios PKI son proporcionados bajo varias ACs por lo que la relación no será jerárquica y siempre serán de igual a igual.

En este modelo los usuarios tendrán la suficiente confianza en una Autoridad Certificadora única, pero a pesar de esto se debe tomar en cuenta que los usuarios no tendrán la misma Autoridad Certificadora, ya que los usuarios tendrán la suficiente confianza en la AC que realizó la emisión del certificado.

Existen relaciones bidireccionales y una de las maneras de comprobar dicho evento es emitir certificados entre ellas por parte de las ACs, para que una Autoridad Certificadora pueda ser agregada a la malla debe realizar el intercambio de certificados con otra AC que ya sea perteneciente de la malla.

Para realizar el camino de la construcción de este modelo en malla se somete a varias elecciones que en muchas ocasiones puede tener como respuesta caminos válidos y otras no, como se representa en la Figura 14.

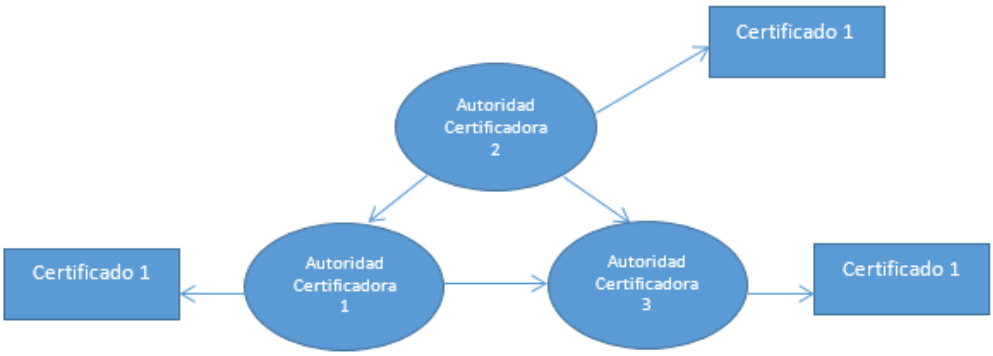

Figura 14. Modelo Malla

4.1.3 Modelo Mixto

El modelo mixto es utilizado para obtener la unión de dos o más PKI, este proceso se realiza cuando la Autoridad Certificadora raíz son certificadas entre si y por medio de esto obtienen entre ellas una relación de confianza, como se representa en la Figura 15.

La explicación más sencilla, es observar que una PKI A como una B son conectadas, cuando esto sucede la Autoridad Certificadora raíz de la PKI A y una Autoridad Certificadora cualquiera de la PKI B, procederán a certificarse mutuamente, se debe tomar en cuenta que dentro de un modelo en malla se debe seleccionar una AC cualquiera para que esta permita servir como vínculo con otra PKI.

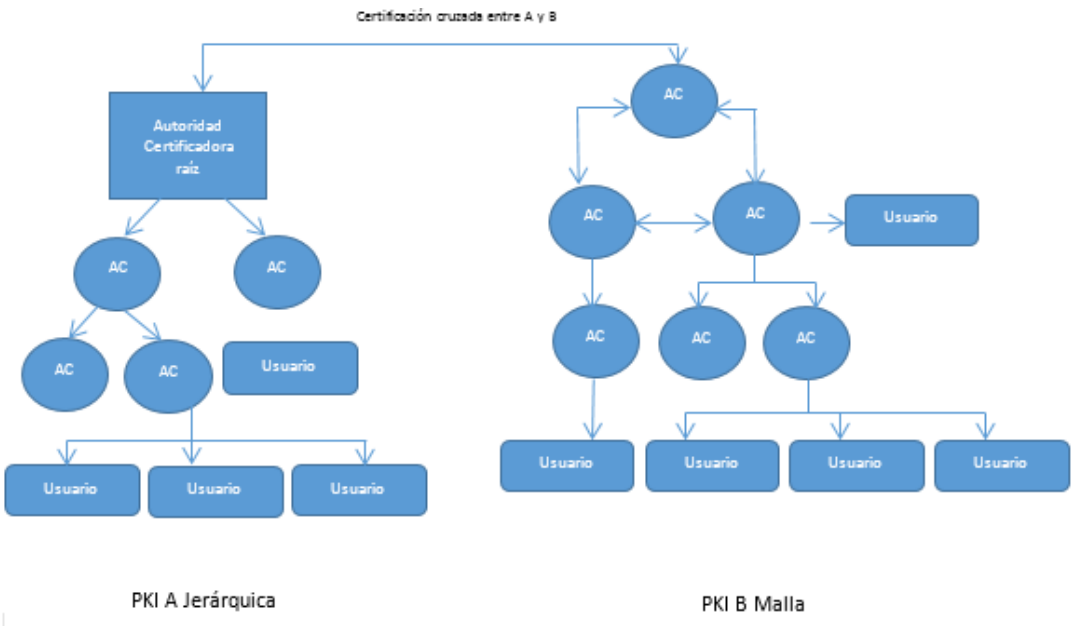

Figura 15. Modelo Mixto

4.1.4 Modelo en Puente

El modelo en puente permite conectar varias PKI entre sí, siendo esta apartada de su propia estructura por lo que le hace independiente, este proceso será permitido mientras es introducida una Autoridad Certificadora puente, la que permite que varias PKI establezcan relaciones de confianza.

Una de las diferencias con el modelo de malla es que la Autoridad Certificadora puente no permite la emisión de certificados a los usuarios finales, solamente puede tener una relación con una AC por cada PKI, esta estructura tiene un crecimiento lineal mientras que en el modelo de malla crece de manera exponencial, como se representa en la Figura 16.

