



Copia No Controlada

1. Introducción

1.1. ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01

Este documento establece las normas y condiciones generales de los servicios de certificación digital que presta CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e con su certificado raíz válido hasta el Martes, 02 de Abril de 2030 04:42:02 p.m. y cuyo serial se identifica con el número hexadecimal 07 7e 52 93 7b e0 15 e3 57 f0 69 8c cb ec 0c, en relación con la gestión de la información para el proceso de verificación y emisión de Firmas Electrónicas, las condiciones aplicables por tipo de producto y/o servicio, emisión, uso, revocación, las políticas de seguridad, controles técnicos, los mecanismos de información, difusión, servicio al cliente, entre otras.

El certificado raíz será utilizado exclusivamente para la emisión de certificados de autoridades de certificación subordinadas y lista de certificados de autoridades subordinadas intermedias revocadas, los certificados de CA subordinada a su vez emitirán los certificados de entidad final, los cuales utilizarán los clientes del servicio de certificación digital de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e quién actuará como Autoridad de Registro Local (AR ó ARL utilizado indistintamente en este documento).

La ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 está dirigida a todas aquellas personas individuales o jurídicas, solicitantes, suscriptores, en general a usuarios de las Firmas Electrónicas y terceros que confíen en ellos como evidencias jurídicas y probatorias, o en el ámbito que sean implementados, en cumplimiento de la Ley Para el Reconocimiento de las Comunicaciones y Firmas Electrónicas Decreto Número 47-2008 del Congreso de la República de Guatemala, Reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas Acuerdo Gubernativo 135-2009, Guía de Evaluación del Registro de Prestadores de Servicios de Certificación para la Firma Electrónica del Ministerio de Economía de la República de Guatemala, en su versión vigente.

La actualización y/o modificación de la **ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01**, se realizará a través del Procedimiento para Modificar la ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 y su ESPECIFICACIÓN TÉCNICA POLÍTICAS DE CERTIFICACIÓN ET-FE-02, PR-FE14.

1.2. CÁMARA DE COMERCIO DE GUATEMALA

La CÁMARA DE COMERCIO DE GUATEMALA, es una entidad, constituida por Decreto Gubernativo Número 493, de fecha 26 de febrero de 1894, y ha significado un importante motor en el desarrollo del sector comercial y empresarial guatemalteco. Su amplia trayectoria de 117 años en defensa del comercio y la libertad de empresa, la ha posicionado como la Entidad que mejor representa a sus agremiados y sus objetivos para su desarrollo.

CÁMARA DE COMERCIO DE GUATEMALA tiene sus oficinas centrales en la ciudad de Guatemala, en la 10ma. Calle 3-80 zona 1 y se encuentra en proceso de solicitud de autorización para prestar los servicios de certificación digital abierta al Registro de Prestadores de Servicios de Certificación -RPSC- del Ministerio de Economía de Guatemala.

CÁMARA DE COMERCIO DE GUATEMALA es el ente ejecutor del Proyecto ATN/ME-9031-GU Apoyo al Desarrollo del Comercio Electrónico del BANCO INTERAMERICANO DE DESARROLLO, el cual define como componente uno del Proyecto Confianza en las Transacciones en Línea Fortalecida, creando condiciones reglamentarias y operacionales favorables para los operadores y usuarios cuya actividad C es Implementación de un Servicio de Certificación Digital (Autoridad de Registro) y capacitación del personal de CÁMARA DE COMERCIO DE GUATEMALA del documento Memorando de Donantes. El BANCO INTERAMERICANO DE DESARROLLO financió parcialmente el valor de este Proyecto para otorgar este servicio a la población guatemalteca.

1.3. Protección De Los Derechos De Propiedad Intelectual

Por medio de la presente disposición se establece que toda la información contenida en la Declaración de Prácticas de Certificación **ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01**, pertenece única y exclusivamente a la CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e de tal forma que esta se reserva todos los Derechos relacionados con la propiedad intelectual del presente documento (**ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01**), incluyendo la información, técnicas, modelos, políticas internas, procesos y procedimientos, de acuerdo a la normatividad nacional e internacional relacionada con la materia.

1.4. Intervinientes y estructura del Sistema de Certificación Digital

Los siguientes son los partícipes del **Sistema de Certificación Digital** de **CÁMARA DE COMERCIO DE GUATEMALA** a través de su instancia Firma-e:

1.4.1. Autoridad de Certificación AC Raíz

La AC Raíz, es la Autoridad de Certificación origen de la jerarquía de certificación digital. Este componente de Certicámara es responsable por la emisión de los Certificados digitales que acreditan su plataforma de emisión.

La estructura de sus datos es:

Campo del Certificado Raíz Valor del Certificado Raíz
Clave de la AC raíz 4096 bits
Versión V3
Serial
Identificador único del certificado. Menor de 32 caracteres hexadecimales.
Algoritmo de firma del certificado
SHA1withRSAEncryption

1.4.2. Titulares de Certificados

Los certificados emitidos por la AC raíz tienen como titulares a la propia AC raíz, y a Certicámara S.A.

1.4.3. Certificadoras subordinadas

Cumpliendo con el Marco de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre las Firmas Electrónicas (2001) de las Naciones Unidas, la regulación Guatemalteca y el marco legal colombiano, estos son derivados de la jerarquía de la AC Raíz, donde requieren que la AC Raíz les firme su certificado para que ellos a su vez emitan certificados a los suscriptores finales siguiendo con la cadena de confianza desde el punto raíz de Certicámara, como entidad de certificación abierta acreditada ante la Superintendencia de Industria y Comercio de la República de Colombia.

Para todas las CAs pertenecientes a la infraestructura de llave pública de Certicámara aplica lo expresado en la ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 y ESPECIFICACIÓN TÉCNICA POLÍTICA DE CERTIFICADOS ET-FE-02, coherente con los requisitos generales establecidos por el marco jurídico descrito en el inciso sobre las referencias normativas.

La estructura de los datos del certificado para las autoridades subordinadas es:

Campo del Certificado del Certificado Raíz
Clave pública de la ENTIDAD SUBORDINADA 2048 bits
Versión V3
Serial
Identificador único del certificado.
Menor de 32 caracteres hexadecimales.
Algoritmo de firma del certificado SHA1withRSAEncryption
Datos del emisor
CN
Autoridad de Certificación Raíz de la cadena de certificación

1.4.4. Parte Confiante

Persona que recibe, hace uso o confía de cualquier manera en las Firmas Electrónicas de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** y que por lo tanto se vincula jurídicamente por los términos de esta **ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01**.

1.4.5. Tercero Idóneo

Persona individual o jurídica, que se considera idónea y que podrá estar a cargo, de forma segura y confiable para el **suscriptor**, del procedimiento de la generación de las claves pública y privada. Garantizando con ello la seguridad de que nadie distinto del suscriptor conocerá dichas claves, de conformidad con los términos establecidos en esta **ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01** y siguiendo en todo momento las instrucciones de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, cumpliendo los requerimientos de las auditorías internas y externas que garantizan el aseguramiento de este mecanismo, sin embargo la generación del par de llaves de los suscriptores está a cargo del software de la CA.

1.4.6. Solicitante

Persona individual o jurídica que solicita la emisión de una Firma Electrónica a nombre propio, o de terceros, o en nombre y representación legal de una persona jurídica.

1.4.7. Suscriptor

Es aquella persona, individual o jurídica, que figura en el **certificado digital o firma electrónica avanzada** como titular de la misma, según se deriva de la **Especificación Técnica Políticas de Certificación ET-FE-02** establecida para cada uno de ellos.

1.4.8. Autoridad de Registro:

Es la función que cumple CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e cómo Autoridad de Registro ó conocida como Autoridad de Registro Local, términos utilizados en esta Declaración de Prácticas indistintamente. Para realizar recepción de solicitudes, validación de información y aprobación de emisión de las Firmas Electrónicas, cumpliendo con lo establecido en las normas legales guatemaltecas vigentes para autoridades de certificación, Especificación Técnica Políticas de Certificación ET-FE-02 y parámetros establecidos en los principios de Web Trust.

Existe una autoridad local de registro en la Ciudad de Guatemala. En Bogotá – Colombia, se recopila la información de aprobaciones de la autoridad local de registro de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e y el encargado de la autoridad de registro central ó Registrador envía la información al servidor de autoridad de registro de la PKI para el procesamiento y emisión de certificados digitales.

1.5. Suministro del Certificado digital o firma electrónica avanzada

1.5.1. Cobertura de Logística

La entrega de los certificados digitales se realizara de conformidad a la ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01, cumpliendo con los requerimientos de seguridad necesarios para garantizar que la entrega es personal y que se mantiene en todo momento confidencialidad de la llave privada del certificado del suscriptor.

1.5.2. Requisitos de entrega

La entrega se realiza físicamente en las instalaciones de CÁMARA DE COMERCIO DE GUATEMALA, a través de su instancia Firma-e previa identificación del suscriptor; por lo que el Suscriptor deberá presentar sus documentos de identificación vigentes y originales. CÁMARA DE COMERCIO DE GUATEMALA se reserva el derecho de solicitar cualquier otro documento para corroborar la identidad de la persona que reclama el dispositivo

1.5.3. Tiempo de entrega y gestión

Para la entrega de la Firma Electrónica Avanzada CÁMARA DE COMERCIO DE GUATEMALA, a través de su instancia Firma-e, se reserva el plazo de análisis e investigación para la acreditación de los Solicitantes por un período de tiempo razonable.

1.5.4. Descarga del certificado directamente por parte del suscriptor

En el marco de acuerdos contractuales o en el caso de renovación de certificados digitales, los suscriptores realizarán la generación y descarga del certificado digital o firma electrónica avanzada de manera directa, utilizando los mecanismos tecnológicos que proporciona la plataforma de emisión CÁMARA DE COMERCIO DE GUATEMALA, a través de su instancia Firma-e en su página <http://www.firma-e.com.gt>.

1.6. Usos permitidos para el Certificado Raíz de la entidad de certificación y los certificados digitales en general

El certificado digital o firma electrónica avanzada raíz sólo puede utilizarse para la identificación de la propia autoridad certificación raíz y para la distribución de su clave privada de forma segura. El uso de los certificados emitidos por la AC raíz estará limitado a la firma de certificados digitales y la firma de las listas de certificados revocados correspondientes.

1.6.1. Reglas generales aplicables a las Firmas Electrónicas emitidos por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

El **suscriptor** sólo puede dar a las Firmas Electrónicas los usos que se especifiquen en el contrato que suscriba con **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** de manera individual, o aquellos usos permitidos en esta **DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01**. El contrato celebrado con el suscriptor podrá limitar el alcance de los usos, en función del entorno dentro del cual se está utilizando el certificado digital o firma electrónica avanzada, o de las características especiales del proyecto que se está desarrollando. Cualquier otro uso que se le dé se considerará una violación de esta **ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01** y constituirá una causal de revocación de la **Firma Electrónica Avanzada** y de terminación del contrato con el **suscriptor**, sin perjuicio de las acciones penales o civiles a las que haya lugar.

- El **suscriptor** considera y acepta que los productos y servicios que se anuncian son tal y como se ofrecen individualmente, que los certificados digitales principalmente certifican la identidad de la persona individual que aparece como suscriptor del servicio, que no existe ningún tipo de información implícita que implique servicios o prestaciones adicionales a los expresamente mencionados y que la utilización de los mismos es de su exclusiva responsabilidad.
- El uso de la Firma electrónica y los mensajes de datos que se firmen digitalmente con él, incluyendo transacciones electrónicas monetarias, sin importar su monto, son TOTAL responsabilidad del correspondiente suscriptor y, por lo tanto, CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e no tiene responsabilidad alguna sobre la verificación o fe pública de los mensajes de datos firmados, pues no conoce ni tiene obligación legal de conocer los mensajes firmados digitalmente o el monto de las transacciones que se efectúen con el certificado digital o firma electrónica avanzada en

sistemas de transacciones electrónicas de terceros. En general, CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e como entidad prestadora de Servicios de Certificación Digital y Tercero de Confianza no compromete su responsabilidad en el uso que realice el suscriptor de las firmas digitales, por lo tanto no se tienen límites financieros aplicables en este sentido.

- Toda **parte confiante** de la Firma Electrónica deberá:
 - Verificar la confiabilidad de la firma electrónica del **suscriptor**, así como la de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** y cualquiera otra que figure en los **Firmas Electrónicas**, según lo establecido en esta **ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01** .
 - Verificar que la **Firma Electrónica Avanzada** en la que se pretende confiar no se encuentra registrada en la **base de datos de certificados digitales revocados** que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** tiene para el efecto, y que se encuentra publicada en el sitio de Internet <http://www.firma-e.com.gt>.
 - Delimitar con precisión los datos que se encuentran firmados digitalmente en el mensaje que recibe.

LA CLAVE PÚBLICA CONTENIDA EN UNA FIRMA ELECTRÓNICA AVANZADA ES UN RECURSO TÉCNICO QUE PUEDE UTILIZARSE COMO UN MEDIO PARA CIFRAR O ENCRIPtar LOS MENSAJES DE DATOS QUE SE ENVÍAN, DE TAL MANERA QUE ÚNICAMENTE EL TENEDOR DE LA CLAVE PRIVADA PUEDE DESENCRIPTAR DICHO MENSAJE Y ACCEDER A DICHA INFORMACIÓN. SI LA CLAVE PRIVADA SE PIERDE O SE DESTRUYE, LA INFORMACIÓN QUE HAYA SIDO ENCRIPtADA CON LA CLAVE PÚBLICA NO PODRÁ SER DESCIFRADA. EL **SUSCRIPtor** Y LA **PARTE CONFIANTE** RECONOCEN Y ACEPTAN QUE LA UTILIZACIÓN DE LA CLAVE PÚBLICA DEL **SUSCRIPtor** PARA ENCRIPtar DOCUMENTOS ES SU EXCLUSIVA RESPONSABILIDAD, Y QUE PERDERÁN TODA LA INFORMACIÓN QUE SE ENCUENTRE ENCRIPtADA SI LA CLAVE PRIVADA SE PIERDE O DESTRUYE. **CÁMARA DE COMERCIO DE GUATEMALA A TRAVÉS DE SU INSTANCIA FIRMA-E** NO ASUME NINGUNA RESPONSABILIDAD POR ESTE CONCEPTO.

- Si durante el periodo de vigencia parte o toda la información contenida en la Firma Electrónica pierde actualidad o validez, el suscriptor deberá iniciar el procedimiento de revocación del mismo de conformidad con lo establecido en la sección de Revocación de certificados digitales de esta **ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01** .
- Las Firmas Electrónicas deberán utilizarse tal y como son suministrados por **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**.
- Las Firmas Electrónicas deberán ser retenidas indefinidamente en la base de datos, independiente del estado en que se encuentren.
- Las **Firmas Electrónicas** pueden ser utilizadas con los siguientes propósitos:
 - **Identificación:** El **suscriptor** de la **Firma Electrónica** puede identificarse como persona individual y adicionalmente puede vincularlo con una cualidad o condición que la entidad prestadora de servicios de certificación verifica al momento de emitir la Firma Electrónica, demostrando el acceso a la clave privada asociada con la clave pública que se incluye en la **Firma Electrónica**.

- **Integridad:** El uso de la Infraestructura de Clave Pública le permite comprobar a una **parte confiante** que un mensaje de datos recibido no ha sido alterado entre el envío y la recepción del mismo ni en ningún otro momento.
- **No repudio:** La persona que recibe un mensaje de datos firmado digitalmente y respaldado por una **Firma Electrónica** permite que, cumplidos todos los requisitos de procedimiento del **Sistema de Certificación Digital**, el **suscriptor** no pueda negar el envío de dicho mensaje de datos.

Adicionalmente, si así lo dispone el suscriptor, se podrá utilizar el certificado digital o firma electrónica avanzada para lograr el siguiente atributo:

- **Confidencialidad:** La clave pública del **suscriptor** puede ser usada para cifrar todos los documentos que se le envían, impidiendo que terceras personas tengan acceso a las comunicaciones que se transmiten a través de comunicaciones electrónicas abiertas. LA UTILIZACIÓN DE LA CLAVE PÚBLICA POR PARTE DEL SUSCRIPTOR PARA ENCRIPITAR LA INFORMACIÓN DEBERÁ EN TODO CASO AJUSTARSE A LAS PRESCRIPCIONES LEGALES DE GUATEMALA O DE CUALQUIER OTRO PAÍS DEL MUNDO EN DONDE SE UTILICE EL SISTEMA DE CERTIFICACIÓN DIGITAL EN MATERIA DE TECNOLOGÍAS DE INCRIPCIÓN DE INFORMACIÓN. A pesar de ser posible su utilización para el cifrado de datos, **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no se responsabiliza por esta actividad, debido a que, por motivos de seguridad, la entidad de certificación no guarda copia de la clave privada del Suscriptor. No se garantiza, por tanto, la recuperación de los datos cifrados en caso de pérdida de la clave privada por parte del Suscriptor, el Suscriptor o el Tercero que confía lo hará, en todo caso, bajo su propia responsabilidad.
- El uso y adecuación de los certificados digitales a las necesidades del suscriptor le corresponde de manera exclusiva a éste, respecto de lo cual **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no asume responsabilidad alguna. En ese orden de ideas si de la utilización de la Firma Electrónica Avanzada se desprende algún deber de información a las partes confiantes, éste deber es exclusiva responsabilidad del suscriptor.

1.6.2. Usos prohibidos

- Las Firmas Electrónicas no podrán ser utilizadas por ninguna persona y bajo ninguna circunstancia para fines o en operaciones ilícitas bajo cualquier régimen legal del mundo, particular pero no exclusivamente aquellas que requieren de una autorización estatal para ser realizadas.
- Se encuentra terminantemente prohibido cualquier uso de las Firmas Electrónicas que resulte contrario a la legislación guatemalteca, a los convenios internacionales suscritos por Guatemala, a las normas supranacionales, a las buenas costumbres, a las sanas prácticas comerciales, y a todas las normas contenidas en esta **Declaración de prácticas de certificación**, en la Práctica de Certificación y en los contratos que se firmen entre CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e y el Suscriptor.
- Se encuentra prohibido el uso de los certificados digitales y del Sistema de Certificación Digital como sistema de control para actividades de alto riesgo o para sistemas a prueba de error, dentro de los que se incluyen pero sin limitarse a los siguientes:

- Sistemas de navegación de transporte terrestre, aéreo o marítimo.
 - Sistemas de control de tráfico aéreo.
 - Sistemas de control de armas.
- Los certificados digitales no podrán utilizarse en ningún sistema cuyo fallo pueda ocasionar la muerte o lesión de personas, u ocasionar un serio perjuicio al medio ambiente.
 - El soporte físico del certificado digital o firma electrónica avanzada suministrado por **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** (si aplica) solo puede ser utilizado dentro del contexto del Sistema de Certificación Digital. No podrá incorporarse en el soporte físico suministrado por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e información diferente a aquella expresamente autorizada por esta, ni usarse por fuera del Sistema de Certificación Digital

1.7. Políticas de administración de la AC raíz

1.7.1. Especificaciones de la Organización Administrativa

Nombre: CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e
Correo electrónico: info@firma-e.com.gt
Dirección: 10ma calle 3-80 Zona 1, Guatemala, Guatemala.
Número de teléfono (502) 24172700
Número de Fax (502) 22209393
Sitio Web www.firma-e.com.gt

1.7.2. Persona contacto

Nombre: Ing. Rodrigo Ortiz Rímola
Correo electrónico: rortiz@firma-e.com.gt
Dirección: 10ma calle 3-80 Zona 1, Guatemala, Guatemala.
Número de teléfono (502) 24172700
Número de Fax (502) 22209393
Sitio Web www.firma-e.com.gt

1.8. Definiciones

1.8.1. Certificados digitales

Los **certificados digitales** son archivos digitales que contienen una firma electrónica avanzada en los que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** realiza ciertas declaraciones, respecto de la identidad del suscriptor del servicio, basada en la información que suministra el suscriptor y en procedimientos propios de verificación. Un **certificado digital o firma electrónica avanzada** contiene la información esencial que le permite a una persona que lo recibe a través de un medio electrónico conocer la identidad del remitente del mismo.

Todos los **certificados digitales** que CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e emite son firmados digitalmente por ella. La persona que lo recibe puede tener la seguridad que el mismo no ha sido alterado y que es efectivamente **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** quien lo ha expedido.

1.8.2. Las Entidades de Certificación Digital

Las Entidades de Certificación Digital son **TERCEROS DE CONFIANZA** que se dedican a la prestación de servicios de certificación digital, a través de un **Sistema de Certificación Digital**. Los servicios de certificación digital brindan seguridad a las comunicaciones que se realizan en redes abiertas, como por ejemplo Internet, mediante la emisión de firmas electrónicas en los que ofrecen información a los usuarios sobre la persona con la que se están comunicando.

Para emitir los Firmas Electrónicas las Entidades de Certificación Digital utilizan la Infraestructura de Clave Pública (PKI, por sus siglas en inglés), que es el conjunto de elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que solo posee el suscriptor del servicio y una pública que se incluye en el certificado digital o firma electrónica avanzada, logran:

- Identificar a quien envía una comunicación.
- Impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos.
- Impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos.
- Evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío.

1.8.3. Cadena de Confianza: Autoridad de Certificación Raíz de Certicámara

La Autoridad de certificación raíz (AC) es la autoridad de certificación Raíz de la Infraestructura de Clave Pública de Certicámara cuya función principal es emitir los certificados digitales a su plataforma de certificación digital. Donde un certificado digital o firma electrónica avanzada es un documento electrónico que asocia la identidad de un sujeto (entidad, individuo, dispositivo, etc.) con su correspondiente clave pública y uno o más atributos. El caso específico de un certificado raíz, se corresponde a un certificado que ninguna entidad de confianza superior firma digitalmente como raíz, es decir posee un certificado auto firmado, y es a partir de allí, donde comienza la cadena de confianza. Este proceso de auto firmado hace que los campos del Certificado Raíz cumplan con los estándares internacionales y aplicables que garantizan la interoperabilidad.

Entonces la AC Raíz dispone de un certificado auto firmado con su clave privada, con el que firma los certificados de clave pública de la plataforma de certificación de Certicámara, que a su vez emplean sus claves privadas, para firmar los certificados de los suscriptores finales, de modo que toda la jerarquía se encuentra cubierta por la confianza de la AC Raíz.

Los certificados digitales de clave pública son generados de acuerdo al estándar X.509 versión 3 (1996). El X.509 es el estándar fundamental que define la estructura del certificado de clave pública. El X.509 es el sector de estandarización de Telecomunicación de la Unión Internacional de Telecomunicaciones (Internacional Telecommunications Union-Telecommunications, ITU-T) y el estándar de formato de certificado de la Organización para la Estandarización (Organization for Standardization, ISO).

La arquitectura general, de la certificación digital de Certicámara es la siguiente: La arquitectura jerárquica parte de la Raíz, ancla de la Cadena de Confianza de la certificación digital, llamada Autoridad de Certificación (AC) Raíz. No existe otra AC que pueda firmar el certificado de la AC Raíz. Este es el único caso, en el que la AC Raíz crea un certificado auto firmado por sí misma.

2. Publicación de información de la AC y repositorios de los certificados

2.1. Repositorios

Los Certificados de la AC raíz y AC Subordinada estarán disponible los 365 días del año, durante las 24 horas del día, y en caso de interrupción por causa de fuerza mayor, el servicio se restablecerá en el menor tiempo posible.

- **Para los certificados de las AC Raíz y la ENTIDAD SUBORDINADA acreditados:**

- WEB:
 - AC Raíz Certicámara S.A.
http://www.Certicámara.com/ac_offline_raiz_Certicámara.crt
 - AC Subordinada Certicámara S.A.
http://www.Certicámara.com/ac_online_subordinada_Certicámara.crt

- **Para la lista de certificados revocados (CRL):**

- WEB:
 - AC Raíz Certicámara S.A.
http://www.Certicámara.com/repositoriorevocaciones/ac_raiz_Certicámara.crl
 - AC Subordinada Certicámara S.A.
http://www.Certicámara.com/repositoriorevocaciones/ac_subordinada_Certicámara.crl

CRL con extensión crítica

AC Raíz Certicámara S.A.

http://www.Certicámara.com/repositoriorevocaciones/ac_raiz_Certicámara_extension_critica.crl

AC Subordinada Certicámara S.A.

http://www.Certicámara.com/repositoriorevocaciones/ac_subordinada_Certicámara_con_extension_critica.crl

- **Para la ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01:**

- WEB:
<http://www.firma-e.com.gt/dpc>

- **Para la verificación de estado de revocación de certificados OCSP**

- WEB:
<http://ocsp.Certicámara.com>

El repositorio público de la AC raíz no contiene ninguna información confidencial o privada.

2.2. Publicación

Es obligación para la Entidad de Certificación publicar la información relativa a sus prácticas, sus certificados y el estado actualizado de dichos certificados. Las publicaciones que realice CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, de toda información clasificada como pública, se anunciará en su respectiva página Web de la siguiente manera:

- La lista de Certificados Revocados (CRL), se encuentra disponible en formato CRL V2, en el repositorio de la AC raíz.

- Las Políticas de Certificados de la AC raíz, se podrán ubicar en la versión actualizada del presente documento.
- Todas las versiones del presente documento son públicas y se encuentran disponibles en el sitio Web de la AC raíz <http://www.firma-e.com.gt/dpc> , en formato PDF firmado digitalmente.
- Las llaves públicas de los certificados emitidos por la AC subordinada se encuentran disponibles en el repositorio público LDAP, en formato X.509 v3 y en la dirección <https://ssl.firma-e.com.gt/consulta> los cuales podrán ser consultados por un parámetro de búsqueda <http://www.Certicámara.com/certificadosemitidos/>
- Los datos de contacto de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e en la dirección <http://www.firma-e.com.gt/contacto>
- Los manuales de operaciones de la AC raíz y toda la información considerada relevante a los certificados emitidos se encuentra en la dirección <http://www.firma-e.com.gt/manuales>
- Estado de revocación de certificados OCSP, se encuentra disponible para su consulta vía web en la dirección <https://ssl.firma-e.com.gt/consulta>

2.3. Frecuencia de publicación

2.3.1. Certificados de la AC Raíz

La publicación del certificado se realizará con anterioridad a su puesta en vigencia a través de la página web de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e <http://www.firma-e.com.gt/>. El periodo de validez es hasta el martes, 02 de abril de 2030 a las 4:42:02 p.m.

2.3.2. Lista de Certificados Revocados (CRL)

Se realizarán dos tipos de publicaciones para la lista de Certificados Revocados de la AC Subordinada Certicámara S.A. (CRL):

- Periódicamente:
 - La publicación se efectúa cada hora de manera automática, con una vigencia de tres (3) días.
- Eventualmente:
 - Cada vez que se revoque un certificado digital o firma electrónica avanzada.
 - Cada vez que se comprometa una clave privada.

2.3.3. Estado de revocación de certificados OCSP

El servicio se encuentra disponible de manera continua para su consulta vía web y se actualiza automáticamente en los siguientes casos:

- Cada vez que se revoque un certificado digital o firma electrónica avanzada.
- Cada vez que se comprometa una clave privada.

2.3.4. Declaración de Prácticas de Certificación

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, publicará en el repositorio, las nuevas versiones de este Documento, inmediatamente tras la aprobación de las mismas.

2.4. Controles de acceso al repositorio de certificados

El acceso a la información publicada por la AC Raíz solo será de consulta y no podrá ser modificada por personas no autorizadas. La información pública solo será actualizada por el personal encargado de esta función que labora en CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

Además se garantiza la consulta a la CRL, a los certificados emitidos, al servidor OCSP y ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 en sus versiones anteriores y actualizadas.

Copia No Controlada

3. Identificación y autenticación

3.1. Registros de nombres

3.1.1. Tipos de nombres

La AC Raíz, sólo genera y firma certificados con tipos de nombres acordes al estándar X. 500.
Para la AC raíz:

El DN de la AC raíz está formado por los siguientes atributos:

CN = AC Certicámara S.A.
O = Sociedad Cameral de Certificación Digital - Certicámara S.A.
C=CO

El nombre alternativo (AN) de la AC raíz está formado por los siguientes atributos:

CN = AC Certicámara S.A.
O = Sociedad Cameral de Certificación Digital - Certicámara S.A.
C=CO

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e establece en esta política la emisión de diferentes tipos de certificados. Cada tipo de certificado se identificara por un OID (Object Identifier) único, incluido en el certificado como identificador de política, dentro de la extensión X.509 Certificate Policies.

Certificado tipo I – Certificados para *
(OID política 2.5.862.1.2.)

Este certificado lo genera la Entidad de Certificación de primer nivel para su identificación, es el certificado raíz auto firmado de la infraestructura de clave pública de Certicámara. El uso de este certificado está enmarcado en las actividades de la AC raíz.

3.1.2. Necesidad de que los nombres sean significativos

Las políticas definidas, garantizan que los nombres distintivos (DN) de los certificados son suficientemente significativos para vincular la clave pública con una identidad.

3.1.3. Interpretación de formatos de nombres

Las reglas utilizadas para la interpretación de los nombres distinguidos en los certificados emitidos están descritas en la ISO/IEC 9595 (X.500) Distinguished Name (DN). Adicionalmente todos los certificados emitidos utilizan codificación UTF8 para todos los atributos, según la RFC 3280 ("Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile")

3.1.4. Unicidad de los nombres

La AC raíz define como campo DN (Distinguished Name) del Certificado de Autoridad como único y sin ambigüedad. Para ello se incluirá como parte del DN, específicamente en el campo CN (Common Name), el nombre o razón social del titular del certificado. Por lo tanto, la unicidad se garantiza mediante la confianza sobre la unicidad de los nombres mercantiles en el registro mercantil de la República de Guatemala, documentos de identificación tales como Cédula de Vecindad, Documento Personal de Identificación (DPI) según corresponda en conjunción con sus registros de códigos de identificación tributaria y de identificación tales como Cédula de Vecindad, Código Único de Identificación o Pasaporte según corresponda

El OID para cada uno de esos campos son los siguientes:

- NIT del Solicitante: 1.3.6.1.4.1.23267.50.101.104
- NIT empresa: 1.3.6.1.4.1.23267.2.3
- Cédula de Vecindad: 1.3.6.1.4.1.23267.2.2
- Código Único de Identificación: 1.3.6.1.4.1.23267.2.2
- Pasaporte: 1.3.6.1.4.1.23267.2.2

3.1.5. Resolución de conflictos relativos a nombres

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e no actúa como árbitro o mediador, ni resuelve ninguna disputa relativa a la titularidad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales, etc. Así mismo, este organismo se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

3.2. Validación inicial de la identidad

3.2.1. Métodos de prueba de posesión de la clave privada

El sistema de certificación implementado y utilizado por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e para la administración del ciclo de vida de sus certificados controla y garantiza de forma automática la emisión del certificado firmado al poseedor de la clave privada correspondiente a la clave pública incluida en la solicitud. Esta garantía se logra mediante el formato PKCS#10 que incluye en la propia solicitud una firma electrónica de la misma realizada con la clave privada correspondiente a la clave pública del certificado.

3.2.2. Autenticación de la identidad de una organización o persona

El solicitante presentará la solicitud de acreditación ante CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e con los siguientes requisitos e información:

1. Identificación completa del solicitante.
2. Documentos de identificación emitidos por las autoridades competentes.
3. Contrato de adhesión de los servicios de certificación digital, suscrito por el solicitante con su firma manuscrita o con su firma electrónica emitida por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

3.2.3. Comprobación de las facultades de representación legal

La comprobación de la representación legal del solicitante ante CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e se realizará mediante el cruce con bases de datos de terceros y la comprobación de los documentos legales, establecidos en la legislación guatemalteca que lo califique como representante legal. CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e emitirá una credencial al representante legal el cual le permitirá realizar las solicitudes de acreditación ante CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

3.3. Identificación y autenticación de las solicitudes de renovación de la clave

3.3.1. Identificación y autenticación de las solicitudes de renovación rutinarias.

La identificación y autenticación para la renovación del certificado se debe realizar utilizando las técnicas para la autenticación e identificación inicial. Este método de renovación requiere que la clave privada no esté ni vencida ni revocada.

3.3.2. Identificación y autenticación de las solicitudes de renovación de la clave después de una revocación – clave no comprometida.

La política de identificación y autenticación para la renovación de un certificado después de una revocación sin compromiso de la clave será la misma que para el registro inicial. Adicionalmente el solicitante deberá demostrar satisfactoriamente a CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e que las causas de revocación anteriores ya no están presentes.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e podrá negar discrecionalmente la renovación extraordinaria de un certificado digital o firma electrónica avanzada.

3.4. Identificación y autenticación de las solicitudes de renovación de la clave

La política de identificación para las solicitudes de renovación podrá ser la misma que para el registro inicial. La política de autenticación aceptará solicitudes de renovación firmadas digitalmente por el suscriptor del certificado o de forma manual en las instalaciones de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e puede definir otras políticas de identificación siempre y cuando se garantice la posibilidad de autenticación de identidad de acuerdo a la Declaración de Prácticas de Certificación de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

La AC raíz o cualquiera de las entidades que la componen pueden solicitar de oficio la revocación de un certificado si tuvieran el conocimiento o sospecha del compromiso de la clave privada del suscriptor, o cualquier otro hecho que recomendara emprender dicha acción.

4. El ciclo de vida de los certificados

4.1. Solicitud de certificados

Los procedimientos operativos establecidos por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e para la acreditación serán responsabilidad de los aspirantes a la acreditación. Este proceso se puede llevar a cabo de forma manual dirigiéndose ante las oficinas de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, a través del sistema automatizado de solicitud de productos y servicios visitando la dirección electrónica <https://solicitudes.firma-e.com.gt> o a través de cualquier otro medio electrónico que disponga CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, bien sea a través de su página web o de la de un tercero, dentro del desarrollo de un proyecto.

La documentación física entregada por el solicitante a CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e será almacenada en archivo físico durante 10 años.

Los usuarios que hacen uso del sistema de solicitud de productos y servicios suscriben de manera electrónica mediante aceptación de términos, las condiciones del servicio, especificadas en la presente ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 y en el contrato de prestación de servicios de certificación digital.

Una vez aprobada la solicitud por los sistemas de verificación de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, el solicitante presenta las garantías necesarias para obtener la acreditación como suscriptor de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, en la cadena de confianza y pasa a ser un suscriptor.

La acreditación del suscriptor establece que opera de conformidad con las políticas y procedimientos establecidos por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e se reserva el derecho de solicitar documentos adicionales a los que sean exigidos en el formulario de solicitud en presentación original o fotocopias de los mismos cuando así lo considere necesario para verificar la identidad o cualquier calidad del solicitante, así como de exonerar de la presentación de cualquiera de ellos cuando la identidad del solicitante haya sido suficientemente verificada por Cámara de Comercio de Guatemala por otros medios. CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e se reserva el derecho de exigir que las fotocopias de los documentos solicitados sean auténticas. Sin limitarse a ellos, CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e podrá exigir adicionalmente:

1. Licencia de conducir.
2. Constancia de Carencia de Antecedentes Penales y/o Policíacos.
3. Carné de afiliación al Instituto Guatemalteco de Seguridad Social.
4. Pasaporte Vigente.
5. Carné de afiliación al I.R.T.R.A.
6. Carné de Colegiado Profesional.
7. Referencias o Certificaciones bancarias de la empresa y/o del **solicitante**.
8. Referencias personales del solicitante.
9. Referencias comerciales del solicitante.
10. Certificados y/o Contratos Laborales.
11. Traducción oficial de cualquier documento que considere necesario para el proceso de identificación.