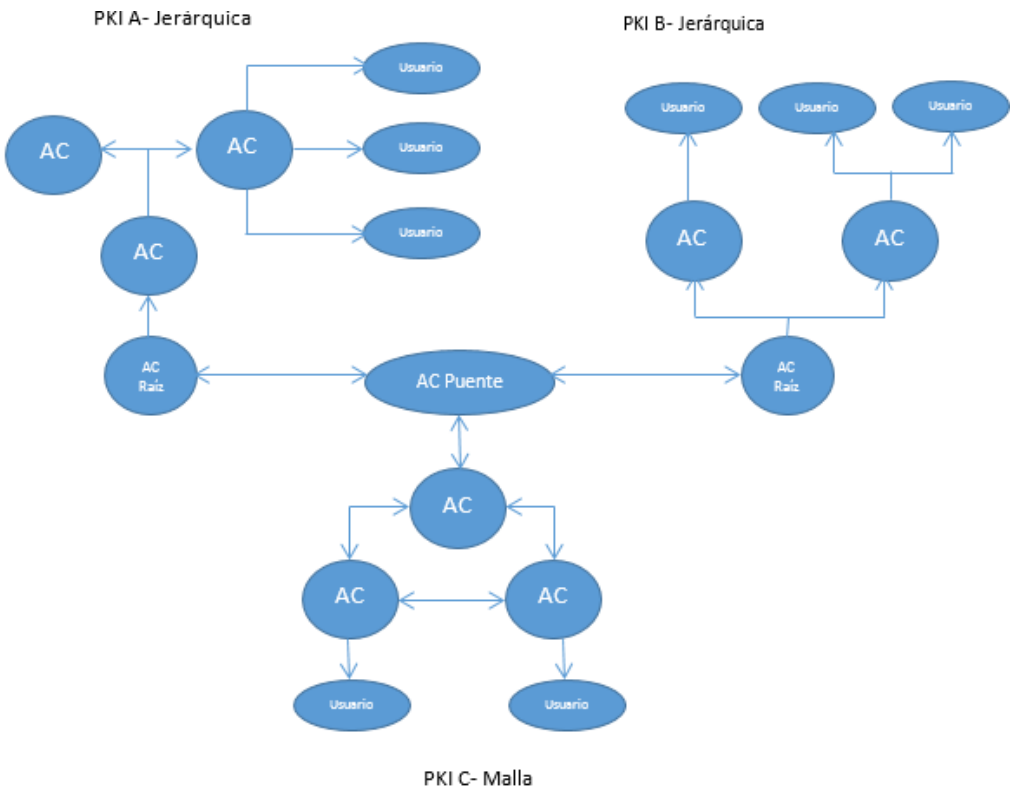

Figura 16. Modelo Puente

4.1.5 Modelo de la PKI para el Sistema Nacional de Educación Superior del Ecuador

El Sistema Nacional de Educación Superior del Ecuador al tener 74 Instituciones a nivel nacional requiere un modelo de certificación que permita establecer relaciones de confianza entre los usuarios de la PKI, evitando listas extensas de AC Subordinadas difíciles de administrar.

El modelo puente por sus características es apropiado para el diseño de una PKI basada en Smart Grid para el Sistema Nacional de Educación Superior, estableciendo al SENESCYT como Autoridad Certificadora Puente, la misma que no emite certificados a las entidades finales(personas, dispositivos o aplicaciones), sin embargo establece relaciones de confianza entre las siguientes autoridades certificadoras raíz:

- AC Raíz Sierra Norte
- AC Raíz Sierra Sur
- AC Raíz Costa
- AC Raíz Oriente-Galápagos

Las ACs Raíz descritas anteriormente, son el ancla principal de confianza para todas las Universidades correspondientes a cada región, además son las Autoridades de Certificación de mayor confianza con las ACs Subordinadas que son las Instituciones de Educación Superior. Las Autoridades Certificadoras Raíz son las únicas que permiten expedir certificados a sus AC Subordinadas. Cada AC Subordinada debe cumplir funciones que sean semejantes a las de una Autoridad Certificadora Raíz.

Para complementar el modelo puente, en cada región del Sistema de Educación Superior, se implementa el modelo jerárquico de 2 niveles. Este modelo es escalable y permite asignar una Autoridad Certificadora Subordinada cuando se integre una nueva Institución Superior al modelo y permite el crecimiento de la estructura PKI, sin alterar su funcionalidad al trabajar con sistemas distribuidos.

Este modelo realiza procesos de verificación que son realizados de forma unidireccional, comprobando todas las relaciones de confianza de una PKI siempre tomando como punto de inicio la AC Raíz SENESCYT, siendo esta la autoridad de confianza. En la Figura 17 se representa el Modelo de Certificación Puente para la PKI del Sistema Nacional de Educación Superior del Ecuador.

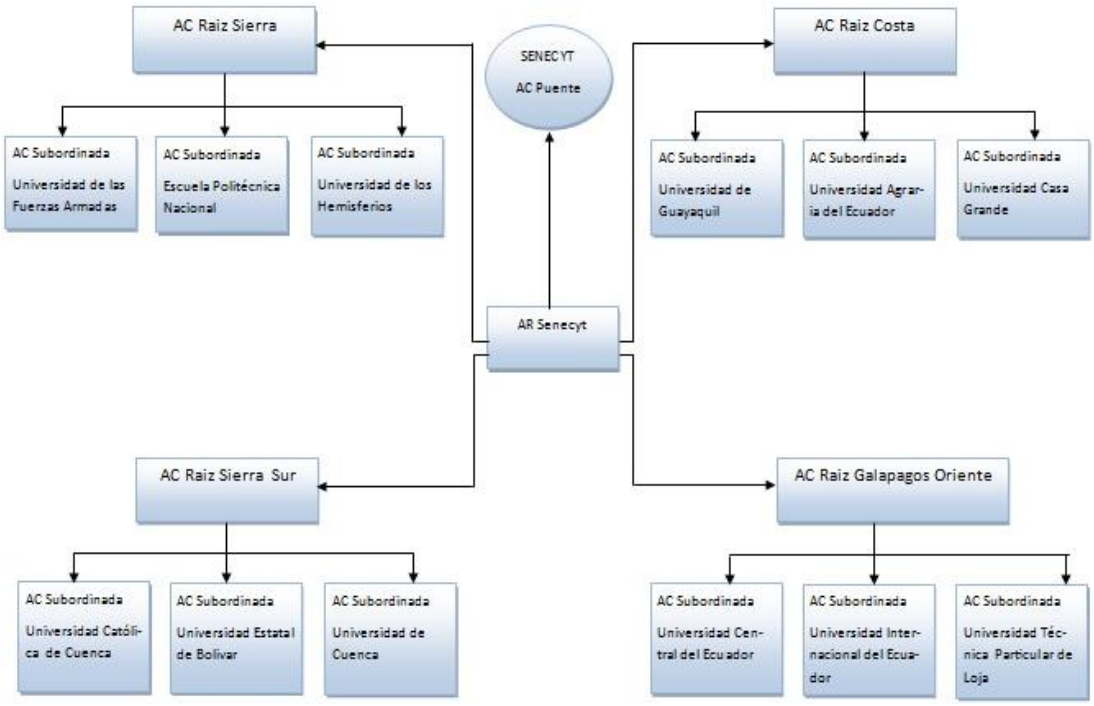

Figura 17. Modelo de Certificación

4.2 Componentes PKI

Los componentes que conforman una PKI son diseñados para desempeñar funcionalidades que permitan cumplir con los requerimientos de seguridad como autenticidad, confidencialidad, integridad y no repudio.

El modelo puente utilizado en este proyecto, define al SENESCYT como Autoridad Certificadora puente. En el modelo jerárquico utilizado en las regiones se define los siguientes niveles.

4.2.1 TTP Nivel 1

Las Autoridades de Certificación raíz reciben peticiones de AC subordinadas, una vez realizado el proceso de validación y certificación de datos, la AC raíz envía a las AC subordinadas los certificados, como lo indica la Figura 18.

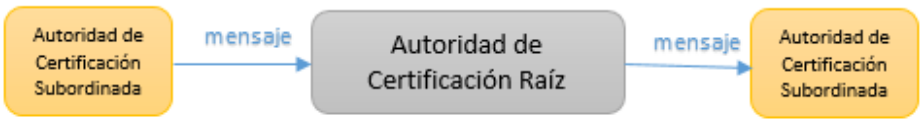

Figura 18. TTP Nivel 1

En el nivel 1 de la TTP, la autoridad de certificación raíz debe siempre estar disponible para emitir certificados a las AC subordinadas. Cada AC cuenta son su propia red de datos e infraestructura tecnológica. Las autoridades certificadoras raíz son:

- AC Raíz Sierra Norte
- AC Raíz Sierra Sur

- AC Raíz Costa
- AC Raíz Oriente-Galápagos

Las Autoridades de Certificación Subordinadas que participan en este nivel son todas las Instituciones de Educación.