La solicitud de un servicio de certificación digital puede radicarse en la sede principal del Operador de PKI, que CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e posee para la prestación del servicio, o puede efectuarse a través de los canales electrónicos o físicos que para el efecto disponga CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e se reserva el derecho de negar la emisión de una Firma Electrónica a un solicitante, a su propia discreción, por lo que no podrá exigírsele responsabilidad alguna por este motivo.

4.2. Rechazo de la solicitud de una Firma Electrónica

Si CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e decide rechazar la solicitud de emisión de una Firma Electrónica, lo notificará por escrito al solicitante, a la dirección física o electrónica que se haya indicado en el sistema automatizado de solicitud de productos y servicios en la dirección electrónica <https://solicitudes.firma-e.com.gt> con indicación de los motivos que la justifican.

En caso de que los defectos encontrados sean subsanables, se le otorgará al solicitante de la Firma Electrónica un plazo de quince días hábiles para llevar a cabo la subsanación, transcurrido el cual la Entidad de Registro procederá a confirmar o a revocar por escrito su decisión de manera definitiva.

4.3. Emisión de certificado

Luego de verificar y aprobar las exigencias establecidas en la legislación guatemalteca y en esta ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01, el sistema de la AC procederá a realizar la emisión del certificado al suscriptor.

4.3.1. Acciones de la AC durante la emisión de la Firma Electrónica

La emisión de las firmas electrónicas implica la autorización de la solicitud por parte del sistema de la AC Subordinada. Después de la aprobación de la solicitud se procederá a la emisión de los certificados de forma segura y se pondrán los certificados a disposición del SUSCRIPTOR.

En la emisión de las firmas electrónicas la AC Subordinada:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Protege la confidencialidad e integridad de los datos de registro.
- Todos los certificados iniciarán su vigencia en el momento que se indica en el propio certificado.
- Se utilizará el campo de "not before" con este fin. Ningún certificado será emitido con un periodo de validez que se inicie con anterioridad de la fecha actual. Sin embargo, si se podrán emitir certificados cuyo periodo de validez se inicie en el futuro o una fecha posterior a la actual.

4.3.2. Notificación al solicitante por parte de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e acerca de la emisión de su firma electrónica

El SUScriptor sabrá sobre la emisión efectiva del certificado por medio de una notificación al mismo, mediante correo electrónico remitido por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e. Así mismo, se publica en el sitio web de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e los certificados digitales emitidos.

4.3.3. Aceptación de Firmas electrónicas - Forma en la que se acepta la Firma Electrónica

Se considera aceptado la firma electrónica por parte del suscriptor una vez se complete el proceso de firmado de la petición del certificado por la AC Subordinada dentro de las instalaciones de CÁMARA DE COMERCIO DE GUATEMALA.

4.3.4. Publicación del certificado por la AC

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e proveerá diversos tipos de comunicación como correos electrónicos, comunicaciones escritas, repositorio LDAP, repositorio Web y los que considere pertinentes para publicar la aceptación de un certificado.

El servidor de la autoridad de registro introducirá las llaves públicas de las firmas electrónicas emitidas por la autoridad de certificación subordinada en la estructura de directorio LDAP (Lightweigh directory access protocol) de la PKI, en el momento que la firma electrónica sea emitida.

4.3.5. Notificación de la emisión del certificado por la AC a otras Autoridades

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e notificará a las entidades, organismos del gobierno y empresas privadas la emisión de un certificado por medio de la página Web de CÁMARA DE COMERCIO DE GUATEMALA <https://.firma-e.com.gt>.

4.4. Uso del par de claves y de la Firma Electrónica

El uso de las firmas electrónicas emitidas por la AC raíz y la AC Subordinada son los previstos en la legislación Guatemalteca y en sus reglamentos.

4.4.1. Uso de la clave privada del certificado por la ENTIDAD SUBORDINADA

El titular sólo puede utilizar la clave privada y el certificado para los usos autorizados en esta ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01. CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e emite certificados con los campos de uso de clave privada limitados a firma de certificados y firma de CRL.

4.4.2. Uso de la clave pública y del certificado por los terceros de buena fe

Los terceros de buena fe sólo pueden depositar su confianza en las Firmas Electrónicas para aquello que establece esta ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 y la Ley.

Los terceros de buena fe pueden realizar operaciones de clave pública de manera satisfactoria confiando en la firma Electrónica emitida por la cadena de confianza. Así mismo, deben asumir la responsabilidad de verificar el estado de la Firma Electrónica utilizando los medios que se establecen en esta ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01.

4.5. Renovación de la Firma Electrónica con cambio de clave

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e notifica con al menos quince días calendario de anticipación a sus **suscriptores** la terminación de la vigencia de su **Firma Electrónica**. Esta notificación puede realizarse por correo electrónico a la dirección de correo electrónico proporcionada por el suscriptor o por cualquier otro medio idóneo de comunicación cuando CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e lo considere pertinente. Aquellos suscriptores cuya Firma Electrónica se encuentren almacenados en dispositivo criptográfico, serán notificados adicionalmente por el software controlador del dispositivo, el cual le permitirá consultar su vigencia en cualquier momento.

Sin embargo, no es obligación de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e garantizar la efectividad de la notificación sobre la terminación de la vigencia de su certificado o confirmar la recepción de la misma, pues es una obligación del Suscriptor conocer la vigencia de su Firma Electrónica y adelantar los trámites de renovación ante CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e con antelación al vencimiento de su firma, teniendo en cuenta que esta solicitud deberá surtir el proceso de verificación de datos, conciliación de pago y aprobación por parte de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, proceso que CÁMARA DE COMERCIO DE GUATEMALA adelantará según lo establecido en los acuerdos de nivel de servicio establecidos con el suscriptor y dependiendo de la calidad y veracidad de la información proporcionada por el suscriptor.

Es importante destacar, que CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e notificará a través del correo electrónico proporcionado por el Suscriptor, además del vencimiento de la firma electrónica, otros procesos o procedimientos como mantenimiento u otros, para lo cual se hace uso de la dirección de correo electrónico suministrada por el solicitante en el proceso de emisión de la firma electrónica, dirección electrónica que será responsabilidad del suscriptor, y por lo tanto es obligación del suscriptor completar correctamente dicha dirección en el sistema automatizado de solicitud de productos y servicios en la dirección electrónica <https://solicitudes.firma-e.com.gt>.

4.5.1. Causas para la renovación de una Firma Electrónica

La causa de la renovación de una firma por parte del suscriptor es por la caducidad.

4.5.2. Entidad ó suscriptor que puede solicitar la renovación de la Firma Electrónica

Las entidades o suscriptores están autorizados(as) para solicitar la renovación de una firma con cambio de clave cuando:

- Se encuentre próximo a caducarse el servicio y el suscriptor desee continuar utilizando una firma que acredite las condiciones que le fueron aprobadas en la firma electrónica. Las

entidades o suscriptores deberán de realizar esta solicitud con al menos 15 días de anticipación.

4.5.3. Procedimiento de solicitud para la renovación de una Firma Electrónica

El suscriptor deberá cumplir nuevamente con el proceso de acreditación para solicitar la renovación de una firma. Por tal motivo, el procedimiento de solicitud para la renovación de una firma es el mismo que el de acreditación. Salvo que no tendrá que adjuntar documentos a la solicitud a menos que estos hayan perdido vigencia en caso que aplique.

4.5.4. Notificación de la emisión de una nueva firma electrónica a un suscriptor

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e notificará al suscriptor sobre la emisión efectiva de una nueva firma por medio de un correo electrónico al mismo emitido por el sistema de renovaciones de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

4.5.5. Publicación del certificado renovado por la AC

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e proveerá diversos tipos de comunicación como correos electrónicos, comunicaciones escritas, repositorio LDAP, repositorio Web,y los que considere pertinentes para publicar la renovación de una firma.

4.5.6. Notificación de la emisión de una firma por la AC a otras entidades

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e notificará a las entidades, organismos del gobierno y empresas privadas la renovación de una firma por medio de la página Web de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

4.6. Modificación de Firmas Electrónicas

Durante el ciclo de vida de una firma la modificación de los campos no está determinado efectuarse en la AC raíz o en la AC Subordinada.

4.7. Revocación de firmas electrónicas

La revocación de una **firma electrónica** es el mecanismo por el que se da por terminado su periodo de confiabilidad en forma anticipada al presentarse alguna de las causas establecidas en la presente **Declaración de Prácticas de Certificación ET-FE-01**, originando la pérdida de confianza en el mismo.

4.7.1. Supuestos de revocación

4.7.1.1. Revocación voluntaria del suscriptor.

El **suscriptor** podrá voluntariamente solicitar a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** la revocación de la **firma electrónica** emitida, en cuyo caso **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** iniciará el procedimiento de revocación de la **firma**.

4.7.1.2. Otros supuestos de revocación

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e revocará la **firma electrónica** respecto de la cual tenga conocimiento de que se ha producido alguno de los siguientes hechos:

- Compromiso de la clave privada del **suscriptor** por cualquier motivo o circunstancia.
- La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.
- Por muerte o incapacidad sobrevenida del **suscriptor**.
- Por liquidación de la persona jurídica representada que consta en la **Firma electrónica**.
- Por la confirmación de que alguna información o hecho contenido en la **firma electrónica** es falsa, así como la ocurrencia de hechos nuevos que provoquen que los datos originales no se adecuen a la realidad.
- Por el compromiso de la clave privada de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** o de su sistema de seguridad de manera tal que afecte la confiabilidad de la **firma**, por cualquier circunstancia, incluyendo las fortuitas.
- Por el cese de actividades de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, salvo que las **firmas electrónicas** expedidas sean transferidos a otra Entidad de Certificación.
- Por orden judicial o de entidad administrativa competente.
- Pérdida, inutilización o compromiso de la seguridad del **soporte físico** de la **firma electrónica** que haya sido debidamente notificada a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**.
- Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato y en esta **Declaración de Prácticas de Certificación ET-FE-01**
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la confiabilidad del **certificado digital o firma electrónica avanzada**.
- El manejo indebido por parte del **suscriptor** de la **Firma Electrónica**.
- Por el incumplimiento del suscriptor o de la persona jurídica que representa o a la que está vinculado a través del Contrato del servicio de Certificación Digital proporcionado por **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**.
- Por reporte de cartera vencida ocasionado por el pago no efectuado de los servicios que le está proporcionando **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** al suscriptor o a la persona jurídica que representa. En este supuesto de revocación **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** realizará una suspensión de la firma el cual será identificado dentro de la CRL en el campo de "Código de razón de la lista de revocación de firmas" con el valor "Posesión de certificado (6)" ó en inglés "Certificate Hold (6)", con lo cual se podrá interpretar que el certificado se encuentra suspendido y podrá ser rehabilitado por **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** dependiendo de la actualización de reporte de cartera vencida. Se aclara que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no ofrece el servicio de suspensión de certificados a los suscriptores.
- Por la concurrencia de cualquier otra causa especificada en la presente **Declaración de Prácticas de Certificación**.

CÁMARA DE COMERCIO DE GUATEMALA A TRAVÉS DE SU INSTANCIA FIRMA-E NO TIENE DEBER ALGUNO DE INVESTIGACIÓN O REVISIÓN DE LA OCURRENCIA DE CUALQUIERA

DE LAS CAUSALES DE REVOCACIÓN ESTABLECIDAS EN ESTE APARTADO. CÁMARA DE COMERCIO DE GUATEMALA A TRAVÉS DE SU INSTANCIA FIRMA-E INICIARÁ EL PROCEDIMIENTO DE REVOCACIÓN DE FIRMAS ELECTRÓNICAS TAN SOLO UNA VEZ TENGA NOTICIA DE LA OCURRENCIA DE CUALQUIERA DE ELLAS.

EL SUScriptor Y LA PARTE CONFIANTE TIENEN LA OBLIGACIÓN DE INICIAR EL PROCEDIMIENTO DE REVOCACIÓN DE LA FIRMA ELECTRÓNICA- TAN PRONTO COMO TENGAN CONOCIMIENTO DE LA EXISTENCIA DE ALGUNO DE ESTOS SUPUESTOS. EL INCUMPLIMIENTO DE ESTA OBLIGACIÓN LOS HACE RESPONSABLES DE LOS PERJUICIOS OCASIONADOS POR ESTA OMISIÓN.

4.7.2. Efectos de la revocación

El efecto de la revocación de la **firma electrónica** es la pérdida de confiabilidad del mismo, originando el cese permanente de la operatividad de la **firma electrónica** conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación digital.

Se prohíbe el uso de la **firma electrónica**, del **soporte físico del certificado digital o firma electrónica avanzada**, o de cualquier otro bien o servicio que **Cámara de Guatemala, a través de su instancia Firma-e** haya proporcionado al **suscriptor**, una vez haya sido revocada la firma electrónica.

La revocación de la **firma electrónica** por causa imputable a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** originará la emisión de una nueva **firma electrónica** a favor del **suscriptor** por el plazo equivalente al restante para concluir el período originario de validez de la **firma electrónica** revocada, asumiendo **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** el costo implícito en la nueva emisión. En los demás casos el costo del nuevo **certificado digital o firma electrónica avanzada** será asumido por el **suscriptor**.

Una vez cumplido el procedimiento de revocación, la Firma Electrónica será publicada en la **base de datos de certificados digitales revocados**, para notificar a las **partes confiantes** que dicha **firma electrónica** ha sido revocada.

4.7.3. Procedimiento de revocación

4.7.3.1. Legitimación activa

El **suscriptor** una vez tenga conocimiento de la existencia de alguna de las causales que dan lugar a la revocación, podrá informársela a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** para que la evalúe y proceda de conformidad con el procedimiento establecido.

En todo caso, **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** podrá iniciar de oficio el procedimiento de revocación de **firmas electrónicas**, en cualquiera de los casos previstos en el apartado anterior.

Las autoridades judiciales o administrativas podrán, en aquellos supuestos contemplados en la ley, ordenar a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** la revocación de cualquier **firma electrónica**.

4.7.3.2. Recepción de solicitudes de Revocación

La solicitud de revocación de **firmas electrónicas** podrá hacerse telefónicamente llamando en horario hábiles de Lunes a Viernes de 8:00 a 17:00 horas, a la línea de atención de servicio exclusivo de revocaciones: 24172700 Ext.732 o a cualquiera de los números que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** ha destinado para el efecto, los cuales se pueden consultar en la sección de Revocación de **Certificados Digitales** en <http://revocaciones.firma-e.com.gt/> , o a través de los medios electrónicos que disponga **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**.

Si la persona que expone una causal que da lugar a la revocación de la **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no es el **suscriptor** o en caso de ser este último no puede identificarse satisfactoriamente, o no pueden comprobar de manera fehaciente la existencia de la causal de revocación, deberá dirigirse personalmente a cualquiera de las oficinas de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** en horarios de oficina, con la prueba de la existencia de la causal de revocación respectiva, sin perjuicio de que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** disponga de las medidas que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** establezca para la seguridad del **Sistema de Certificación Digital**. Se aclara que una vez se reciba la solicitud de revocación por medio de correo físico o correo electrónico, adjuntando la carta escaneada de solicitud de revocación y se compruebe la veracidad de dicha solicitud, se procederá a la revocación de la firma, sin periodos de gracia para dichas revocaciones.

4.7.4. Revocación

Si **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** lo considera necesario realizará, mediante su personal o por intermedio de terceras personas, las averiguaciones y gestiones pertinentes para comprobar la existencia de la causal de revocación que sea invocada. Dichas gestiones podrán incluir la comunicación directa con el **suscriptor** y la presencia física del tercero que invoca la causal de revocación.

Si la causal es comprobada, **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** incorporará la **firma electrónica** en la **Base de datos de certificados digitales revocados** como **firma electrónica** revocada. De lo contrario, dará por terminado el proceso de revocación de la firma electrónica. Se aclara que Cámara de Comercio de Guatemala, no ofrece el servicio de suspensión de certificados a los suscriptores.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e debe Informar al suscriptor, dentro de las 24 horas hábiles siguientes, la suspensión del servicio o revocación de su (s) certificado (s), de conformidad con la normatividad vigente.

Si el suscriptor desea obtener una nueva firma electrónica, debe completar nuevamente el sistema automatizado de solicitud de productos y servicios en la dirección electrónica <https://solicitudes.firma-e.com.gt>.

4.7.5. Revocación del certificado digital o firma electrónica avanzada por parte del usuario

El usuario de los servicios de certificación digital podrá revocar el certificado de firma electrónica asociado a su nombre, comunicándose por medio telefónico a CÁMARA DE COMERCIO DE GUATEMALA, en la cual se verificará la identidad del usuario mediante la aplicación de un test con información relacionada a su historial.

El sistema notificará automáticamente al correo electrónico del usuario, la revocación efectiva del certificado de firma electrónica.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e puede suspender los certificados de firma electrónica al término de la vigencia del contrato de prestación de servicios de certificación digital, en virtud del tiempo que haya sido contratado por parte del suscriptor.

Un tercero podrá solicitar la revocación de un certificado de firma electrónica mediante comunicación al oficial de revocaciones al correo electrónico revocaciones@firma-e.com.gt, cuando conozca de la ocurrencia de una de las causales de revocación. El oficial de revocaciones tiene la potestad de suspender dicho certificado mientras valida la veracidad de la causal de revocación y dependiendo del resultado de la validación, podrá reactivar o revocar el certificado de firma electrónica.

4.7.6. Comunicación y Publicación de la revocación

La decisión de revocar la **firma electrónica** será comunicada por **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** al **suscriptor** mediante correo electrónico o a través del medio que encuentre conveniente para el efecto.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e notificará a las Entidades de Registro, a través de correo electrónico o cualquier otro medio que estime conveniente, la lista de firmas electrónicas revocadas sobre los cuales haya recibido solicitud de revocación.