4.2.2 TTP Nivel 2

En la TTP Nivel 2, los usuarios finales son los estudiantes, docentes y administrativos, así como pueden ser equipos pertenecientes a la institución. Las ACs Subordinadas tienen las mismas políticas y procedimientos que la AC raíz, como se representa en la Figura 19.

Figura 19. TTP Nivel 2

Los certificados que validan a los usuarios, son emitidos por la AC subordinada, es decir la institución superior a la que pertenecen, sin embargo en la ruta de certificación también está involucrada la AC raíz, correspondiente a la AC Región y la AC Puente SENESCYT. La Autoridad de Registro SENESCYT (AR) realiza el proceso de registro de las entidades usuarias por encargo de la AC y valida los atributos del usuario que solicita el certificado digital. En la Figura 20 se muestra la Cadena de Certificación final:

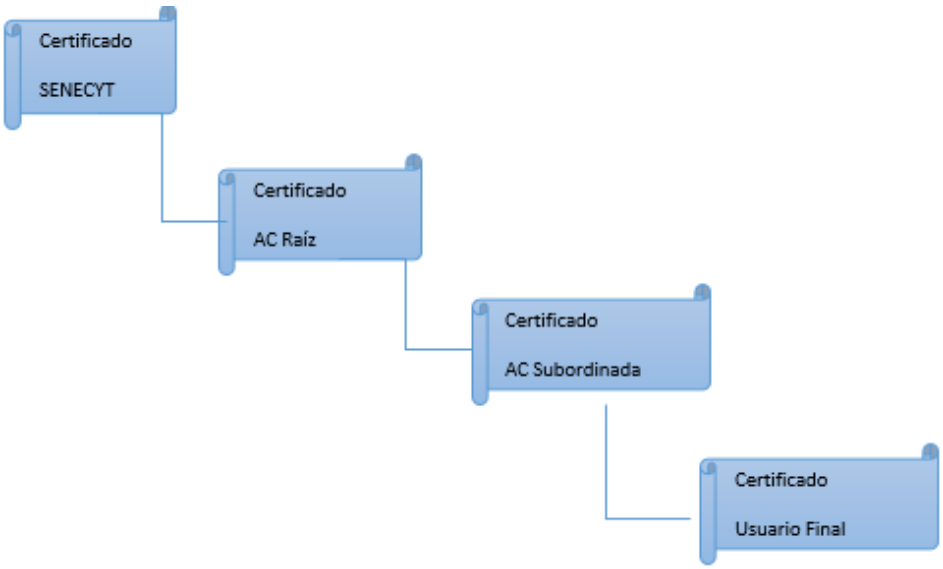

Figura 20. Cadena de Certificación

La Autoridad Certificadora Puente SENESCYT, dispone de una Autoridad de Registro SENESCYT para corroborar los datos de las solicitudes realizadas por los usuarios finales, así como para validar y emitir al usuario las certificaciones emitidas por las AC Subordinadas.

4.2.3 La Autoridad Certificadora

La Autoridad Certificadora Subordinada correspondiente a cada Institución de Educación Superior, emite los certificados siempre y cuando sean confirmados por la Autoridad de Registro AR SENESCYT. Las ACs Raíz Regionales pueden emitir los certificados de AC Subordinadas a las AR.

Las ACs Raíz Regionales emiten certificados a las Instituciones de Educación Superior, pero no emiten certificados para usuarios finales, en cambio las Instituciones de Educación Superior, quienes son ACs Subordinadas pueden realizar la emisión de certificados de los usuarios finales.

4.2.4 La Autoridad de Registro

Las AC Puente SENESCYT trabaja conjuntamente con la Autoridad de Registro SENESCYT para controlar la identidad los solicitantes de certificados. Una AR autoriza la solicitud de un certificado y entrega al usuario solicitante el certificado emitido por la AC Subordinada, previamente verificando los contenidos de las solicitudes en lugar de la AC. Existen dos modelos para que una AR verifique el contenido de los certificados:

1. Primer modelo: La AR recoge la información y la verifica antes de ser presentada a la AC.
2. Segundo modelo: La AC recibe la solicitud del certificado que envía a la AR, la cual trabaja bajo la revisión del contenido y verifica si la información es la adecuada y correcta y da respuesta a la AC.

La AR Senescyt utiliza el primer modelo, es decir, recoge la información de la solicitud y verifica los datos de la solicitud para poder entregar a la AC Subordinada y esta a su vez genere el certificado solicitado.

4.2.5 Repositorio

Los repositorios son creados para permitir máxima disponibilidad y rendimiento ya que los datos con los que se trabajan establecen la integridad, los repositorios deben limitar a los usuarios que actualicen la información ya que si esto no sucede puede que existan atacantes donde cambien los certificados con información errónea y se produzca un proceso de negaciones de servicio.

4.2.6 Usuarios

Los usuarios son todas las personas, dispositivos o aplicaciones, a quienes serán emitidas certificados o a su vez van a utilizar los certificados de los demás, aquí se demuestra las partes de confianza. De esta manera es de esperar que los usuarios a los que se hayan expedido certificados mantengan la clave privada asociada dentro de la confidencial.

4.3 Roles PKI

El proceso general de certificación se realiza de la siguiente manera:

Los usuarios finales de las Instituciones de Educación Superior del Ecuador envían una solicitud para la aprobación de un certificado a la Autoridad de Registro Senescyt para verificar los datos del solicitante y aprobar o rechazar la petición. Si la AR aprueba los datos de la solicitud del certificado, envía la solicitud a la AC Subordinada correspondiente para que la firme. De esta manera, la AC Subordinada procede a descargar los datos de la solicitud desde la página web y generar el certificado.

El certificado emitido es reconocido por la AC Raíz Regional y la AC Puente SENESCYT, ya que se encuentran en una relación de confianza. La revocación de certificados tiene un proceso parecido al de la generación del mismo y la AR Senescyt aprueba la solicitud de revocación para que la AC Subordinada envíe certificados al repositorio. Para asegurar la autentificación, autorización y administración

de la PKI es necesario definir los roles de los participantes de la PKI como lo indica la figura 21.