La revocación de la firma electrónica comenzará a producir efectos a partir de su publicación por parte de **Cámara de Comercio de Guatemala** en la **base de datos de certificados digitales revocados**, salvo que la causa de revocación sea el cese de actividades de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

Las **listas antiguas de certificados digitales revocados** CRL se mantendrán almacenadas en la base de datos del servidor de la autoridad de certificación y la copia de respaldo de esta base de datos será almacenada en medios ópticos (DVD/CD) que permitan su fácil y segura recuperación. **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** almacenará estas bases de datos contenedoras de las listas históricas en DVD/CD y los depositará para custodia en las oficinas de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, o en instalaciones especializadas cuando lo considere oportuno bajo riguroso criterios de confidencialidad como una cintoteca para su consulta hasta diez años posterior a la pérdida de vigencia del certificado raíz de la autoridad de certificación.

Cuando una persona o entidad requiere consultar una CRL antigua puede solicitar información a través de teléfono 24172700 Ext.732 o enviar una comunicación con una dirección de correo electrónico a las siguientes direcciones:

Dirección: 10ma. Calle 3-80 Zona 1, Guatemala.
Dirección de correo electrónico: info@firma-e.com.gt

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e atenderá la solicitud enviando por correo electrónico la CRL requerida.

4.8. Servicios de comprobación de estado de las Firmas Electrónicas.

4.8.1. Características Operativas

Para la validación de las firmas electrónicas se dispone de varios prestadores de Servicios de Validación que proporcionan información sobre el estado de las firmas emitidos por la jerarquía de certificación. Se trata de un servicio de validación en línea (**Autoridad de Validación, AV**) que implementa el Online Certificate Status Protocol siguiendo la RFC 2560. Mediante el uso de ese protocolo se determina el estado actual de un certificado electrónico sin requerir las CRLs. Un cliente de OCSP envía una petición sobre el estado del certificado a la AV, la cual, tras consultar su Base de Datos, ofrece una respuesta sobre el estado del certificado vía HTTP por medio de la dirección <http://ocsp.Certicámara.com>

También se dispondrá del archivo CRL publicado en el sitio web de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e en el URL <http://www.firma-e.com.gt/descargas>

4.8.2. Disponibilidad del Servicio

El servicio de comprobación de estado de firmas electrónicas está utilizable de forma ininterrumpida todos los días del año.

4.8.3. Características adicionales

Para hacer uso del Servicio de validación en línea consultando la dirección <http://ocsp.Certicámara.com>, es responsabilidad del tercero de buena fe disponer de un Cliente OCSP que cumpla la RFC 2560.

4.9. Finalización de la suscripción

La finalización de la suscripción de una firma se produce en los siguientes casos:

- Revocación de la firma por cualquiera de las causas de revocación.
- Caducidad de la vigencia de la firma.

4.10. Custodia y recuperación de la llave

4.10.1. Prácticas y políticas de custodia y recuperación de la clave

La clave privada de la AC raíz se custodia por un dispositivo criptográfico HSM. Para el acceso al repositorio de claves privadas se usa el esquema umbral limite (k,n) de Shamir tanto en software como en dispositivos criptográficos.

5. Controles de seguridad física, de gestión y de operaciones

5.1. Controles de seguridad física

5.1.1. Ubicación y construcción

Todas las operaciones críticas de la AC raíz y la AC Subordinada están protegidas físicamente con todas las medidas de seguridad necesarias para los elementos más críticos y con vigilancia durante las 24 horas al día, los 7 días a la semana. Estos sistemas están separados de otros de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, de forma que sólo el personal autorizado pueda acceder a ellos.

Los Centros de Proceso de Datos de la AC raíz y la AC Subordinada cumplen los siguientes requisitos físicos:

- Para evitar posibles daños, las instalaciones se encuentran alejadas de salidas de humos.
- No posee ventanas al exterior de la torre.
- Circuito cerrado de televisión en las áreas críticas o de acceso restringido.
- Control de acceso basado en tarjeta de proximidad, PIN y biometría.
- Sistemas de protección y prevención de incendios: detectores, extintores, formación del personal para actuar ante incendios, etc.

5.1.2. Acceso físico

El acceso físico a las instalaciones de la AC Raíz y la AC Subordinada de Certicámara, están protegidas por diversos controles de acceso, de modo que sólo el personal autorizado puede acceder a las mismas. Los controles de acceso, zonas y procesos están definidos en las políticas de seguridad de la AC raíz y AC Subordinada.

Estos controles son basados en la identificación de nivel 2 con tarjeta inteligente, nivel 3 de huella biométrica, con circuito cerrado de televisión permanente para registrar cada uno de los accesos a las instalaciones, archivando periódicamente los mismos.

Los sistemas de la AC raíz estarán físicamente separados de otros sistemas de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e de forma que únicamente el personal autorizado pueda acceder a ellos, y se garantice la independencia de los otros sistemas informáticos.

Los Sistemas de la AR de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, utiliza controles biométricos para el acceso a área destinada a la recepción de documentación, análisis entrega de certificados digitales.

Circuito de Cámaras de Grabación 24x7 autónomo.

5.1.3. Alimentación eléctrica y aire acondicionado

Los Sistemas donde están ubicados los equipos de la AC Raíz y AC Subordinada de Certicámara cuentan con las condiciones de potencia y ventilación necesarias para evitar fallos de potencia u otras anomalías eléctricas o en los sistemas eléctricos.

El cableado de los equipos está protegido para evitar interceptaciones o daños y se han adoptado medidas especiales para evitar las pérdidas de información provocadas por la interrupción en el flujo de suministro eléctrico, conectando los componentes más críticos a UPS para asegurar un suministro continuo de energía eléctrica, con una potencia suficiente para mantener la red eléctrica durante los eventos de apagado controlado del sistema y para proteger a los equipos frente fluctuaciones eléctricas que los pudieran dañar.

Los sistemas de aire acondicionado, conserva las estancias de los equipos con las condiciones de humedad y temperatura adecuadas para el correcto funcionamiento y mantenimiento de los mismos.

Los Sistemas de la Autoridad de Registro de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e cuentan con un sistema de soporte de UPS de respaldo energético para asegurar la no pérdida de información operativa.

5.1.4. Exposición de agua

La instalación de la AC Raíz y AC Subordinada de Certicámara, está protegida para evitar las exposiciones al agua de los mismos, mediante detectores de humedad, inundación y otros mecanismos de seguridad apropiados al medio.

Los Sistemas de la AR de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, está protegida para evitar las exposiciones al agua de los mismos, mediante detectores de humedad, inundación y otros mecanismos de seguridad apropiados al medio.

• Protección y prevención de incendios

La instalación de la AC Raíz y AC Subordinada de Certicámara, cuenta con sistema de detección y extinción inteligentes. Está conformado por:

- Panel de control inteligente
- Una bomba de gas ECARO 25, no daña la capa de ozono y no contamina el ambiente.
- Boquillas de extensión en el techo
- Detectores de incendios en el techo y techo falso
- Sistema de prealarma. Activa los detectores de incendios para detectar, controlar y localizar el evento. Si dos detectores de incendios son activados de manera simultánea el sistema procede a descargar el gas transcurridos treinta segundos del estado de alarma.
- Activación manual de bombona de gas. Cuando falle la activación automática de la bombona, se cuenta con una palanca debidamente identificada.
- Posee un botón para realizar la descarga de gas ECARO 25, en caso de falla del sistema.

La instalación de la AR de de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, cuenta con sistema de detección y alarma de incendios.

5.1.5. Sistemas de almacenamiento

La información relacionada a la infraestructura de la AC raíz y AC Subordinada de Certicámara se almacenan de forma segura en armarios ignífugos y cajas fuertes, según la clasificación de la información en ellos contenida.

Estos sistemas de almacenamientos se encuentran en desiguales entidades para eliminar riesgos asociados a una única ubicación. La AC Raíz y AC Subordinada, cuenta con lugares de almacenamiento interno y externo.

La instalación de la AR de de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, cuenta con lugares de almacenamiento interno y externo.

5.1.6. Eliminación de residuos

La AC Raíz y la AC Subordinada mantienen mecanismos de revisión de todos los materiales desechables donde se almacena información (disquetes, papel, películas, etc.) son revisados, antes de su eliminación o reutilización, con el objeto de comprobar si contienen información sensible, siendo físicamente destruidos, salvo que puedan reutilizarse como medio de soporte, en cuyo caso se elimina la información de manera segura.

5.1.7. Almacenamiento de copias de seguridad

Todas las copias de seguridad son almacenadas en entidades distantes a la AC Raíz y AC Subordinada. Estas dependencias están protegidas con medios y mecanismos de seguridad, apegadas a buenas prácticas internacionales de seguridad.

La copia de seguridad de bases de datos, aplicaciones y archivos de transacción logs, son enviadas a diario a un sitio externo durante los días laborales de la semana.

La instalación de la AR de de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, cuenta con un Procedimiento de Copias de Seguridad PR-IF-02.

5.2. Controles funcionales

5.2.1. Roles de confianza

La AC Raíz, AC Subordinada y la AR Local, cuentan con un personal que por sus responsabilidades son sometidos a procedimientos de control especiales debido a que su actividad es esencial para el correcto funcionamiento de la entidad prestadora de servicios de certificación digital CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e. Así tienen la consideración de roles de confianza:

- Responsable de la clave privada de la Autoridad de Certificación Raíz y AC Subordinada. Este cargo no existe par la AR Local.

- Responsables de la protección de la clave privada de la AC raíz y la AC Subordinada. Para lograr esta protección los administradores deben usar una tarjeta inteligente como método de autenticación fuerte. Este proceso de autenticación es necesario para la activación y desactivación de la clave privada. Este cargo no existe par la AR Local.
- Administrador de HSM: Encargados de la definición de claves de administración del HSM, de su custodia, de su configuración y puesta en marcha. Encargados de configurar el acceso al HSM por parte de las aplicaciones, de la inicialización del token PKCS#11, de asistir en las tareas de exportación e importación del material criptográfico, etc. También realizará el respaldo correspondiente del HSM. Este cargo no existe par la AR Local.
- Usuario Registro o Registrador: Se encargan exclusivamente de las funciones relacionadas con la emisión, tramitación y la revocación de las firmas electrónicas. Estos procedimientos son realizados sobre la aplicación de Registro utilizando los controles de autenticación y autorización propios del sistema. Adicionalmente, podrán suspender certificados, tras recibir la solicitud del Directorio y cualquier otra actividad extraordinaria con la debida autorización. Las Authority Revocation Lists (ARL) son emitidas y publicadas manualmente por el administrador del sistema o en su ausencia por el personal de soporte interno en el URL correspondiente al CDP especificado en los certificados emitidos para autoridades de certificación subordinada con la periodicidad establecida en la ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 (1 año para las ARL) y deben colaborar con los Auditores en todo aquello que les sea requerido para verificar la publicación. Este Cargo existe para la AC Raíz, AC Subordinada y la AR Local.
- Administrador del Sistema: Responsable por realizar todas las tareas relacionadas con la instalación, configuración y mantenimiento del sistema de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e. Responsable del funcionamiento de los sistemas que componen el sistema de la AC raíz y AC Subordinada, del hardware y del software base. La responsabilidad de este perfil incluye, entre otros, la administración del sistema de base de datos, del repositorio de información (OCSP, LDAP, Web, Active Directory, etc.) y de los sistemas operativos. Debe velar por la prestación de servicios con el adecuado nivel de calidad y fiabilidad, en función del grado de criticidad de éstos. Son responsables de la correcta ejecución de la Política de Copias, y en particular, de mantener la información suficiente que permita restaurar eficientemente cualquiera de los sistemas. Se encargará de llevar a cabo o delegar de manera controlada las copias de backup locales. Este cargo no existe para la AR Local.
- Oficial de Seguridad: Debe cumplir y hacer cumplir las políticas de seguridad de la AC raíz y AC Subordinada, y debe encargarse de cualquier aspecto relativo a la seguridad: física, de las aplicaciones, de la red, etc. Será el encargado de gestionar los sistemas de protección perimetral y en concreto de la gestión de las reglas de los Firewalls. Debe encargarse de la instalación, configuración y gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos. Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, etc. Es el responsable de la gestión y control de los sistemas de seguridad física del ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01, de los sistemas de control de acceso, de los sistemas de acondicionamiento ambiental y de alimentación eléctrica. Debe encargarse de explicar los mecanismos de seguridad al personal que deba conocerlos, de concienciar a todo el personal de la AC raíz y la AC Subordinada, y de hacer cumplir las normas y políticas de seguridad. Debe establecer los calendarios para la ejecución de análisis de vulnerabilidades, ensayos y pruebas de los planes de contingencia del servicio y auditorías

de los sistemas de información. Debe colaborar con los Auditores en todo aquello que les sea requerido. Este Cargo existe para la AC Raíz, AC Subordinada y la AR Local.

Responsabilidades:

- Constatar la existencia de toda la documentación del ciclo productivo requerida y enumerada
 - Comprobar la coherencia de la documentación con los procedimientos, activos inventariados, etc.
 - Comprobar el seguimiento de incidencias y eventos.
 - Comprobar la protección de los sistemas: explotación de vulnerabilidades, logs de acceso, usuarios, etc.
 - Comprobar alarmas y elementos de seguridad física.
 - Comprobar adecuación a normativa y legislación.
 - Comprobar conocimiento de los procedimientos por parte del personal implicado.
 - Autorizados a consultar archivos, trazas y logs de auditoría de las entidades de la PKI.
- Coordinador de Autoridad de Certificación: Se encargará del seguimiento y control en el desarrollo de las funciones atribuidas a cada perfil de los descritos anteriormente, y de la distribución de nuevas tareas entre los perfiles. Se encargará de servir de medio de comunicación entre el personal adscrito a cada uno de los perfiles y la dirección de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.
- Responsabilidades:
- Se encargará de plantear decisiones estratégicas a la dirección de la Autoridad de Certificación y de aprobar decisiones tácticas.
 - Orientará al personal de AC raíz y AC Subordinada sobre la formación a adquirir, cursos, talleres y facilitará el desarrollo de esos cursos y planes de formación. Debe colaborar con los Auditores en todo aquello que les sea requerido.
 - El Homologo para el cumplimiento de estas funciones en la AR Local será el Gerente de Firma-e como Administrador ante la Regulación Guatemalteca.

5.2.2. Número de personas requeridas por tarea

Como medida de seguridad las responsabilidades están compartidas entre los distintos roles y personas, de modo que la actitud negligente o dolosa de alguno de ellos no afecta gravemente a la actividad de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e Raíz o AC Subordinada. El número de personas requeridas por tarea estarán distribuidas de la siguiente manera:

- Responsables del par de claves de la AC raíz y AC Subordinada: Los responsables de las tarjetas inteligentes y activación de la clave privada son:
 - Operador de la Autoridad de HSM
 - Operador de la Autoridad de Certificación

5.2.3. Identificación y autenticación para cada rol

Los usuarios encargados de cada uno de los roles descritos en los apartados anteriores se autentican mediante la utilización de criptografía fuerte. Esta autenticación se lleva a cabo utilizando firmas electrónicas resguardadas por medio de tarjetas inteligentes para la AC raíz y AC Subordinada.

La autenticación se complementa tanto para la AC raíz, AC Subordinada y la AR Local con las correspondientes autorizaciones para acceder a determinados activos de información del sistema de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

5.3. Controles de seguridad personal

5.3.1. Requerimientos de antecedentes, calificación, experiencia y acreditación.

El personal que ejecuta actividades en las instalaciones o sistema de la AC raíz y AC Subordinada debe poseer la cualificación y experiencia en entornos de prestación de servicios de certificación. Adicionalmente el personal debe cumplir los requerimientos de seguridad de la organización y poseer:

- Nociones y experiencia en entornos de certificación digital.
- Educación básica sobre seguridad en sistemas de información.
- Formación específica para su función.
- Título académico o experiencia en la industria equivalente

En el caso de la AR Local el personal cumple con los requerimientos establecidos por la Normatividad Guatemalteca vigente, para los Sistemas de Certificación Digital.

5.3.2. Requerimientos y frecuencia de actualización de la formación CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

Se preverá inducciones al personal ante cambios tecnológicos del entorno, introducción de nuevas herramientas o modificación de procedimientos operativos.

Adicionalmente se llevará a cabo sesiones formativas ante cambios en la Declaración de Prácticas de Certificación u otros documentos relevantes al funcionamiento, administración y/o gerencia de la AC raíz y AC Subordinada.

5.3.3. Sanciones por acciones no autorizadas

Las cláusulas contractuales del personal de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, definen el procedimiento sancionador para los empleados que incumplen las mismas, especificando las sanciones por efectuar una acción no autorizada, el uso no autorizado de la autoridad o el uso no autorizado de los sistemas. En cualquier caso si CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, sospecha de que algún empleado está efectuando una acción no autorizada, automáticamente suspende su permiso de acceso, con la posibilidad de despedido de la institución. Y actuar en concordancia con la Normatividad Guatemalteca vigente.

5.3.4. Documentación proporcionada al personal CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e se encuentra en implementación de un Sistema de Gestión de Calidad ISO 9001:2008 con apego Seguridad de la Información ISO 27001:2005 que proporciona a sus empleados toda la documentación y buenas prácticas de seguridad de la información necesarias para el correcto desempeño de sus tareas. Entre la documentación provista se encuentran:

- Declaración de Prácticas de Certificación
- Manuales de Operación, administración, instalación y utilización de herramientas de la AC raíz y AC Subordinada.
- Procedimiento de Gestión de Riesgo
- Política de Privacidad
- Organigrama y funciones del personal

5.4. Procedimiento de control de seguridad

5.4.1. Tipos de eventos registrados

La AC Raíz y la AC Subordinada, almacenan registros electrónicos de eventos (logs) relativos a su actividad como entidad de certificación.