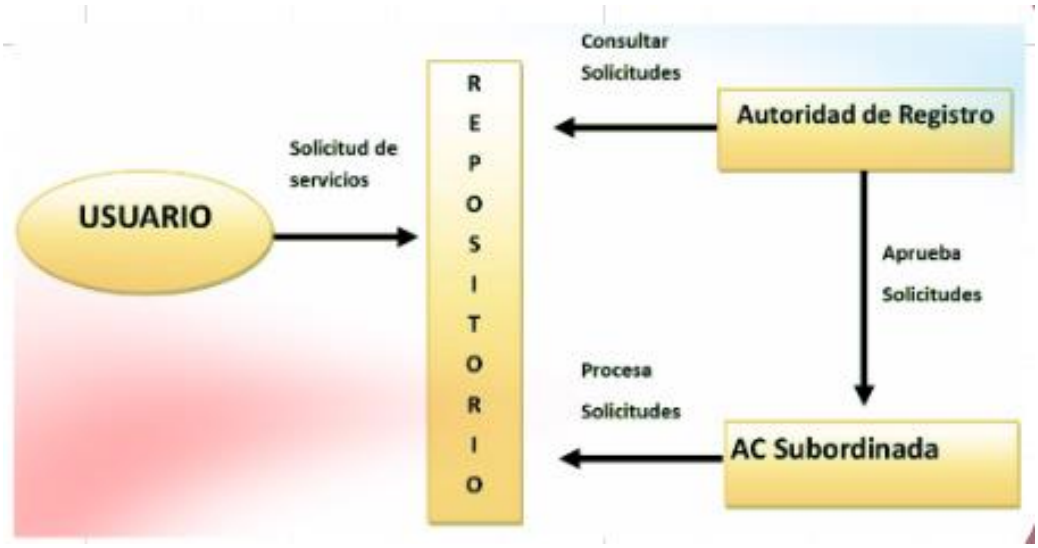

Figura 21. Roles PKI

4.3.1 AC Puente Senescyt

La Autoridad de Certificación Puente es el componente esencial de una PKI y realiza cuatro funciones básicas para las Autoridades de Certificación Regional:

1. Emisión de certificados.
2. Crear y firmar certificados.
3. Mantener información del estado de los certificados.
4. Emitir CRLs.

La AC Puente Senescyt autofirma su propio certificado.

4.3.2 Autoridad de Registro

La autoridad de registro se encarga de procesar la solicitud de la certificación y se lo entrega a la autoridad de certificación subordinada. La AR Senescyt le ayuda a la AC Subordinada corroborando la validez de la información de las solicitudes. Las ACs Subordinadas confían en la información proporcionada por la AR acreditada por medio de la firma digital. Una AR puede cumplir con su objetivo de los siguientes modelos:

- La AR recoge y verifica la información antes de presentar a la AC Subordinada la solicitud para el certificado.
- La AR revisa el contenido las solicitudes enviadas por la AC Subordinada o los usuarios finales y determina si la información es correcta. La AR Senescyt aprueba o rechaza las peticiónes.

4.3.3 AC Raíz Regional

La Autoridad de Certificación Regional es el componente de la PKI que realiza cuatro funciones básicas para las Autoridades de Certificación Subordinadas:

1. Emisión de certificados.
2. Crear y firmar certificados.
3. Mantener información del estado de los certificados.
4. Emitir CRLs.

4.3.4 AC Subordinada

La AC Subordinada tiene la obligación de publicar los certificados y CRLs para que los usuarios tengan acceso a la información necesaria e implementen servicios de seguridad, así también debe conocer el estado de los certificados expirados o revocados que emitió.

La Autoridad Certificadora controla la calidad del certificado emitido. La AC puede observar la revocación de los certificados de las siguientes formas:

- Eliminados desde el directorio o base de datos en la que se encuentra. Como resultado la búsqueda no debe ser positiva, por lo que siempre se demostrará que ya no se encuentran vigentes y cualquier tipo de búsqueda será fallida, se deducirá que estos fueron revocados.
- Sistema de lista de revocación (CRL) debe encontrarse fuera del directorio. Esta es una lista de certificados que ya no son válidos, sin importar la razón.

La revocación de un certificado se realiza si se desea eliminar la relación que origina un certificado entre una universidad y la clave pública, este proceso puede ser realizado antes que el certificado expire. En este caso se publica una lista de certificados revocados a la cual se denomina CRLs (Certificate Revocation List).

La CRL consta de una firma digital que suministra mecanismos de autenticidad e integridad, el emisor del certificado y de la CRL es la misma autoridad. La CRL mediante el estándar X.509 utiliza dos tipos de extensiones:

1. Aplicables sólo a una entrada de la lista.- Cuando una aplicación procesando una CRL no reconoce una extensión marcada como crítica que sólo aplica a un campo de la lista considerará el certificado como revocado
2. Aplicables globalmente a la CRL.- Cuando una aplicación procesando una CRL no reconoce una extensión marcada como crítica que aplica globalmente a la CRL considerará los certificados identificados como revocados, pero además considerará que la lista no es completa y actuará adicionalmente como indique la política.

Cuando una extensión es no crítica puede ser ignorada por la aplicación.

4.3.5 Usuario Final

El usuario final quien puede ser un alumno, profesor o administrador, es quien envía una solicitud de servicio como Solicitar Certificado, Consultar Solicitudes, Descargar Certificado, Renovar Certificado, Suspensión o Revocatoria o Reactivar. Hay dos tipos de usuarios finales soportados por una PKI.

1. Poseedores de Certificados: Obtienen certificados de la infraestructura y usan sus claves privadas para implementar servicios de seguridad, como generar firmas digitales, descifrar datos usando sus claves privadas y establecer claves simétricas a través de protocolos. Para cumplir estos objetivos el poseedor de un certificado realiza las siguientes acciones:
    - Identificar la AC Subordinada que emite los certificados.
    - Solicitar el certificado a través de una AR.

- Incluir el certificado en las transacciones que lo requieran.

2. Partes Confiantes: Usan la clave pública de un certificado para verificar la firma o cifrar datos y usan la PKI para implementar servicios de seguridad utilizando la clave pública en el certificado. Pueden verificar firmas digitales, cifrar datos (claves simétricas) y usar la clave pública para establecer claves simétricas a través de protocolos de acuerdo de claves, para lo cual deben realizar las siguientes acciones:
    - Identificar una AC como su punto inicial de confianza.
    - Verificar firmas de certificados y CRLs.
    - Obtener certificados y CRLs del repositorio.
    - Construir y validar caminos de certificación.

Para el Sistema Nacional de Educación, los usuarios finales de las Instituciones de Educación Superior participan en ambos papeles tanto como poseedores de certificados, así como parte confiante. Las ACs y la AR también son usuarios porque generan, verifican firmas y transmiten claves entre sí.

Para la revocación de certificados los usuarios deben realizar una petición a la AR, de esta manera la AR Senescyt valida la información del solicitante y envía la solicitud a la AC Subordinada, la misma que se encarga de la actualización de la lista de certificados revocados conocida como CRL (Certificate Revocation List).

CAPÍTULO 5

MODELO DE GESTIÓN PKI

Este capítulo describe las políticas y procedimientos implementados en el modelo PKI basado en Smart Grid para el Sistema Nacional de Educación Superior, las cuales fueron establecidas siguiendo el estándar X.509.

La confiabilidad de los documentos electrónicos está relacionada con las prácticas, procedimientos técnicos y normas legales consideradas por los componentes de la PKI SmartGrid del Sistema Nacional de Educación Superior, como resultado del análisis del marco legal aplicado en una PKI basado en un ambiente Smart Grid se establece el ciclo de vida del certificado, representado en la Figura 21.

Figura 22. Ciclo de Vida del Certificado

5.1 Políticas de Certificación

Una política de certificación reúne las reglas que muestran cuando un certificado es aplicable en un Smart Grid, ya que describe los roles, responsabilidades y relaciones entre el usuario final y la Autoridad de Certificación durante el ciclo de vida de un certificado digital, en ellas se definen las reglas de solicitud, descarga, gestión y uso de los certificados digitales.

El modelo contemplado para la PKI es un modelo puente, donde la Autoridad Certificadora puente es el SENESCYT y cada región será constituida por un Modelo Jerárquico de 2 niveles. La AC Puente-SENESCYT junto con la Autoridad de Registro AR-SENESCYT

Las políticas descritas a continuación, están clasificadas de acuerdo al ciclo de vida de un certificado:

5.1.1 Solicitar Certificado

- Cada certificado emitido por una AC debe estar firmado por una AC de mayor grado en el esquema jerárquico de autoridades certificadoras formándose así una cadena de certificados, en los que unas AC se avalan a otras hasta llegar a la AC Puente Senescyt, que se avala a sí misma
- La Autoridad de Certificación Puente, SENESCYT, emite certificados a Autoridades de Certificación Raíz cuyo periodo de validez es de 5 años.
- Las Autoridades de Certificación Raíz de cada región, es decir: Sierra Norte, Sierra Sur, Costa, Galápagos-Amazonía, emiten certificados a las Auto-

ridades de Certificación Subordinadas correspondiente a las Instituciones de Educación Superiores de la región y su periodo de validez de es 3 años.

- La Autoridad Certificadora Subordinada de cada Institución es la encargada de emitir certificados a los usuarios finales cuyo periodo de validez para estudiantes, administrativo o docente es de dos años.
- Los certificados emitidos a una AC Subordinada de la Institución, tendrán un periodo de validez de 2 años para las instituciones de educación superior correspondientes.
- La Autoridad de Registro Senescyt se encarga de recibir, verificar o rechazar solicitudes de los usuarios finales para la emisión o extinción del certificado y las solicitudes de suspensión, revocación y reactivación de certificados digitales.
- La AC-Subordinada descarga la solicitud aprobada por la AR-Senescyt en un archivo de extensión .txt.
- La AC-Subordinada es la encargada de subir el al portal web para la descarga.
- La AR Senescyt emite la clave de exportación del certificado y el PIN de descarga al usuario mediante correo electrónico.
- El Certificado generado por la AC Subordinada utiliza el algoritmo de Hash sha1 con una longitud de clave pública RSA de 1024 bits.
- El certificado será entregado al usuario en formato .pfx con nombre de archivo correspondiente al número de cédula.

- Un certificado lo puede solicitar un usuario que puede ser estudiante, administrativo o docente de la institución.
- El usuario debe solicitar el certificado mediante la página web llenando los formularios correspondientes.
- El administrador de la AR Senescyt debe aprobar la solicitud del usuario para que el administrador AC Subordinado de la institución proceda con la creación del certificado.
- El usuario para solicitar un certificado se debe ingresar a la página web "https://www.acnagrid.com\certificacion".
- El administrador AC tiene un plazo de 24 horas, a partir de la elaboración de la solicitud de emisión. Para entregar a la AR Senescyt el archivo de petición de emisión del "Certificado AC Subordinado"
- La AR Senescyt genera de forma aleatoria el PIN de descarga y la clave de Exportación, dichos códigos están guardados en la base de datos con criptografía md5.

5.1.2 Suspensión

- La suspensión representa la pérdida de validez temporal de un certificado, y es reversible.
- La AR-Senescyt tiene un plazo de siete días para reactivar o cancelar el certificado que se encuentra suspendido, pasado dicho plazo la revocación definitiva del certificado será automática.
- La suspensión se realiza mediante una solicitud a través de la página web.

- La suspensión de un certificado podrá ser solicitada por la AC Subordinado de la institución a la que corresponde el usuario.
- La solicitud de la suspensión podrá efectuarse antes de la fecha de caducidad del certificado.
- La solicitud de la suspensión podrá efectuarse por los siguientes motivos:
    - Disposición del Consejo Nacional de Telecomunicaciones.
    - Falsedad de datos.
    - Incumplimiento de contrato.

5.1.3 Reactivar

- Un certificado puede ser reactivado si su estado es de "SUSPENSIÓN" Y representa activación del certificado.
- La AC- Subordinada tiene un plazo de siete días para reactivar el certificado que se encuentra suspendido, caso contrario pasado dicho plazo la revocación definitiva del certificado será automática.
- La reactivación se realiza través de la página web, en la pestaña "Reactivar" por la AC- Subordinada.
- La solicitud de la suspensión será aprobada por la AR-Senescyt.

5.1.4 Extinción

- La extinción se realiza mediante una solicitud a través de la página web, en la pestaña Extinción.

- La extinción de un certificado representa la pérdida de validez del mismo, y es irreversible.
- La extinción de un certificado podrá ser solicitada por la el titular del certificado.
- La solicitud de la extinción podrá efectuarse antes de la fecha de caducidad del certificado.
- La solicitud de extinción podrá efectuarse por los siguientes motivos:
    - Fallecimiento o incapacidad del Titular.
    - Disolución persona jurídica, titular de la firma.
    - Causa Judicialmente declarada
    - Caducidad de la firma electrónica
    - Secuestro

5.1.5 Renovar

- La AR Senescyt debe verificar la identidad del usuario y el período de validez del certificad antes de renovar un "Certificado AC-Subordinado".
- Para renovar un certificado el estado del mismo debe ser "CADUCADO"
- La renovación de un certificado se lo puede realizar cuando expire el plazo de validez y su estado debe ser "CADUCADO", se lo realiza con una solicitud de renovación a través de la página web.

Las siguientes políticas, se refieren a la autenticación, por parte de la AR Senescyt, a los elementos descritos a continuación conforme al estándar X.509 v3.

5.1.6 Revocatoria

- La revocatoria se realiza mediante una solicitud a través de la página web.
- La cancelación o revocación de un certificado representa la pérdida de validez del mismo, y es irreversible.
- La revocación de un certificado podrá ser solicitada por la AC Subordinado de la institución a la que corresponde el usuario.
- La solicitud de la revocatoria podrá efectuarse antes de la fecha de caducidad del certificado.
- La solicitud de la revocatoria podrá efectuarse por los siguientes motivos:
    - Disposición del Consejo Nacional de Telecomunicaciones.
    - Falsedad de datos.
    - Incumplimiento de contrato.
    - Secuestro Titular
- Se considera secuestro del titular una vez que los familiares presenten la denuncia.

5.1.7 Tipos de nombres

- Nombre: Este elemento contendrá el nombre y el apellido del solicitante.
- E-Mail: Este elemento contendrá el correo electrónico del solicitante.
- Cédula: Identificador del Registro único del solicitante.
- Región: Este elemento permite seleccionar la región a la que pertenece el solicitante.