Estos registros son guardados, de manera automatizada y en los demás casos en formato papel u otros medios. Estos ficheros están a disposición del Oficial de Seguridad de la Información en los casos en que sea necesario.

Cada registro de eventos incluye datos relativos a:

- Fecha y hora en que se produjo
- Número de serie o secuencia de entrada en el registro
- Identificación del personal que introdujo en el evento según su rol
- Los eventos que registra la AC Raíz y la AC Subordinada son los siguientes:
- Eventos de sistema:
 - Instalación de Sistema Operativo
 - Instalación de la aplicación de la AC Raíz y AC Subordinada
 - Instalación de los módulos de hardware criptográfico (HSM)
 - Cambio de módulo de hardware criptográfico (HSM)
 - Eliminación de módulo criptográfico
 - Intentos de acceso a la AC Raíz y AC Subordinada
- Configuración de cambios al equipo de la AC Raíz y AC Subordinada, en concreto:
 - Hardware
 - Software
 - Sistema Operativo
 - Usuarios
 - Perfiles de seguridad
 - Privilegios de administrador
 - Auditorías
 -
- Acceso físico:
 - Acceso del personal al centro de computo de datos

- Acceso del personal al sistema
- Conocimiento o sospecha de violación de la seguridad física
- Anomalías inesperadas:
 - Fallos en el chequeo de la integridad del software
 - Ataques a la red (confirmados o bajo sospecha)
 - Fallos en la red
 - Fallos en el equipamiento
 - Fallos de energía
 - Quebrantamientos de la Práctica de Certificación
 - Reinicio del Sistema Operativo

Acciones de los operadores de AC Raíz y AC Subordinada:

- Gestión de cuentas
- Realización de copias de seguridad de las bases de datos
- Almacenamiento de las bases de datos
- Manipulación de ficheros
- Envío al directorio de cualquier documento o archivo
- Acceso a las bases de datos
- Firma de las tablas que utiliza en la aplicación
- Uso indebido de las claves privadas
- Acciones tomadas en respuesta a cualquier solicitud
- Carga de la tarjeta inteligente con certificados
- Envío de las claves al modulo criptográfico
- Los relacionados con la gestión del ciclo de vida de los certificados y CRLs

5.4.2. Análisis de registros de logs

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e cuenta con una herramienta de análisis de logs, que emite automáticamente alertas al área de Administración del Sistema, con el objeto de que las posibles fallas o alertas sean validadas y remediadas si se requiere.

Ahora bien, en caso de eventos extraordinarios, la extracción de logs deja trazas de auditoria para su posterior revisión.

5.4.3. Periodo de retención para los logs de auditoria

- El área de Seguridad de la Información custodiará por un tiempo máximo de 2 años los correos de logs generados de sistema, seguridad y aplicación enviados y firmados digitalmente por el Área de sistemas.
- Semanalmente el área de sistemas realizara revisión de los logs generados de sistema, seguridad y aplicación.
- El software de monitoreo de logs guarda adicionalmente en una base de datos todos los registros, que hacen parte del alcance del procedimiento de Copias de Respaldo.

5.4.4. Sistema de recopilación de información de auditoria

El sistema de recopilación de información es ejecutado por: sistemas operativos, procesos en la aplicación de la AC raíz y AC Subordinada, y por el personal que las opera. Por lo tanto, este sistema es una combinación de procesos automáticos. Las características de este sistema son las siguientes:

- Permite verificar la integridad de la base de datos.
- Asegura el no repudio por parte de los autores de las operaciones realizadas sobre los datos. Esto se consigue mediante las firmas electrónicas.
- Guarda un registro histórico de actualización de datos, es decir, almacena versiones sucesivas de cada registro resultante de diferentes operaciones realizadas sobre él.
- La siguiente tabla es un resumen de los posibles peligros a los que una base de datos puede estar expuesta y que pueden detectarse con las pruebas de integridad:
 - Inserción o alteración fraudulenta de un registro de sesión.
 - Supresión fraudulenta de sesiones intermedias.
 - Inserción, alteración o supresión fraudulenta de un registro histórico.
 - Inserción, alteración o supresión fraudulenta del registro de una tabla de consultas.

5.4.5. Notificación al sujeto causa del evento

Cada vez que se audite un evento el Administrador del sistema informa, previamente, al autor del mismo. Sin embargo, cuando un operador conoce algún evento susceptible de auditoria, debe informar inmediatamente al Oficial de Seguridad de la Información para que proceda en función de la gravedad del evento.

5.4.6. Análisis de vulnerabilidad

La AR Local CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, aplica un Procedimiento de Seguridad de la Red de Datos

5.5. Archivo de informaciones y registros de eventos

5.5.1. Tipo de informaciones y eventos registrados

- Respecto al ciclo de vida de las claves de AC Raíz y AC Subordinada:
 - Generación de las claves de la AC Raíz y AC Subordinada
 - Instalación de claves criptográficas y sus consecuencias
 - Copia de respaldo de las claves
 - Almacenamiento de las claves
 - Recuperación de claves criptográficas
 - Depósito de las claves
 - Uso de las claves
 - Destrucción de claves
 - Custodia de claves y de aparatos o cualquier otro soporte de claves
- Relacionados con el ciclo de vida de los certificados:
 - Recepción de solicitudes para certificados
 - Sometimiento de claves públicas para certificación
 - Distribución de las claves públicas
- Relacionados con el ciclo de vida de los dispositivos criptográficos (HSM):
 - Recepción dispositivos
 - Entrada o traslado al lugar de almacenamiento
 - Uso de dispositivos
 - Desinstalación de dispositivos
 - Designación del dispositivo para el servicio o reparación
 - Retirada de dispositivos
- Otros:
 - Actualización de la ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01

- Modificaciones de las obligaciones contractuales
- Acuerdos de confidencialidad
- Trazas de auditoría
- Accesos y modificaciones de la documentación solicitada por los auditores.
- Convenios suscritos por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e
- Autorización de acceso a los sistemas de información.

5.5.2. Periodo de retención para el archivo

Las trazas de la información suministrada por los suscriptores son conservadas durante un periodo de dos años.

5.5.3. Protección del archivo

Las medidas de seguridad definidas están destinadas a proteger los archivos de accesos (internos o externos) no autorizados, de modo que sólo ciertas personas pueden consultar, modificar o eliminar los archivos. Los archivos son almacenados en lugares seguros, con todas las medias de seguridad necesarias para protegerlos de factores naturales.

5.5.4. Procedimientos de copia de seguridad del archivo

Se realizan dos copias diarias de los ficheros que componen los archivos a retener. Una copia se realiza en local y se almacena en un sitio seguro dentro del centro de datos principal de la AC Subordinada, el cual cumple con las condiciones ambientales y físicas de seguridad.

La segunda copia de los datos se realiza de forma cifrada y remota, se almacena en el Centro de Datos Alterno, ubicado en un edificio distinto a la sede principal de la AC Subordinada. Los procedimientos se describen en el documento de políticas y procedimientos de la AC raíz y AC Subordinada.

5.5.5. Procedimientos para obtener y verificar información archivada

Los eventos registrados están protegidos mediante técnicas criptográficas, de forma que nadie salvo las propias aplicaciones de visualización y gestión de eventos pueda acceder a ellos. Sólo el personal autorizado tiene acceso a los archivos físicos de soportes y archivos informáticos, para llevar a cabo verificaciones de integridad u otras.

Esta verificación debe ser llevada a cabo por el Oficial de Seguridad de la Información que debe tener acceso a las herramientas de verificación y control de integridad del registro de eventos de la PKI. De forma automática se realizan comprobaciones de la integridad de los archivos electrónicos (backups), en tiempo de su generación y se crea una incidencia en el caso de errores o comportamientos imprevistos.

5.6. Cambio de clave

Las claves de los certificados emitidos por AC Raíz dejarán de tener validez en el mismo momento en que lo haga su certificado autofirmado. Una vez expirado la AC Raíz generará un nuevo par de claves que autofirma para generar el nuevo certificado raíz.

5.7. Recuperación en caso de desastre

Los requisitos de notificación y los procedimientos de recuperación en caso de compromiso de la clave privada corresponden a la AC Raíz y Subordinada de Certicámara:

5.7.1. Procedimientos de gestión de incidentes y vulnerabilidades

La AR Local cuenta con un Procedimiento para la Implementación de Planes de Contingencia para la generación de desastres.

El Procedimiento garantiza que CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e pueda continuar prestando sus servicios esenciales de producción de certificados en presencia de desastres, después de identificar, evaluar, gestionar y minimizar cualquier tipo de riesgo.

5.7.2. Alteración de los recursos hardware, software y/o datos

La AC Raíz y AC Subordinada, disponen de un plan de continuidad del negocio de actividades que le permiten seguir operando si el hardware, software y/o los datos son alterados (pero no destruidos). CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, actualiza periódicamente este plan con el fin de asegurar su vigencia en todo momento.

El plan incluye los procedimientos necesarios para garantizar la contingencia de la actividad durante el período de tiempo transcurrido entre el desastre y el restablecimiento de la situación original (dando prioridad a la publicación de las CRL's).

5.7.3. Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad

El plan de continuidad del negocio de la AC Raíz y AC Subordinada considera el compromiso o sospecha de su clave privada como un desastre. En este caso el Documento prevé la publicación y difusión, inmediatamente, de la revocación de su certificado con el objeto de impedir la confianza en el mismo.

El plan de continuidad del negocio de la AC Raíz y AC Subordinada prevé la revocación de su certificado como consecuencia inmediata del compromiso de la clave privada.

5.7.4. Seguridad de las instalaciones tras un desastre natural o de otro tipo

La AC Raíz y la AC Subordinada, disponen de ubicaciones externas para mantener almacenadas las copias de seguridad, para minimizar los efectos en caso de desastre natural o de otro tipo sobre las instalaciones primarias.

5.8. Cese de la actividad

En el evento en que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** deba por cualquier circunstancia cesar sus actividades deberá:

Iniciar en forma inmediata el Procedimiento para el cese de Actividades de Firma-e PR-FE-09 ante el **Registro de Prestadores de Servicios de Certificación – Ministerio de Economía.**

Comunicar la extinción mediante el envío de un correo electrónico dirigido a todos los **suscriptores** cuyas **firmas electrónicas** permanezcan en vigor y la publicación de un anuncio en dos diarios de amplia circulación nacional. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

Procurar establecer, cuando ello fuera posible, acuerdos con terceras personas para transmitir todas sus obligaciones y derechos dentro del sistema de prestación de servicios certificación con la intención de continuar el servicio. Si se produce la subrogación, a la cual el **suscriptor** da su consentimiento de manera expresa, esta **Declaración de Prácticas de Certificación** seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito.

Proceder, en caso de no haberse podido llevar a cabo transferencia de derechos y obligaciones a otra entidad, a la revocación de todos los **firmas electrónicas** una vez transcurrido el plazo de dos meses desde la comunicación.

Indemnizar adecuadamente a aquellos **Suscriptores** que lo soliciten cuando sus firmas electrónicas sean revocadas con anterioridad al plazo previsto de vigencia, pactándose como tope para la indemnización el costo efectivo del servicio, descontando a prorrata el coste por los días transcurridos desde el inicio del contrato hasta la fecha de resolución.

Cualquier otra obligación que establezca la ley.

Copia No Controlada

6. Controles de seguridad técnica

6.1. Generación e instalación de par de claves

6.1.1. Generación del par de claves

La AC Raíz, genera el par de claves (Pública y Privada) utilizando un dispositivo de hardware criptográfico (HSM) que cumple con los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con FIPS 140-2 Nivel 3 o superior nivel de seguridad, y la creación de llaves de la CA utiliza un algoritmo de generación de números pseudo aleatorio.

El procedimiento de generación de las claves para las subordinadas acreditadas ante CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e es idéntico, en su propio HSM.

6.1.2. Entrega de la clave privada a la entidad subordinada

La ENTIDAD SUBORDINADA es responsable de la generación de su par de claves y por lo tanto responsable de su resguardo y custodia.

6.1.3. Entrega de la clave pública a la entidad subordinada

Las claves públicas generadas bajo el control de la ENTIDAD SUBORDINADA se envían a CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e como parte de una solicitud de acreditación. Esta solicitud se realiza en formato PKCS#10, firmado digitalmente con la clave privada correspondiente a la clave pública que se solicita certificar.

6.1.4. Disponibilidad de la clave pública

La clave publica de la AC raíz estará disponible en <http://www.firma-e.com.gt/descargas> las 24 horas del día los 7 días de la semana de forma continua, a menos que se notifique de un mantenimiento programado o por defectos ocasionados por terceros ajenos a la prestación de servicios de certificación digital de CÁMARA DE COMERCIO DE GUATEMALA, como lo pudieran ser empresas proveedoras de Internet o energía eléctrica o cualquier servicio que requiera el usuario para acceder por parte del usuario a la clave pública.

6.1.5. Tamaño de las claves

Los algoritmos criptográficos empleados por la AC Raíz para firmar los certificados son SHA1withRSA y SHA256withRSA.

La longitud de la clave con el algoritmo RSA de la AC Raíz es de 4096 bits, y los de las ENTIDADES SUBORDINADAS podrán ser de 2048 bits.

6.1.6. Parámetros de generación de la clave pública y verificación de la calidad

La AC raíz debe generar sus pares de claves de acuerdo con RFC 3280 y PKCS#1.

El algoritmo de generación de claves es el RSA. La verificación de la calidad se realiza de acuerdo con el informe especial del ETSI SR 002 176, que indica la calidad de los algoritmos de firma electrónica.

Los algoritmos y parámetros de firma utilizados por la AC raíz para la firma de certificados electrónicos y listas de certificados revocados son los siguientes:

- Algoritmo de firma: RSA
- Parámetros del algoritmo de firma: Longitud del Módulo=4096/2048
- Algoritmo de generación de claves: rsagen1
- Método de relleno: emsa-pkcs1-v1_5
- Funciones criptográficas de Resumen: SHA-1/SHA-256

6.1.7. Hardware/Software de generación de claves

La AC Raíz, genera su par de claves utilizando un modulo de hardware criptográfico (HSM). La autenticación contra el HSM requiere de al menos 2 de 3 operadores. Este procedimiento sigue el esquema K de N, con el modo no persistente del dispositivo criptográfico. En este modo es necesario garantizar la conexión física del último juego de tarjetas en el lector del HSM, para abrir la clave privada de la AC Raíz.

6.1.8. Generación del par de llaves de los suscriptores

El algoritmo que se utiliza para la generación del par de llaves de los suscriptores es RSA no inferior a 2048 bits usando como función criptográfica de resumen o hash, el denominado SHA1. Los suscriptores utilizan dispositivos de hardware token USB para generar su llave privada, los cuales cumplen con el estándar FIPS 140 Nivel 3. En el caso de generación de certificado en formato PKCS#12 se utiliza el algoritmo RSA no inferior a 2048 bits usando como función criptográfica de resumen o hash, el denominado SHA1, cumpliendo el estándar FIPS 140 Nivel 1 por el uso de Microsoft Enhanced Cryptographic Provider.

6.1.9. Propósitos de utilización de claves

Los certificados emitidos por la AC Raíz incluyen la extensión Keyusage para restringir el propósito de la clave pública del certificado, indicando que la claves solo es para:

- Firma certificado
- Firma CRL

6.2. Protección de la clave privada

La clave privada de la AC Raíz, es protegida por un esquema de seguridad generada por un dispositivo criptográfico. Con la finalidad de mantener el resguardo de las claves privadas del certificado auto firmado, la clave privada nunca se encuentra descifrada fuera del HSM. Las copias de seguridad mantienen el secreto de la clave privada de la misma forma en que se resguarda la clave privada original.

6.2.1. Estándares para los módulos criptográficos

El HSM que utiliza la AC Raíz, para generar sus claves es certificado FIPS 140-2 Nivel 3.

La clave pública ha sido almacenada en formato electrónico firmado, de modo que están protegidas de fallos electrónicos y/o problemas con la potencia eléctrica.

Por lo tanto, la puesta en marcha de una AC implica las siguientes tareas:

- Inicialización del estado del módulo HSM.
- Creación de las tarjetas de administración y de operador.
- Generación de las claves de la AC.

6.2.2. Control “n” de “m’ de la clave privada

La clave privada, de la AC Raíz, se encuentra bajo control multipersona.

Ésta se activa mediante la inicialización del software de AC por medio de una combinación de operadores de la AC, administradores del HSM y usuarios de Sistema Operativo. Éste es el único método de activación de dicha clave privada.

6.2.3. Custodia de la clave privada

La clave privada de la AC raíz y AC Subordinada se encuentra alojada en un dispositivo criptográfico. El mismo cumple con los requisitos establecidos en un perfil de protección de dispositivo seguro de firma electrónica de autoridad de certificación normalizado, de acuerdo con FIPS 140-2 Nivel 3 de seguridad.

El resto de claves privadas de operadores y administradores se encuentran contenidas en smartcards criptográficas en poder de los administradores de cada entidad, la llave privada de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e no es conservada en fideicomiso por un tercero.

6.2.4. Copia de seguridad de la clave privada

Las copias de seguridad de las claves privadas se realizan con dispositivos criptográficos adicionales. La clonación del material criptográfico de un HSM sólo es viable con la colaboración de un mínimo de tres administradores del HSM, operadores del HSM, un Administrador de Sistemas y los custodios del material criptográfico.

6.2.5. Archivo de la clave privada

En relación al numeral 6.2.3 las copias de backup de las claves privadas estarán bajo custodia de forma cifrada en el centro de cómputo alterno. Las copias de backup de las claves privadas se realizan en archivos seguros ignífugos.