- Institución: Este elemento permite seleccionar la institución a la que pertenece el solicitante.
- Usuario: Este elemento permite seleccionar el tipo de usuario como: estudiante, administrativo o docente.
- Contraseña: Este elemento permite ingresar la clave del usuario que servirá para verificar su identidad ante una petición de un certificado.
- Confirmar Contraseña: Este campo valida y confirma la clave ingresada.

5.1.8 Autenticación de la identidad

- La AR Senescyt es la encargada de autenticar el certificado y de la verificación del DN, a través de la documentación suministrada por el suscriptor.
- El titular del certificado, puede solicitar la revocatoria, la suspensión o el levantamiento de la misma mediante la página web.
- En caso de pérdida de claves, el usuario debe realizar una solicitud de cambio de clave personalmente en la institución a la que pertenece.

5.1.9 Confidencialidad

La AC Puente Senescyt considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito del titular del Certificado

La siguiente información será considerada confidencial:

- Claves de usuario del certificado emitido por la AC-Subordinada.
- PIN de descarga del certificado.
- Clave de exportación del certificado.

La siguiente información será considerada no confidencial:

- Los datos existente en el certificado x.509 v3 emitido por la AC- Subordinada.
- La lista de certificados revocados y suspendidos.
- Cualquier información publicada en el portal web.

5.1.10 Registro de documentos

- La AR Senescyt será la responsable de resguardar la documentación necesaria para la gestión del ciclo de vida de los certificados emitidos por la AC- Subordinada por un periodo de 5 años.

5.2 Política de Seguridad Lógica de la PKI

La seguridad lógica proporciona un esquema para evitar la pérdida de registros y salvaguardar la integridad de la información almacenada en la AC-Puente Senescyt. La aplicación de estas políticas permite reducir el potencial de la AC-Puente Senescyt para perder información generada por el software base y los programas de aplicación.

5.2.1 Backup externo

La AR Senescyt deberá mantener un almacén externo seguro para la custodia y respaldo de la base de datos y toda la configuración de la AC-Puente Senescyt, para lo cual se describen las siguientes políticas:

- Periodicidad de las copias de respaldo: La realización de copias de seguridad de forma periódica se realizara mensualmente.
- Almacenamiento de las copias de respaldo: La copia de respaldo se almacena en las instalaciones de la Autoridad de Registro.

5.2.2 Control de eventos

En la AC- Puente Senescyt se deben establecer controles, con una frecuencia mínima de una vez al mes, que permitan determinar los eventos realizados dentro de la PKI. Para lo cual, en la AC - Puente Senescyt deberán generarse los logs de los siguientes eventos:

- Encendido y apagado de la Infraestructura tecnológica.
- Creación, borrado o establecimiento de contraseñas y privilegios.
- Inicio y fin de sesión.
- Cambios en la configuración de los componentes PKI
- Actualización del antivirus

5.3 Política de seguridad física de la PKI

La seguridad física proporciona el esquema para minimizar los daños e intromisiones no autorizadas en las actividades y en la información administrada por la AC-Raíz. La aplicación de estas políticas permite:

- Proteger la infraestructura de certificación ubicándolo en áreas protegidas.
- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento de la infraestructura de certificación

5.3.1 Ubicación y construcción

- Las instalaciones de la AC- Puente Senescyt estarán ubicadas dentro del territorio ecuatoriano en una zona en la cual no este comprometido la seguridad física de la PKI, la misma que contará con control de acceso, protección contra siniestros.
- En concreto, las instalaciones donde se realizan los procedimientos de certificación deben ofrecer protección a radiación solar, piso falso, detección y extinción de incendios, sistema anti-humedad, sistema de refrigeración y sistema de suministro eléctrico.
- La instalación, modificación, ampliación y operación de la PKI se lo hará de conformidad a las políticas establecidas en el título habilitante emitido por la ARCOTEL.

5.3.2 Prevenciones

Las instalaciones de la AC- Puente Senescyt deben estar equipadas con:

- Sistemas de alimentación para garantizar el acceso continuo e ininterrumpido de energía eléctrica.
- Sistemas de calefacción /ventilación/ acondicionamiento de aire, para controlar la temperatura y la humedad.
- Las instalaciones de la AC- Puente Senescyt deberán estar ubicadas en una zona libre de inundación. Para lo cual, dichas instalaciones serán ubicadas como mínimo en una segunda planta.
- Las instalaciones de la AC- Puente Senescyt que albergan la infraestructura tecnológica de la PKI deberán disponer de sistemas de detección y extinguidor de incendios

5.4 Política de los roles de certificación

La seguridad de los componentes de la PKI requiere de un recurso humano que garantice la integridad, confidencialidad y disponibilidad de los mismos. En consecuencia, estas políticas permiten determinar, para el personal involucrado en los procedimientos de certificación, los requerimientos de capacitación y los compromisos de confidencialidad mediante una declaración juramentada.

5.4.1 Capacitación

- El personal de la AC- Puente Senescyt, una vez al año, recibirán una adecuada capacitación en la innovación de los procedimientos de certificación digital.

- Una vez al año, toda persona involucrada en el área de certificación será evaluada en base a su idoneidad y rendimiento de sus labores profesionales en la AC- Puente Senescyt.
- El informe de evaluación deberá incluir recomendaciones sobre necesidades de capacitación.

5.4.2 Confidencialidad

- Todos los empleados de la AC- Puente Senescyt, firmarán un compromiso de confidencialidad o no divulgación, en lo que respecta a los procedimientos de certificación.
- De la misma manera, mediante el compromiso de confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo.
- Ningún mensaje de correo electrónico será considerado como privado.
- La AC- Puente Senescyt se reserva el derecho de revisar por ella misma o mediante la prestación de servicios de un tercero, sin previo aviso, los mensajes de correo electrónico del personal y los archivos LOG del servidor de correo, con el fin de prevenir actividades que puedan afectar al funcionamiento de la PKI.
- Los empleados de la AC- Puente Senescyt pueden acceder únicamente al nivel de seguridad física y a las aplicaciones a los que están autorizados.

5.5 Procedimientos de Certificación

Los procedimientos nos permiten indicar y determinar el método que se va utilizar para poder gestionar, generar y administrar los certificados digitales de una PKI, en esta sección se encontrarán descritas los principales procedimientos que serán la base dentro de este proyecto de tesis.

Para poder trabajar con los procedimientos, se debe establecer tanto el marco legal como las políticas del modelo de una PKI para las Instituciones de Educación Superior, es importante determinar dichos procedimientos basándose en los siguientes indicios:

A continuación, se determinará los procedimientos necesarios para el modelo PKI, los cuales permiten establecer una PKI que serán aplicadas a las Instituciones de Educación Superior del Ecuador.

5.5.1 Procedimientos Preliminares

Para prestar servicios de emisión de certificados digitales y la operación de una Infraestructura de Clave Pública para el Sistema Nacional de Educación Superior en el Ecuador se deben seguir los siguientes procesos:

5.5.2 Solicitar Certificado

- El usuario debe ingresar a la página web "https://www.acnagrid.com/certificacion/Solicitud.aspx", para solicitar un certificado nuevo, ingresando Nombre y Apellido, Email, Cédula, Región, Institución, Usuario, Contraseña, Confirmar Contraseña, y guardar su solicitud.

- El usuario puede consultar en cualquier momento el estado de su certificado, mediante la pestaña “Consultar Solicitudes”, ingresando la cédula y el Password.
- La AR Senescyt mediante la página web, ingresa al enlace “Administrar” con usuario y contraseña, de esta manera visualiza el certificado para validar la información del solicitante, aprueba o rechaza la solicitud.
- La AC Subordinada de la Institución mediante la página web, ingresa al enlace “Administrar” con usuario y contraseña y busca las solicitudes verificadas previamente por la AR Senescyt y descarga la información para generar el certificado cambiando el estado de la solicitud a “EN PROCESO“.
- La AC Subordinada sube al repositorio el certificado mediante la página web con su usuario y contraseña, seleccionando la solicitud y haciendo clic en gestionar, una vez cargado el certificado se cambia el estado de la solicitud a “EJECUTADO“.

5.5.3 Instalación Certificado

- La solicitud al encontrarse en estado “EJECUTADO“, la AR Senescyt es la encargada de entregarle al usuario un PIN para la descarga en la página web y la clave de exportación del certificado, los mismos que son entregado al usuario por medio del correo electrónico registrado en la solicitud creada.

- El usuario debe instalar los certificados ruta ubicados en el enlace “Certificado” de la página web, para hacer uso del certificado solicitado, los certificados ruta deben ser seleccionados de acuerdo a la institución y región que pertenece.
- El certificado AC – SENESCYT.pfx ubicado en la carpeta “CERTIFICADOS RUTA”, debe ser instalado por todos los usuarios, sin importar la región o institución en la que se encuentran.
- El usuario debe descomprimir el archivo descargado, en el que encontrará los archivos AC – Region- Sierra.pfx, AC – SENESCYT.pfx, AC- Universidad.pfx, los cuales debe instalar según los pasos que indica el manual ubicado en el enlace “Ayuda” de la página web.
- Para descargar el certificado, el usuario ingresa a la pestaña “Descargar Certificado” de la página web, e ingresa el PIN, Cédula, Password y marca las validaciones “Descargar Certificado Raíz” e “Instalación Certificado Raíz” para poder realizar el proceso.

5.5.4 Suspensión

- La AC- Subordinada ingresa a la página web, en la pestaña suspensión el usuario AdministradorAC realizar la solicitud de suspensión.
- En la solicitud de suspensión ingresar Cédula del titular del certificado por suspender, seleccionar en el campo acción SUSPENSIÓN y seleccionar el motivo de acuerdo a la política establecida.

- La Autoridad de Registro Senescyt comprueba que el titular posee un certificado firmado digitalmente por la AC-SENESCYT consultando al repositorio de los certificados.
- Cuando ya se verifica la información la AR Senescyt envía la petición a la AC Subordinada actualizando el estado de la solicitud en "POR SUSPENDER".
- La AC Subordinada verifica las solicitudes en estado "POR SUSPENDER" y procede a la revocación cambiando el estado de la solicitud a "SUSPENDIDO".

5.5.5 Reactivar

- La AC- Subordinada ingresa a la página web, en el enlace Administrar ingresa el nombre de usuario y contraseña para acceder como usuario AdministradorAC.
- Realiza la reactivación ingresando Cédula del titular del certificado y Reactivar Certificado de acuerdo a la política establecida.

5.5.6 Extinción

- El usuario pude solicitar la extinción de su certificado ingresando a la página web https://www.acnagrid.com/certificacion/, haciendo clic en la pestaña Extinción.
- Para realizar la solicitud de Extinción, ingresar Cédula del titular del certificado y seleccionar el motivo de acuerdo a la política establecida.

- La Autoridad de Registro Senescyt comprueba que el titular posee un certificado firmado digitalmente por la AC-SENESCYT consultando al repositorio de los certificados.
- Cuando ya se verifica la información la AR Senescyt envía la petición a la AC Subordinada actualizando el estado de la solicitud en "POR EXTINCIÓN".
- La AC Subordinada verifica las solicitudes en estado "POR EXTINCIÓN" y procede a la extinción cambiando el estado de la solicitud a "EXTINGUIDO".

5.5.7 Renovar

- El usuario realiza la solicitud de renovación una vez que haya caducado el certificado a través de la página Web https://www.acnagrid.com/certificacion/Renovacion.aspx, ingresando el número de solicitud, cédula y Password.
- La AR Senescyt verifica la identidad del usuario y el período de validez del Certificado para aprobar la solicitud y cambia el estado de la solicitud a "POR RENOVAR".
- En el proceso de renovación la AC Subordinada procede a generar un nuevo certificado para el usuario con los datos validados por la AR Senescyt, de las solicitudes en estado "POR RENOVAR", una vez renovada la solicitud la AC Subordinada cambia el estado a "EJECUTADO".

5.5.8 Revocatoria

- La AC- Subordinada ingresa a la página web https://www.acnagrid.com/certificacion/Suspension.aspx, ingresando con el usuario AdministradorAC y realizar la solicitud de Revocatoria.
- En la solicitud de Revocatoria ingresar Cédula del titular del certificado por revocar, seleccionar en el campo acción REVOCATORIA y seleccionar el motivo de acuerdo a la política establecida.
- La Autoridad de Registro Senescyt comprueba que el titular posee un certificado firmado digitalmente por la AC-SENESCYT consultando al repositorio de los certificados.
- Cuando ya se verifica la información la AR Senescyt envía la petición a la AC Subordinada actualizando el estado de la solicitud en "POR REVOCAR".
- La AC Subordinada verifica las solicitudes en estado "POR REVOCAR" y procede a la revocación cambiando el estado de la solicitud a "REVOCADO".

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- • Se realizó un análisis de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y el Reglamento a la Ley de Comercio Electrónico establecidos en el marco legal Ecuatoriano, las cuales son indispensables para implantar normas, políticas y procedimientos para una PKI basado en Smart Grid para el Sistema Nacional de Educación Superior del Ecuador basadas en un modelo de terceras partes confianza, esto constituye una solución que incluye la simplificación de tareas administrativas y reducción en el número de trámites en la aprobación de solicitudes garantizando la validez legal de los documentos electrónicos.
- Se definió un modelo de confianza puente para la PKI basado en Smart Grid para el Sistema Nacional de Educación Superior del Ecuador, el mismo que se basa en la norma PKIx para implementar servicios de certificación digital. El diseño del modelo implica la asignación de una Autoridad Certificadora Puente, una Autoridad de Registro en el Senecyt, Autoridades Certificadoras Raíz en cada región y Autoridades Subordinadas correspondientes a cada universidad, las cuales trabajan directamente con el usuario final para la aprobación de las peticiones de certificación.

- Se establecieron políticas y procedimientos para el ciclo de vida de un certificado, las mismas que ayudan a eliminar la repetición de procesos para que la actualización de la información sea precisa, válida y confiable, de esta manera se lleva un control de buenas prácticas para la implementación de procesos en un ambiente SmartGrid.