6.2.6. Inserción de la clave privada en el módulo criptográfico

Las claves privadas se crean dentro del módulo criptográfico en el momento en que este se inicializa. Posteriormente la clave privada generada dentro del HSM es exportada en forma cifrada.

6.2.7. Método de activación de la clave privada

El único método de activación para la clave privada consiste en la utilización de las tarjetas inteligentes para repartir el acceso en distintas personas y roles. Explícitamente la única combinación para activar la clave privada requiere de dos de tres administradores del HSM, tres de ocho operadores del HSM y un administrador del Sistema Operativo de la aplicación.

6.2.8. Método de desactivación de la clave privada

Un administrador del Sistema Operativo puede proceder a la desactivación de la clave privada de la AC raíz y AC Subordinada. Después de haber sido activada por la combinación descrita en el apartado anterior el operador puede proceder a la desactivación mediante la detención de la aplicación de la Autoridad de Certificación.

6.2.9. Método de destrucción de la clave privada

La AC Raíz y la AC Subordinada eliminarán su clave privada cuando expire su plazo de vigencia o haya sido revocada. La destrucción se realizará utilizando los comandos establecidos para borrar físicamente de la memoria del HSM la parte en la que estaba grabada la clave. Lo mismo ocurrirá con sus copias de seguridad.

6.2.10. Pérdida de vigencia de los sistemas de cifrado

La siguiente tabla ilustra el tiempo que tomaría encontrar la clave privada para diferentes tipos de atacantes con la tecnología actualmente existente¹:

RSA/DSA	Atacante individual	Grupo Pequeño	Red Académica	Gran Compañía	Agencia de Inteligencia
274	Semanas	Días	Horas	Milisegundos	Microsegundos
384	Siglos	Décadas	Años	Horas	Segundos
512	Milenios	Siglos	Décadas	Días	Minutos
768	Inviabile	Inviabile	Inviabile	Siglos	Siglos
2304	Inviabile	Inviabile	Inviabile	Inviabile	Milenios

Las claves que CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e entrega a sus suscriptores son llaves de 2048 bits. Como se puede apreciar, con la tecnología y

¹ Tomado de "Digital Certificates", de Jalal Feghhi, Peter Williams

recursos computacionales actualmente existentes, cualquier intento por descifrar la llave privada de los suscriptores tomaría siglos, haciéndolo en la práctica imposible.

No obstante lo anterior, si alguna circunstancia, como por ejemplo el descubrimiento de nuevas tecnologías, acarrea un incremento en la vulnerabilidad de los sistemas de cifrado de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, ésta tomará tan pronto como le sea posible las medidas necesarias para devolver la confiabilidad al Sistema de Certificación Digital, incluyendo aquellas que se detallan en esta Declaración de Prácticas de Certificación.

6.2.11. Ranking del módulo criptográfico

El módulo criptográfico utilizado tanto por la AC raíz como por la ENTIDAD SUBORDINADA posee la certificación FIPS 140-2 nivel 3.

6.3. Otros aspectos de la gestión del par de claves

6.3.1. Archivo de la clave pública

La clave pública de la AC Raíz y AC Subordinada, es archivada según el formato estándar PKCS#7, por un período de 20 años.

6.3.2. Periodos operativos de los certificados y periodo de uso para el par de claves

El par de claves de la AC raíz tendrá una validez hasta el martes, 02 de abril de 2030. Por otro lado los periodos de operación de los certificados serán de diez años.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación de la AC raíz y AC Subordinada se deben generar y almacenar en tarjetas inteligentes. Su protección se garantiza mediante un PIN en posesión de personal autorizado.

6.4.2. Protección de datos de activación

Sólo el personal autorizado posee las tarjetas criptográficas con capacidad de activación de las claves privadas de ACs, así mismo conocen los PINs necesarios para su utilización.

La clave personal de acceso (PIN) es confidencial, personal e intransferible y es el parámetro que protege las claves privadas permitiendo la utilización de los certificados de AC raíz y AC Subordinada; por lo tanto, deben tenerse en cuenta unas normas de seguridad para su custodia y uso:

- El PIN es confidencial, personal e intransferible.
- Se debe memorizar y no anotarlo en ningún documento físico ni electrónico que conserve o transporte junto a su tarjeta inteligente.
- No debe enviarse ni comunicarse el PIN a ninguna persona.

- Los operadores y administradores deben cambiar el PIN cuando sospechen que es conocido por otra persona.
- Se recomienda cambiar el PIN periódicamente.

6.5. Controles de seguridad en la administración de los computadores personales

6.5.1. Requisitos técnicos específicos

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, ha definido el **Procedimiento de Seguridad de la Información PR-FE-15 que a ella le corresponden en cuanto a** los controles de seguridad técnica aplicables a los equipos informáticos. Estos controles se refieren a aspectos tales como el uso de los equipos, controles de acceso discrecional y obligatorio, auditorías, identificación y autenticación, etiquetas, pruebas de seguridad y de intrusión. La AC raíz así como su AC Subordinada también poseen políticas de seguridad de la información alineadas con lo establecido en esta Declaración de Prácticas de Certificación.

6.5.2. Calificaciones de seguridad computacional de la CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e utiliza productos certificados, por el Nivel E3 de las normas ITSEC.

6.6. Controles de seguridad del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Los requisitos de seguridad para el desarrollo de sistemas para la AC raíz y la ENTIDAD SUBORDINADA son exigibles.

Se debe realizar un análisis de diseño de seguridad durante las fases de diseño y especificación de nuevos requisitos de cualquier componente que se va a utilizar en las aplicaciones de la AC raíz y AC Subordinada. Esto con la finalidad de garantizar que los sistemas involucrados sean seguros.

La infraestructura tecnológica de la AC raíz y AC Subordinada debe estar dotada de entornos de desarrollo y producción claramente diferenciados e independientes. Debe utilizarse procedimientos de control de cambio para las nuevas versiones y actualizaciones.

6.6.2. Controles de administración de seguridad

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, debe mantener un inventario de todos los activos informáticos.

La configuración de los sistemas se debe auditar de forma periódica y realizar un seguimiento del crecimiento de necesidad de recursos de acuerdo a la demanda.

6.6.3. Calificaciones de seguridad del ciclo de vida

Durante todo el ciclo de vida se debe implementar controles de seguridad que permitan instrumentar y auditar cada fase de los sistemas de la AC raíz y AC Subordina.

6.7. Controles de seguridad de la red

La infraestructura tecnológica de la AC raíz y AC Subordinada posee una red con todos los mecanismos de seguridad necesarios para garantizar un servicio fiable e íntegro. Se utiliza firewall o intercambio de datos cifrados entre redes para garantizar integridad. Por otro lado se utilizan tecnologías de renuncias y alta disponibilidad para garantizar un funcionamiento confiable y de alto rendimiento. Adicionalmente la infraestructura debe ser auditada periódicamente por personas internas y externas de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e.

6.8. Controles de ingeniería de los módulos criptográficos

La AC raíz y AC Subordinada utilizan módulos criptográficos hardware y software disponibles comercialmente desarrollados por terceros. La AC raíz y AC Subordinada únicamente utiliza módulos criptográficos con certificación FIPS 140-2 Level 3 (nCipher nForce 400, netHSM 500).

Copia No Controlada

7. Perfiles de certificados, LRAC y OCSP

7.1. Perfil del certificado

Los certificados de la AC raíz y la ENTIDAD SUBORDINADA son emitidos conforme a las siguientes normas:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, April 2002
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.1 (2004-03): Qualified Certificate Profile, 2004
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (prevaleciendo en caso de conflicto la TS 101 862)

7.1.1. Número de versión

La AC Raíz y AC Subordinada, soportan y emiten certificados X. 509 versión 3.

X.509 es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (organización internacional de las Naciones Unidas para coordinación de servicios de redes de telecomunicaciones entre Gobiernos y empresas) para las Infraestructuras de Clave Pública y los Certificados digitales.

7.1.2. Extensiones del certificado

Las extensiones de los certificados de la AC Raíz y AC Subordinada permiten codificar información adicional en los certificados.

Las extensiones estándar X.509 definen los siguientes campos:

- SubjectKeyIdentifier
- AuthorityKeyIdentifier
- BasicConstraints. Marcada como crítica
- Certificate Policies. Marcada como crítica
- KeyUsage. Marcada como crítica
- CRLDistributionPoint. Marcada como crítica
- SubjectAlternativeName. Marcada como crítica
- AuthorityInformationAccess

Los siguientes son los campos de los certificados que se emiten a los suscriptores:

- Fecha y hora de firmado
- Nombre del documento
- Asunto
- Entidad Certificadora
- Serial del Certificado
- Thumbprint
- Certificado válido desde
- Certificado válido hasta

7.1.3. identificadores de objeto (OID) de los algoritmos

Los OID de los algoritmos criptográficos utilizados por la AC Raíz son:

- md5withRSAEncryption (1.2.840.113549.1.1.4)
- SHA1withRSAEncryption (1.2.840.113549.1.1.5)
- SHA256withRSAEncryption (1.2.840.113549.1.1.11)

7.1.4. Formatos de nombres

El certificado de la AC Raíz contiene como DN, en formato X. 500, los nombres del emisor y titular del certificado en los campos emisor (issuer) y sujeto (subject).

7.1.5. Restricciones de los nombres

Los nombres contenidos en las firmas electrónicas están restringidas a distinguished names X.500, únicos y no ambiguos.

7.1.6. Identificador de objeto (OID) de la política de certificación

La AC raíz tiene definida una política de asignación de OID's dentro de su árbol privado de numeración. El OID de las PC de la ACs raíz es: 2.16.862.1.

7.2. Perfil de la CRL

7.2.1. Número de versión

La AC Subordinada, emite las CRLs con formato X. 509 v. 2.

7.2.2. Extensiones de las CRL

Las extensiones de las LRAC emitidas por la AC Raíz, son las definidas por el IETF en su RFC 2459, es decir:

- Authority Key Identifier
- CRL Number
- Issuing Distribution Point

7.3. Servicio de protocolo en línea de estado de certificados OCSP para comprobación de validez de firmas electrónicas emitidos a suscriptores.

7.3.1. Especificación

El estado de validez de una firma electrónica en particular emitido a un suscriptor podrá ser verificado mediante la consulta de lista de certificados revocados (.crl) o mediante el uso del protocolo en línea de estado de los certificados OCSP, el cual se encuentra implementado acorde a lo establecido en el RFC 2560.

7.3.2. Versión

Se utiliza la versión 1 del protocolo OCSP, según lo establecido en el RFC 2560.

7.3.3. Prestación del servicio por parte de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e S.A. y Extensiones

- CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e dispondrá del servicio de validación en el url **<http://ocsp.Certicámara.com>**
- El protocolo OCSP provisto por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e soporta las extensiones estándar establecidas por el RFC2459 y no presenta uso de extensiones personalizadas.

Copia No Controlada

8. Auditoria de conformidad

8.1. Frecuencia de los controles de conformidad para cada entidad

El sistema de acreditación de la AC raíz y AC Subordinada se someterá a una auditoria interna de forma anual, de acuerdo con el programa de Auditorias elaborado por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e. De esta manera se garantiza la adecuación de su funcionamiento y operatividad con las estipulaciones incluidas en esta ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01.

Adicionalmente CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e llevará acabo auditorias internas bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de las claves.

Cada año se llevará a cabo una autoría externa para evaluar el grado de conformidad con los criterios Webtrust para Autoridades de Certificación de AICPA/CICA.

8.2. Auditores

El auditor será seleccionado en el momento de la realización de cada auditoria.

Cualquier empresa o persona contratada para realizar una auditoria de seguridad sobre AC raíz o las ENTIDADES SUBORDINADAS deberá cumplir con los siguientes requisitos:

- Adecuada y acreditada capacitación y experiencia en PKI, seguridad y procesos de auditoria de sistemas de información.
- Independencia a nivel organizativo de la autoridad de AC raíz, para el caso de auditorias externas.

8.3. Relación entre el auditor y la entidad auditada

La relación entre el auditor y la entidad auditada se limitará estrictamente a los procesos e información requerida para la auditoria. Por lo tanto la parte auditada (AC raíz o la ENTIDAD SUBORDINADA) no deberá tener ninguna relación, actual o planificada, financiera, legal, o de cualquier otra clase que pueda derivar en un conflicto de intereses con el auditor. En el caso de los auditores internos, estos no podrán tener relación funcional con el área objeto de la auditoria.

8.4. Tópicos cubiertos por el control de conformidad

Son objeto de auditoria todos los requisitos técnicos, funcionales y organizativos entre ellos:

- La ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 utilizada.
- Política de Seguridad de la Información.
- Administración de la AC Raíz y AC Subordinada
- Consideraciones de Confidencialidad.
- Seguridad Física.
- Modelo de Respaldo.
- Plan de Continuidad del negocio.

- Personal Operativo.

8.5. Acciones a tomar como resultado de una deficiencia

La identificación de cualquier anomalía en la auditoria dará lugar a la corrección inmediata de medidas correctivas para ser solventadas en el menor tiempo posible.

En el caso de una deficiencia grave, CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e podrá determinar la suspensión temporal de las operaciones de la AC raíz o de la AC Subordinada hasta que las deficiencias se corrijan, la revocación de la firma electrónica de la entidad, cambios en el personal, etc.

8.6. Comunicación del resultado

El auditor comunicará los resultados de la auditoria al Gerente de Firma-e de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e y a los responsables de las distintas áreas en las que se detecten no conformidades.

8.7. Último informe de auditoria

En cumplimiento con lo señalado en el numeral 8.3 del capítulo V de la Circular única Número 10 de la Superintendencia de Industria y Comercio, la empresa (**Auditora**), realizó auditoria a **CERTICÁMARA S.A.** como entidad de certificación abierta, por el período comprendido entre el 1 de abril de 2010 al 31 de marzo de 2011. Se realizó examen de conformidad con los criterios **Webtrust** para Autoridades de Certificación de **AICPA/CICA**.

Usted puede consultar el texto del informe de auditoria en:
<https://cert.webtrust.org/SealFile?seal=750&file=pdf>

9. Firmas Electrónicas que emite CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e

Buscando satisfacer las diferentes necesidades que surgen en el contexto del uso creciente de las tecnologías de la información y Comunicaciones, **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** emite diversos tipos de **firmas electrónicas**.

A) FIRMA ELECTRÓNICA PARA REPRESENTANTE LEGAL PARA ENTIDAD PRIVADA:

Se emite a personas individuales nacionales o extranjeras que se han identificado plenamente ante CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Guatemala, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero, vinculándolas con la calidad de representante legal de una persona jurídica.

La **Firma Electrónica para Representante Legal para Entidad Privada** certifican la identidad de una persona individual vinculándola con la representación legal de una persona jurídica, o como comerciante persona individual en el ámbito de su actividad profesional o mercantil.

La **Firma Electrónica para Representante Legal para Entidad Privada** tienen como **suscriptor** tanto a la persona individual que actúa en nombre y representación legal de una persona jurídica, como a la persona jurídica representada que figura igualmente en el **certificado digital o firma electrónica avanzada**.

**REQUISITO PARA SU EMISIÓN:
FIRMA ELECTRÓNICA PARA REPRESENTANTE LEGAL PARA ENTIDAD PRIVADA**

Completar el Formulario de Solicitud de Certificado Digital en el Sistema de Solicitud de Productos y Servicios -SSPS- en la página web: <http://www.firma-e.com.gt> .

Documentos a Presentar:

- Formulario de Solicitud de Certificado Digital impreso y firmado por el Solicitante.
- Orden de Pedido impresa y firmada por el Solicitante.

Fotocopia Legalizada por Notario de los siguientes documentos:

- Cédula de Vecindad o Documento Personal de Identificación DPI
- Nombramiento de Representante Legal
- Patente de Comercio y Sociedad en su caso
- Documento Constitutivo de Entidad

Adicionalmente deberá presentar los siguientes documentos originales:

- Constancia de Inscripción en el Registro Tributario Unificado (RTU) del representante legal de la Entidad.
- Certificación de Inscripción de Empresa Extendida por el Registro Mercantil (Aplica a Empresas Mercantiles y Sociedades).
- Certificación Extendida por el Registro de Personas Jurídicas del Ministerio de Gobernación (Aplica a ONG's, Asociaciones Civiles no lucrativas, Fundaciones, Iglesias y Entidades Extranjeras).
- *Documento de Pago de Certificado*

B) FIRMA ELECTRÓNICA RELACIÓN CON ENTIDAD

Se emite a personas individuales nacionales o extranjeras que se han identificado plenamente ante CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Guatemala, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero, y permite identificarla como persona individual vinculándola como perteneciente a una determinada organización empresarial, ONG's, Asociaciones Civiles no lucrativas, Fundaciones, Iglesias y Entidades Extranjeras pero sin que tenga la representación legal de la misma o facultad de comprometerla jurídicamente.

Los **suscriptores** de este tipo de **certificados digitales** son: 1) La persona individual que logre acreditar suficientemente, a juicio de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, que existe una relación jurídica, laboral o de cualquier otra índole, con la persona jurídica que vaya a aparecer en el **certificado digital o firma electrónica avanzada**. 2) La persona jurídica que figura en el **certificado digital o firma electrónica avanzada**.

REQUISITOS DE EMISIÓN FIRMA ELECTRÓNICA RELACIÓN CON ENTIDAD

Completar el Formulario de Solicitud de Certificado Digital en el Sistema de Solicitud de Productos y Servicios -SSPS- en la página web: <http://www.firma-e.com.gt>

Documentos a Presentar:

- Formulario de Solicitud de Certificado Digital impreso y firmado por el Solicitante.
- Orden de Pedido impresa y firmada por el Solicitante.

Fotocopia Legalizada por Notario de los siguientes documentos:

- Cédula de Vecindad o Documento Personal de Identificación (DPI)
- Patente de Comercio y Sociedad en su Caso (Sí Aplica).

Adicionalmente deberá presentar los siguientes documentos originales:

- Constancia de Inscripción en el Registro Tributario Unificado (RTU) del solicitante.
- Certificación de Inscripción de Empresa Extendida por el Registro Mercantil (Aplica a Empresas Mercantiles y Sociedades).
- Certificación Extendida por el Registro de Personas Jurídicas del Ministerio de Gobernación (Aplica a ONG's, Asociaciones Civiles no lucrativas, Fundaciones, Iglesias y Entidades Extranjeras).

Documentación Laboral:

- Certificación de Relación Laboral firmada y sellada por la Máxima Autoridad de la Entidad, la cual especifique Nombre Completo, Documento de Identificación y Cargo que Desempeña el solicitante. (Aplica a entidades del estado, sujetas a la Ley de Servicio Civil).
- Certificación de Relación Laboral firmada y sellada por la Persona encargada de Administración de Recursos Humanos, la cual especifique Nombre Completo, Documento de Identificación y Cargo que Desempeña el solicitante. (Aplica a empresas privadas, ONG's, Asociaciones Civiles no lucrativas, Fundaciones, Iglesias y Entidades Extranjeras).
- Fotocopia Legalizada de Cédula de Vecindad o de Documento Personal de Identificación de la Persona Encargada de la Administración de Recursos Humanos ó

la Máxima Autoridad de la Entidad (según aplique).

- *Documento de Pago de Certificado*

C) FIRMA ELECTRÓNICA PARA PROFESIONAL TITULADO

Se emite a personas individuales nacionales o extranjeras que se han identificado plenamente ante CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Guatemala, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero identificándola como persona individual vinculándola a la obtención de un título profesional debidamente reconocido en la República de Guatemala o en un Estado Extranjero, y que hayan obtenido el correspondiente registro, licencia, colegiatura o tarjeta profesional requerida para el ejercicio de su profesión en la República de Guatemala o en un Estado Extranjero.

Los **suscriptores** de este tipo de **certificados digitales** son las personas individuales que logren acreditar suficientemente, a juicio de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, que ha obtenido un título profesional debidamente reconocido en la República de Guatemala o en un Estado Extranjero, y que han obtenido el correspondiente registro, licencia, colegiatura o tarjeta profesional requerido para el ejercicio de su profesión en la República de Guatemala o en un Estado Extranjero.

La **Firma Electrónica para Profesional Titulado** no garantiza la calidad, idoneidad del ejercicio profesional del suscriptor.

REQUISITOS DE EMISIÓN FIRMA ELECTRÓNICA PARA PROFESIONAL TITULADO

Completar el Formulario de Solicitud de Certificado Digital en el Sistema de Solicitud de Productos y Servicios -SSPS- en la página web: <http://www.firma-e.com.gt>

Documentos a Presentar:

- Formulario de Solicitud de Certificado Digital impreso y firmado por el Solicitante.
- Orden de Pedido Impresa y firmada por el Solicitante.
- Fotocopia tamaño oficio de ambos lados del Título Profesional.
- Constancia de Colegiado Activo con un plazo de vigencia mayor a un año.
- Constancia de Inscripción en el Registro Tributario Unificado (RTU) del solicitante.

Fotocopia Legalizada por Notario de los siguientes documentos:

- Cédula de Vecindad o Documento Personal de Identificación (DPI).

Documento de Pago de Certificado

La vigencia de la firma electrónica es de un año.

D) FIRMA ELECTRÓNICA PARA FUNCIONARIO PÚBLICO

Se emite a personas individuales nacionales o extranjeras que se han identificado plenamente ante Cámara de Comercio de Guatemala con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Guatemala, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero,

permitiendo identificarla como persona individual y vinculándola como funcionario público perteneciente a una entidad del Estado en la República de Guatemala.

Los **suscriptores** de este tipo de **certificados digitales** son las personas individuales que logren acreditar suficientemente, a juicio de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, que han obtenido el nombramiento o son titulares legales del cargo de notario, cónsul, juez de la república, magistrado, registrador o servidor público en la República de Guatemala y que se encuentran en ejercicio del mismo.

La **Firma Electrónica para Funcionario Público** no garantiza la calidad, idoneidad o cumplimiento efectivo de las funciones a cargo de su titular. **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no garantiza que el suscriptor del certificado de la **Firma Electrónica para Funcionario Público** haya sido sujeto de sanciones disciplinarias, administrativas, penales o de cualquier otra clase en la República de Guatemala o en el exterior. Para la emisión de la **Firma Electrónica para Funcionario Público** CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e se basa en la documentación exhibida y las declaraciones efectuadas por el suscriptor. Mientras la ley o las normas aplicables no establezcan lo contrario, la solicitud de **Emisión la Firma Electrónica para Funcionario Público** no es obligatoria para los Titulares de Función Pública. La emisión de la **Firma Electrónica para Funcionario Público** no limita al suscriptor para solicitar otros certificados digitales.

REQUISITOS PARA SU EMISIÓN FIRMA ELECTRÓNICA PARA FUNCIONARIO PÚBLICO

Completar el *Formulario de Solicitud de Certificado Digital en el Sistema de Solicitud de Productos y Servicios -SSPS-* en la página web: <http://www.firma-e.com.gt>

Documentos a Presentar:

- Formulario de Solicitud de Certificado Digital impreso y firmado por el Solicitante.
- Orden de Pedido impresa y firmada por el Solicitante.
- Constancia de Inscripción en el Registro Tributario Unificado (RTU) del solicitante.

Fotocopia Legalizada por Notario de los siguientes documentos:

- Cédula de Vecindad o, Documento Personal de Identificación del Solicitante
- Certificación de Nombramiento emitido por la Oficina Nacional de Servicio Civil (ONSEC) o de la Oficina de Personal que corresponda en aquellos casos en que cuenten con un régimen propio de administración de personal.
- *Documento de Pago de Certificado*

E) FIRMA ELECTRÓNICA PARA PERSONA INDIVIDUAL

Se emite a personas individuales nacionales o extranjeras que se han identificado plenamente ante CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Guatemala, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero.

La Firma Electrónica para Persona Individual tienen como **suscriptor** a la persona individual que actuando en nombre propio logre acreditar suficientemente, a juicio de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, su identidad a través de la exhibición de la documentación que así lo acredite

**REQUISITOS PARA SU EMISIÓN
FIRMA ELECTRÓNICA PARA PERSONA INDIVIDUAL**

Completar el Formulario de Solicitud de Certificado Digital en el Sistema de Solicitud de Productos y Servicios -SSPS- en la página web: <http://www.firma-e.com.gt>

Documentos a Presentar:

- Formulario de Solicitud de Certificado Digital impreso y firmado por el Solicitante.
- Orden de Pedido impresa y firmada por el Solicitante.
- Constancia de Inscripción en el Registro Tributario Unificado (RTU) del solicitante.

Fotocopia Legalizada por Notario de los siguientes documentos:

- Cédula de Vecindad o Documento Personal de Identificación
- *Documento de Pago de Certificado*

F) FIRMA ELECTRÓNICA PARA PERSONA JURIDICA

El Certificado de **Firma Electrónica para Persona Jurídica** (Entidad – Empresa) es un tipo de Certificado digital o firma electrónica avanzada que identifica a una persona jurídica de derecho público o privado, entidad del Estado o persona jurídica comerciante inscrito en el registro mercantil de la República de Guatemala, quien tiene el derecho de uso de un determinado sistema de información que será programado para firmar de manera automatizada o manual a nombre de esa persona jurídica. Así mismo, tendrá la calidad de suscriptor la persona individual que actúa como representante legal de la persona jurídica.

Garantizando el cumplimiento de las siguientes condiciones en conjunto y simultáneamente:

- Que una persona jurídica determinada se ha identificado como tal y ha solicitado el servicio a través de su representante legal, y
- Que esa persona jurídica podrá programar un sistema de información para que firme digitalmente mensajes de datos, de manera masiva o individual a través de medios electrónicos, vinculándose jurídicamente.

De conformidad con la normatividad vigente y aplicable para este caso, el Certificado de **Firma Electrónica Persona Jurídica** (Entidad – Empresa), emitidos por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e contempla las siguientes características:

- (i) Cumplimiento de los estándares fijados por el Registro de Prestadores de Servicio de Certificación -RPSC- del Ministerio de Economía;
- (ii) Cumplimiento de las condiciones relacionadas con la privacidad de la llave privada, pues no hay pérdida de unicidad de la firma; ni pérdida de control exclusivo, ya que el Usuario suscriptor se compromete – de conformidad con la presente ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 – a restringir el acceso a la llave privada;
- (iii) El control exclusivo se refiere a una persona, -puede ser por lo tanto individual o jurídica, de conformidad con la ley - y sí el Certificado de Firma Electrónica Persona Jurídica (Entidad – Empresa) está ubicado en la máquina de la entidad, se debe entender que la persona jurídica a quien se emite, es quien controla de manera exclusiva la firma;

(iv) Es en cualquier caso - desde la ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01 y desde la normativa guatemalteca vigente - responsabilidad del suscriptor custodiar las llaves;

Por lo anterior, un Certificado de **Firma Electrónica Persona Jurídica** (Entidad – Empresa) emitido por CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, deriva los atributos propios de la certificación digital: Autenticidad, Integridad y No repudio.

**REQUISITOS PARA SU EMISIÓN
FIRMA ELECTRÓNICA PARA PERSONA JURIDICA**

Completar el Formulario de Solicitud de Certificado Digital en el Sistema de Solicitud de Productos y Servicios -SSPS- en la página web: <http://www.firma-e.com.gt>

Documentos a Presentar:

- Formulario de Solicitud de Certificado Digital impreso y firmado por el Representante Legal de la entidad.
- Orden de Pedido impresa y firmada por el Representante Legal de la Entidad.

Fotocopia Legalizada por Notario de los siguientes documentos:

- Cédula de Vecindad o Documento Personal de Identificación (DPI) del Representante Legal
- Nombramiento del Representante Legal con la debida razón de inscripción del Registro de Personas Jurídicas del Ministerio de Gobernación (Presentar original y verificar que esté vigente). (Sí Aplica)
- Patente de Comercio Original (Sí Aplica)
- Patente de Sociedad Original (Sí Aplica)

Adicionalmente deberá presentar los siguientes documentos originales:

- Constancia de Inscripción en el Registro Tributario Unificado (RTU) del solicitante.
- Constancia de Inscripción en el Registro Tributario Unificado (RTU) del Representante Legal
- Fotocopia de Estatutos o acuerdo Gubernativo (según corresponda a la institución)
- Fotocopia del primer testimonio de la escritura pública de constitución, debidamente registrada.
- Perfil de la empresa (Modelo)
- Fotocopia de un recibo por prestación de servicios, tales como agua potable, energía eléctrica, o teléfono, u otro servicio similar, del bien inmueble que ocupa la entidad.
- Acta de Constitución (Sí Aplica).
- *Documento de Pago de Certificado*

10. Tarifas

El valor que fija CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e para los certificados de firma electrónica se establece de acuerdo a las condiciones contractuales acordadas con los solicitantes del servicio de certificación digital y serán adecuadamente calculados y liquidados por el sistema de solicitud de productos y servicios que CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e publica en su sitio Web para uso de los solicitantes. En caso de no existir un acuerdo contractual vigente que establezca una condición de precio especial, el precio base de los certificados de firma

electrónica de Representante Legal de para Entidad Privada, Relación con Entidad, Funcionario Público, Profesional Titulado y Persona Individual será de Un Mil Trescientos Quetzales (Q.1300.00) y para Persona Jurídica será de Cuatro Mil Setecientos Quetzales (Q. 4700.00) por cada año de vigencia del servicio, dicho año de vigencia se pagara de forma anticipada anualmente a menos de que el solicitante establezca pagar más de una anualidad u otra vigencia anticipada.

En ese orden de ideas, CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e podrá emitir el certificado de firma electrónica con una vigencia original de hasta 3 años, que serán pagados en su renovación del servicio por el solicitante anualmente o de conformidad con lo que se convenga de manera particular. De no recibirse la confirmación del pago de la renovación del servicio, el certificado de firma electrónica será suspendido, y sí el solicitante no manifiesta interés de renovación futura en un tiempo no mayor a un mes, término en el cual CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, comprobará el pago efectivo, se procederá a revocación definitiva del certificado.

10.1. Políticas de Reembolso para Suscriptores:

Los suscriptores de firmas electrónicas podrán solicitar reembolso de dinero en los siguientes casos:

- **Cuando se realiza una consignación de dinero mayor a la establecida:** en este caso el área de Contabilidad de Cámara de Comercio realiza las validaciones necesarias para confirmar el pago adicional y efectuará el respectivo reembolso a la entidad o persona que haya realizado dicha solicitud.
- **Cuando se solicita una firma electrónica que no aplique para el suscriptor: la Gerencia de Firma-e** realiza verificación de las firmas electrónicas emitidas anteriormente para el solicitante y según el resultado de dicha revisión (se solicitó una firma que no necesita el cliente), autoriza al área de contabilidad para que se haga efectivo el reembolso.

11. Obligaciones de los Intervinientes

11.1. Obligaciones de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e tiene las siguientes obligaciones en la prestación de sus servicios:

- Implementar y mantener los sistemas de seguridad que resulten razonables en función del servicio prestado y en general la infraestructura necesaria para la prestación del servicio de Certificación Digital.
- Cumplir con la **Declaración de Prácticas de Certificación** (ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01) y con los acuerdos realizados con los **suscriptores**.
- Informar al **suscriptor** las características de la prestación del servicio, los límites de responsabilidad, y las obligaciones que asume como interviniente en el proceso de certificación digital. En particular **CÁMARA DE COMERCIO DE GUATEMALA a**

través de su instancia Firma-e deberá informar al **suscriptor** o terceras personas que lo soliciten, sobre el tiempo y recursos computacionales requeridos para validar la firma electrónica que se efectúa con los certificados de firma que emite a sus suscriptores.

- Comprobar directamente o a través de las **Entidades de Registro** debidamente acreditadas ante Cámara de Comercio de Guatemala, la información definida en esta **Declaración de Prácticas de Certificación** como verificable para la emisión de **firmas electrónicas**.
- Abstenerse de acceder o almacenar la clave privada del **suscriptor**.
- Conservar por sí mismo o por interpuesta persona la custodia del **soporte físico** de la **firma electrónica** hasta la entrega efectiva del mismo al **suscriptor (si aplica)**.
- Permitir y facilitar la realización de las auditorias por parte de Ministerio de Economía.
- Expedir **firmas electrónicas** de conformidad con lo establecido en la sección de procedimiento de emisión de **firmas electrónicas** de esta **Declaración de Prácticas de Certificación**, y las especificaciones acordadas por el **suscriptor** en el **contrato de suscripción**.
- Publicar las firmas electrónicas expedidas y llevar el **Registro de Firmas electrónicas**.
- Actualizar la información que tiene registrada en la solicitud de autorización ante el Ministerio de la Economía y toda aquella que esta entidad establezca.
- Informar al Ministerio de Economía la ocurrencia de cualquier evento establecido en la **Declaración de Prácticas de Certificación**, que comprometa la prestación del servicio.
- Mantener el control y confidencialidad de su clave privada y establecer las seguridades razonables para que no se divulgue o comprometa.
- Procurar diligentemente la prestación permanente e ininterrumpida de los servicios de certificación digital.
- Permitir el acceso de los **suscriptores**, de las **partes confiantes** y de terceros a esta **Declaración de Prácticas de Certificación** y al repositorio de la **Entidad de Certificación**.
- Actualizar la **Base de datos de certificados digitales revocados** en los términos establecidos en esta **Declaración de Prácticas de Certificación** y efectuar los avisos y publicaciones que se establezcan por ley en ésta.
- Revocar las **firmas electrónicas** que se requiera de conformidad con lo establecido en la sección 4.7 de esta **Declaración de Prácticas de Certificación**.
- Informar al **suscriptor**, **dentro de las 24 horas hábiles siguientes, la suspensión del servicio o revocación de su (s) firma (s) electrónica** de acuerdo a la normatividad vigente.
- Disponer de una línea telefónica de atención a **suscriptores** y terceros, que permita las consultas y la pronta solicitud de revocación de firmas electrónicas por los **suscriptores**.
- Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas electrónicas y **certificados digitales** emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración.
- Conservar física o electrónicamente la documentación que respalda las **firmas electrónicas** emitidas, por el término previsto en la ley para los papeles de los comerciantes y tomar las medidas necesarias para garantizar la integridad y la confidencialidad que le sean propias.
- Atender las peticiones, quejas y reclamos hechas por los **suscriptores**, de conformidad con lo establecido en esta **Declaración de Prácticas de Certificación**.

- Otorgar a la información suministrada por el **suscriptor** el tratamiento que se establece en la sección de **Manejo de la Información Personal** de esta **Declaración de Prácticas de Certificación**.
- Cumplir con las instrucciones que establezca El Ministerio de Economía a través de sus disposiciones en la Guía de Evaluación del Registro de Prestadores de Servicios de Certificación -RPSC- para la Firma Electrónica, en su versión vigente.
- Advertir, sobre las medidas de seguridad que deben observar los **suscriptores** de firmas electrónicas para la utilización de estos mecanismos.

De conformidad con la normatividad guatemalteca vigente, **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** cuenta con una línea telefónica que permite la atención de las peticiones, quejas y reclamos de los **suscriptores**, de las **partes confiantes** y de los terceros.

El cumplimiento de todas o parte de las obligaciones o procedimientos de emisión de **firmas electrónicas** o de la prestación en general del servicio de certificación digital podrá ser realizado en forma directa por **CÁMARA DE COMERCIO DE GUATEMALA** como Entidad de Registro o Autoridad de Registro, a través de su instancia Firma-e.