6.2 Recomendaciones

- • Hacer una retroalimentación de las normas, políticas y procedimientos conforme se actualice la Ley de Comercio Electrónico en el Ecuador y aplicarlo según establece el reglamento, es preciso crear una fuente de conocimiento actualizado periódicamente, para que sean utilizados como herramienta de orientación para certificar documentos y reducir la tasa de errores de procesos realizados en forma manual.
- La estructura del modelo puente establecido permite agregar nuevas PKIs independientes si el volumen de instituciones incrementa, por lo que se recomienda llevar un control periódico del número de instituciones para rediseñar el modelo si fuera necesario.
- El cumplimiento de las políticas y procedimientos descritos en el documento son de gran importancia para velar por la seguridad y veracidad de la documentación, se recomienda capacitar al personal que tiene acceso a los recursos que maneja la PKI tanto a nivel físico como lógico del PKI al definir los procedimientos para generar un certificado digital que asegura que los riesgos sean mínimos al ofrecer este tipo de servicio.

Bibliografía

(s.f.). Obtenido de http://portalae.sci.uma.es:8080/export/sites/default/uma/documentos/criptografia_certificado_digital_firma_digital.pdf

(s.f.).

(23 de Octubre de 2003). Obtenido de Proasetel: http://www.proasetel.com/paginas/articulos/obligaciones_entidades.htm

(23 de Octubre de 2003). Obtenido de Proasetel: http://www.proasetel.com/paginas/articulos/obligaciones_entidades.htm

Arnao, D. N. (s.f.). Obtenido de www.uv.es/~montanan/redes/trabajos/PKI.doc

Arnao, D. N. (s.f.).

Arnao, D. N. (2002). *www.uv.es/~montanan/redes/trabajos/PKI.doc.*

C. Adams, S. L. (s.f.). *Understanding PKI: Concepts, Standars and Deployment Consierations.* 2 edition Addison-Wesley Professional.

CÁRDENAS, E. H. (2006). *MODELO DE GESTIÓN DE SERVICIOS PKI BASADO EN UNA ARQUITECTURA ORIENTADA A SERVICIOS.*

Certificación Electrónica Banco Central del Ecuador. (2015). Obtenido de https://www.eci.bce.ec/quienes-somos

Certificación, A. A. (2015). *www.anf.ec*. Obtenido de www.anf.ec: https://www.anf.ec/ec/certificacion/pki-anf-ac/autoridad-de-certificacion.html

CUESTA RUIZ, J., & PUÑALES CASTERO, M. (2002). *Scribd.* Obtenido de http://es.scribd.com/doc/116154580/Infraestructura-de-clave-publica-PKI

Data, S. (2015). *www.securitydata.net.ec*. Obtenido de www.securitydata.net.ec: https://www.securitydata.net.ec/

Ecuador, B. C. (2015). *www.eci.bce.ec*. Obtenido de https://www.eci.bce.ec/home;jsessionid=c81bec539e5dbec267dee300003f

Ecuador, B. C. (s.f.). *https://www.eci.bce.ec/*. Obtenido de https://www.eci.bce.ec/quienes-somos

EcuadorUniversitario. (2012). Obtenido de EcuadorUniversitario: http://ecuadoruniversitario.com/de-instituciones-del-estado/senescyt/la-senescyt-coordina-el-sistema-de-educacion-superior-con-la-funcion-ejecutiva/

FAO. (s.f.). *www.fao.org*. Obtenido de http://www.fao.org/docrep/004/ad094s/ad094s03.htm

Foster, I. (2002). What is the Grid? En *GRIDToday.*

Fuentes, A., Vazquez , J. L., Huedo, E., Montero, R. S., & Llorente, M. (2005). En *Benefits Achieved in Bioinformatics by Using Grid Computing Technology.*

Gallegos, R. R. (2013). *TERCERA OLA DE TRANSFORMACIÓN DE LA EDUCACIÓN SUPERIOR.* Obtenido de TERCERA OLA DE TRANSFORMACIÓN DE LA EDUCACIÓN SUPERIOR: http://www.educacionsuperior.gob.ec

GRID CAFÉ. (s.f.). Obtenido de Grids Internacionales: http://www.gridcafe.org/grids-internacionales_ES.html

IAEN. (s.f.). Obtenido de http://repositorio.iaen.edu.ec/bitstream/24000/400/4/REGLAMENTO%20PARA%20LA%20ACREDITACION.pdf

infoleg. (s.f.). *infoleg.mecon.gov.ar*. Obtenido de http://infoleg.mecon.gov.ar/infolegInternet/anexos/50000-54999/54714/norma.htm

Judicatura, C. d. (2015). *www.funcionjudicial.gob.ec*. Obtenido de http://www.funcionjudicial.gob.ec/index.php/es/inicio.html

Kapil, R. (s.f.). *PKI Security Solutions for the Enterprise.* Wiley.

La Camara de Quito. (12 de Septiembre de 2011). Obtenido de http://www.lacamaradequito.com/uploads/tx_documents/decreto867.pdf

Lapuente, C. G. (21 de Junio de 2011). *Implantación de un sistema de certificados.* Obtenido de http://upcommons.upc.edu/pfc/bitstream/2099.1/12398/1/61021.pdf

LaTecnología PKI. (19 de 11 de 2009). Obtenido de http://glenys-tics.blogspot.com/2009/11/algunas-ventajas-y-desventajas-de-la.html

Ley 2002-67 (Registro Oficial 557-S, 17-IV-2002). (13 de Octubre de 2011). *Desarrollo Amazónico.* Obtenido de http://www.desarrolloamazonico.gob.ec/wp-content/uploads/downloads/2014/05/LEY-DE-COMERCIO-ELECTRONICO-DE-FIRMAS.pdf

Momoth, J. (2012). *Smart Grid Fundamentals of Design and Analysis.* Wiley.

Senecyt. (s.f.). *http://www.senescyt.gob.ec/*. Obtenido de http://www.senescyt.gob.ec/UNIVERSIDADES.pdf

SNIESE. (s.f.). Obtenido de http://www.sniese.gob.ec/web/guest

SNIESE. (s.f.). Obtenido de http://www.sniese.gob.ec/web/guest/linea-de-base;jsessionid=70FB618084DDF0B1AFCB390FF362B06F

SNIESE. (s.f.). Obtenido de http://www.sniese.gob.ec/web/guest/normativa-del-sniese;jsessionid=70FB618084DDF0B1AFCB390FF362B06F

SNIESE. (s.f.). *www.sniese.gob.ec*. Obtenido de http://www.sniese.gob.ec/web/guest/antecedentes;jsessionid=70FB618084DDF0B1AFCB390FF362B06F

VILLAMARÍN, J. J. (s.f.). *http://www.ieep.org.ec/*. Obtenido de http://www.ieep.org.ec/

Wilkinson, B. (2009). *Grid Computing: Techniques and Applications.* CRC Press.

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR:

PONCE DÍAZ JOHANNA ELIZABETH

ELABORADO POR:

VILLAGÓMEZ CABRERA SANDRA STEFANY

DIRECTOR DE LA CARRERA

ING. MAURICIO CAMPAÑA

Sangolquí, 26 enero de 2016