CÁMARA DE COMERCIO DE GUATEMALA A TRAVÉS DE SU INSTANCIA FIRMA-E NO TIENE OBLIGACIONES ADICIONALES A LAS PREVISTAS EN ESTE SECCIÓN, NI DEBERÁ ENTENDERSE QUE EXISTEN OBLIGACIONES IMPLÍCITAS ADICIONALES A LAS EXPRESAMENTE CONSAGRADAS EN ESTA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN.

11.2. Obligaciones del suscriptor

El **suscriptor** tiene las siguientes obligaciones frente a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** y terceras personas:

- Utilizar la clave privada y la **firma electrónica** emitida tan sólo para los fines establecidos y de acuerdo con los condicionamientos establecidos en el contrato celebrado con él de manera individual y en esta **Especificación Técnica Declaración de Prácticas de Certificación ET-FE-01**, así como en la **Especificación Técnica Políticas de Certificación ET-FE-02** así como en la **certificado digital o firma electrónica avanzada** entregada. Será responsabilidad del **suscriptor** el uso indebido que éste o terceros hagan del mismo.
- Utilizar la clave privada y la firma electrónica para firmar mensajes de datos, explicando a las partes confiantes bajo que calidad se esta firmando (ya sea como persona individual o como persona individual vinculada a una cualidad determinada al momento de la emisión del certificado digital o firma electrónica avanzada), siempre y cuando el sistema de información de la parte confiante no verifique la cualidad en la que este actuando el suscriptor. El mensaje de datos o documento electrónico que el suscriptor firma con su firma electrónica, será el que determinará el contexto de la calidad en la que firma el suscriptor, y si éste este utilizando o no la cualidad asociada a la firma electrónica (si aplica).
- Responder por la custodia de la clave privada y de su **soporte físico (si aplica)** evitando su pérdida, revelación, modificación o uso no autorizado. Especialmente, el **suscriptor** deberá abstenerse, sin importar la circunstancia, de anotar en el **soporte físico** de la **firma electrónica** el código de activación o las claves privadas, ni tampoco en cualquier otro documento que el **suscriptor** conserve o transporte consigo o con el **soporte físico**.

- Solicitar la revocación de la **firma electrónica** que le ha sido entregado cuando se cumpla alguno de los supuestos previstos para la revocación de las **firmas electrónicas**.
- Abstenerse en toda circunstancia de revelar la clave privada o el código de activación de la **firma electrónica** así como abstenerse de delegar su uso a terceras personas.
- Asegurarse de que toda la información contenida en la **firma electrónica** es cierta y notificar inmediatamente a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** en caso de que se haya incluido cualquier información incorrecta o inexacta o en caso de que por alguna circunstancia posterior la información de la **firma electrónica** no corresponda con la realidad. Asimismo, deberá comunicar de manera inmediata el cambio o variación que haya sufrido cualquiera de los datos que aportó para adquirir la **firma electrónica**, aunque éstos no estuvieran incluidos en la propia **firma electrónica**.
- Informar inmediatamente a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** acerca de cualquier situación que pueda afectar la confiabilidad del **certificado digital o firma electrónica avanzada**, e iniciar el procedimiento de revocación de la **firma electrónica** cuando sea necesario. Especialmente, deberá notificar de inmediato la pérdida, robo o falsificación del **soporte físico** y cualquier intento de realizar estos actos sobre el mismo, así como el conocimiento por otras personas del código de activación o de las claves privadas, solicitando la revocación de la **firma electrónica** de conformidad con el procedimiento que se establece en la **Declaración de Prácticas de Certificación**.
- Destruir el **soporte físico** cuando así lo exija **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, cuando haya sido sustituido por otro con los mismos fines o cuando termine el periodo del servicio adquirido de la **firma electrónica con CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**, siguiendo en todo caso las instrucciones de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**.
- Devolver el **soporte físico** de la **firma electrónica** cuando así lo exija **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**.
- Respetar los derechos de propiedad industrial e intelectual de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** y de terceras personas en la solicitud y en el uso de las **firmas electrónicas**. **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no incluirá información en la **firma electrónica** cuya inserción pueda constituir de alguna forma la violación de los derechos de propiedad intelectual o industrial de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** y de terceras personas.
- Cualquier otra que se derive de la ley, del contenido de esta **Declaración de Prácticas de Certificación** o de la **Práctica de Certificación**.
- Abstenerse de monitorear, alterar, realizar ingeniería reversa o interferir en cualquier otra forma la prestación de servicios de certificación digital.

EL SUScriptor PODRÁ UTILIZAR SU FIRMA ELECTRÓNICA PARA: (I) IDENTIFICARSE COMO PERSONA INDIVIDUAL, O (II) ASOCIAR SU IDENTIFICACION PERSONAL A UNA CUALIDAD ESPECIFICA VERIFICADA POR CÁMARA DE COMERCIO DE GUATEMALA A TRAVÉS DE SU INSTANCIA FIRMA-E AL MOMENTO DE EMISIÓN DE LA FIRMA ELECTRÓNICA (SI APLICA). LA UTILIZACIÓN DE LA FIRMA ELECTRÓNICA EN UNO U OTRO CASO DEPENDERÁ DIRECTAMENTE DEL CONTEXTO EN EL QUE SE ESTE UTILIZANDO LA MISMA Y DE SI EL SISTEMA DE INFORMACION DE LA PARTE CONFIANTE PUEDE O NO VERIFICAR LA IDENTIFICACIÓN DEL SUScriptor.

SERA EL DOCUMENTO ELECTRONICO O MENSAJE DE DATOS QUE EL SUScriptor FIRMA DIGITALMENTE, EL QUE OFRECERA EL CONTEXTO DENTRO DEL CUAL EL SUScriptor HACE USO DE LA FIRMA Y SI ESTE UTILIZA O NO LA CUALIDAD ASOCIADA AL CERTIFICADO DIGITAL O FIRMA ELECTRÓNICA AVANZADA.

EN CASO DE QUE EL SISTEMA DE INFORMACION DE LA PARTE CONFIANTE NO PUEDA VERIFICAR LA IDENTIFICACION DEL SUScriptor Y/O NO LO PUEDA ASOCIAR O VINCULAR CON UNA CALIDAD ESPECIFICA, SERÁ EXCLUSIVA RESPONSABILIDAD DEL SUScriptor INFORMAR A LA PARTE CONFIANTE EN QUE CALIDAD O CONDICION SE UTILIZA LA FIRMA ELECTRÓNICA.

11.3. Obligaciones de la parte confiante

El **Sistema de Certificación Digital** de **CÁMARA DE COMERCIO DE GUATEMALA** a través de su instancia **Firma-e** comprende la utilización de un conjunto de elementos integrados en torno a la prestación de un servicio tanto a los **suscriptores** como aquellos que utilizan y confían en los **certificados digitales** emitidos por **CÁMARA DE COMERCIO DE GUATEMALA** a través de su instancia **Firma-e**. Cuando una tercera persona confía en una **firma electrónica**, está aceptando utilizar dicho sistema en su integridad y por tanto acepta regirse por las normas establecidas para el mismo, las cuales se encuentran contenidas esencial pero no exclusivamente en esta **Declaración de Prácticas de Certificación**. Esa tercera persona se convierte en un interviniente del **Sistema de Certificación Digital**, en calidad de **parte confiante**, y por ello asume las obligaciones que se establecen a continuación:

- Verificar la confiabilidad de la firma electrónica y del **certificado digital o firma electrónica avanzada**, revisando especialmente que éste no se encuentre en la **base de datos de certificados digitales revocados** de **CÁMARA DE COMERCIO DE GUATEMALA** a través de su instancia **Firma-e** disponible en el sitio de Internet de **CÁMARA DE COMERCIO DE GUATEMALA** a través de su instancia **Firma-e** o en las oficinas de la misma. La confiabilidad de la firma electrónica y del **certificado digital o firma electrónica avanzada** deberá en todo caso ceñirse a lo establecido en la sección de Confiabilidad de las firmas y los **certificados digitales**.
- Aceptar y reconocer a las **firmas electrónicas** solamente el uso que se permite darles de conformidad con lo establecido en la sección de Uso de los certificados digitales.
- Conocer con detenimiento y cumplir en todo momento con la **Declaración de Prácticas de Certificación** en la utilización de las firmas digitales y los **certificados digitales** de **CÁMARA DE COMERCIO DE GUATEMALA** a través de su instancia **Firma-e**. En especial la **parte confiante** deberá tener presente y actuar en todo momento de acuerdo a las limitaciones de responsabilidad y garantías que ofrece **CÁMARA DE COMERCIO DE GUATEMALA** a través de su instancia **Firma-e**.
- Informar a **CÁMARA DE COMERCIO DE GUATEMALA** a través de su instancia **Firma-e** de cualquier irregularidad o sospecha de la misma que se presente en la utilización del **Sistema de Certificación Digital**.
- Abstenerse de monitorear, alterar, realizar ingeniería reversa o interferir en cualquier otra forma la prestación de servicios de certificación digital.

11.3.1. Confiabilidad de las firmas electrónicas y los certificados digitales.

El **Sistema de Certificación Digital** de **CÁMARA DE COMERCIO DE GUATEMALA** a través de **su instancia Firma-e** es un sistema construido con base en el cumplimiento estricto de sus políticas y procedimientos. La confianza que genera en sus intervinientes depende en forma directa del cumplimiento de los mismos. Todos los intervinientes deberán prestar toda la colaboración a su alcance para la generación de la confianza propia del **sistema de certificación digital**, siguiendo en todo momento las políticas y procedimientos establecidos.

11.3.1.1. **Confiabilidad de las firmas electrónicas**

La **parte confiante**, antes de poder confiar en una firma electrónica certificada por **CÁMARA DE COMERCIO DE GUATEMALA** a través de **su instancia Firma-e**, tiene el deber de seguir estrictamente las indicaciones que se especifican a continuación:

1. La **parte confiante** debe determinar la confiabilidad del **certificado digital o firma electrónica avanzada**, conforme a lo estipulado en la sección siguiente.
2. La **parte confiante** debe verificar que la firma electrónica se haya creado dentro del periodo de vigencia del **certificado digital o firma electrónica avanzada** y que el mismo no se encuentra revocado.
3. La **parte confiante** deberá tener en cuenta todas las demás políticas y procedimientos que rigen la actividad de **CÁMARA DE COMERCIO DE GUATEMALA** a través de **su instancia Firma-e** y que se especifican en su **Declaración de Prácticas de Certificación**.

11.3.1.2. **Confiabilidad del certificado digital o firma electrónica avanzada que contiene una firma electrónica**

La **parte confiante** debe seguir las indicaciones que a continuación se enumeran si pretende confiar en un **certificado digital o firma electrónica avanzada** emitido por **Cámara de Comercio de Guatemala**:

1. La **parte confiante** debe verificar que el **certificado digital o firma electrónica avanzada** no haya expirado, de conformidad con la fecha de vigencia que figura en el mismo.
2. La **parte confiante** debe verificar que el **certificado digital o firma electrónica avanzada** no se encuentra en la **base de datos de certificados digitales revocados** de **CÁMARA DE COMERCIO DE GUATEMALA** a través de **su instancia Firma-e** que se encuentra publicada en el sitio de Internet de **CÁMARA DE COMERCIO DE GUATEMALA** a través de **su instancia Firma-e**. En todo caso, y sin ninguna excepción, está prohibido determinar el estado de revocación de una **firma electrónica** con base en información distinta a la de la **base de datos de certificados digitales revocados**.
3. La confiabilidad del **certificado digital o firma electrónica avanzada** depende de que el mismo se encuentre firmado digitalmente por **CÁMARA DE COMERCIO DE GUATEMALA** a través de **su instancia Firma-e**. La **parte confiante** puede verificar la firma electrónica de **CÁMARA DE COMERCIO DE GUATEMALA** a través de **su instancia Firma-e** verificándola con el certificado raíz, que contiene la clave pública de **CÁMARA DE COMERCIO DE GUATEMALA** a través de **su instancia Firma-e**, el cual se encuentra disponible en el sitio de Internet de **la CÁMARA DE COMERCIO DE GUATEMALA** a través de **su instancia Firma-e**.

El uso de una **firma electrónica** por cualquier interviniente en el **Sistema de Certificación Digital** está sujeto al seguimiento estricto de las normas contenidas en:

(i) El contrato celebrado con cada suscriptor del servicio de certificación digital, que contiene las condiciones generales de contratación de los servicios de certificación digital de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** cuyo clausulado se encuentra en el formulario de solicitud.

y (ii) La presente **Declaración de Prácticas de Certificación** con relación a las firmas digitales emitidas mediante sus **firmas electrónicas**. La **parte confiante** deberá tenerlas en cuenta siempre que pretenda confiar en una firma electrónica contenida en un certificado digital o firma electrónica avanzada.

12. Responsabilidad de los intervinientes

12.1. Responsabilidad de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e

Las obligaciones de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** enumeradas en la sección de obligaciones de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** son de medio y no de resultado. Ello significa que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** utilizará su conocimiento y experiencia en la prestación del servicio de certificación digital, y responderá profesionalmente por la culpa leve en sus actuaciones como Entidad prestadora de servicios de Certificación Digital. **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no puede garantizar que la actividad de certificación tenga un resultado determinado. **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** sólo responderá por aquellos errores que, ocurridos, hubieran podido evitarse por su diligencia profesional.

Los daños producidos o relacionados con la no ejecución o ejecución defectuosa de las obligaciones a cargo del **suscriptor**, de la **parte confiante** o de ambos, correrán por cuenta de éstos, así como todo perjuicio que se ocasione por el uso indebido de las **firmas electrónicas** o las violaciones a sus limitaciones de uso establecidas en el mismo, en la sección de Uso de los certificados digitales que contienen las firmas electrónicas, Especificación Técnica Políticas de Certificación ET-FE-02 o en cualquier otro documento que regule el **Sistema de Certificación Digital**.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e no responderá por los perjuicios ocasionados por el incumplimiento de sus obligaciones por casos de fuerza mayor, caso fortuito o, en general, cualquier circunstancia sobre la que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no pueda tener un control razonable, incluyendo pero sin limitarse a los siguientes: los desastres naturales, las alteraciones de orden público, el corte de suministro eléctrico y/o telefónico, los virus informáticos, las deficiencias en los servicios de telecomunicaciones (Internet, canales de comunicación, etc.) o el compromiso de las claves asimétricas derivado del riesgo tecnológico imprevisible.

Independientemente de la causa u origen de su responsabilidad, **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** fija como cuantía máxima para la indemnización de perjuicios por los daños ocasionados por **certificado digital o firma electrónica avanzada** emitido, la suma de US\$ 200,000.00. En consecuencia, **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** solo indemnizará hasta este valor a las personas perjudicadas por una **firma electrónica** emitida por ésta, independientemente del número de

veces que el mismo se haya utilizado o del número de perjudicados por dichos usos. En caso de que existan varios perjudicados, el monto máximo indemnizable se distribuirá a prorrata entre ellos. Si habiéndose distribuido la indemnización, surgieren nuevos perjudicados, estos deberán dirigirse contra las personas ya indemnizadas para efectos de obtener a prorrata su indemnización.

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e solo responderá por los perjuicios que se ocasionen por la utilización de los servicios de certificación digital dentro del año siguiente a la expiración o revocación de la **firma electrónica**. **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no ofrece ningún tipo de garantía que no esté expresamente estipulada en esta **Declaración de Prácticas de Certificación**, ni responderá por evento que no esté expresamente contemplado en este inciso.

En caso que las leyes aplicables al servicio de certificación digital establezcan la imposibilidad de limitar la responsabilidad en alguno de los aspectos aquí descritos o que se describen en esta **Declaración de Prácticas de Certificación**, se dará a estas cláusulas el mayor alcance que la ley permita darles en cuanto a la limitación de la responsabilidad de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**.

12.2. Responsabilidad del Suscriptor

De conformidad con lo establecido en la ley, el **suscriptor** será responsable y se compromete a indemnizar a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** y a las **partes confiantes** los daños y perjuicios que se ocasionen o puedan ocasionarse por el incumplimiento de cualquiera de sus obligaciones, asumiendo igualmente los gastos judiciales en que **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** pudiera incurrir por esta causa, incluyendo los costos de abogados.

La custodia del **soporte físico** (tarjeta inteligente, token, disco duro, diskette u otro suministrado o no por **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e**) del **certificado digital o firma electrónica avanzada que contiene la firma electrónica** es responsabilidad exclusiva del **suscriptor**.

El **suscriptor** será el único responsable frente a las **partes confiantes** y a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** por todos los perjuicios que se ocasionen por la falsedad inexactitud o insuficiencia de la información que entregue a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** o a la **Parte Confiante**, independientemente de la causa por la cual haya entregado dicha información falsa, inexacta o insuficiente. El **suscriptor** asumirá los perjuicios que sufra como consecuencia de eventos de caso fortuito o fuerza mayor.

En caso de que el sistema de información de la parte confiante no realice la verificación de manera automática, será exclusiva responsabilidad del suscriptor informar a la parte confiante sobre la condición o calidad en la que se está utilizando el certificado digital o firma electrónica avanzada, y por lo tanto **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** no tendrá frente a la parte confiante, ni frente a terceros deber alguno de información sobre la condición o calidad en la que el respectivo suscriptor está utilizando el certificado digital o firma electrónica avanzada, pues ella deriva directamente del contexto en el que este actuando éste.

El **suscriptor** es el único responsable por las obligaciones que emanen de las operaciones o negocios jurídicos que se realicen con los **certificados digitales**, exonerando a **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** de toda responsabilidad por este concepto.

12.3. Responsabilidad de la parte confiante

En todo caso, la **parte confiante** asumirá toda la responsabilidad y riesgos derivados de la aceptación de una **firma electrónica** sin haber realizado previamente la verificación de su confiabilidad, o sin haber seguido los procedimientos establecidos en esta **Declaración de Prácticas de Certificación**, garantizando la plena indemnidad de **CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e** por dicho concepto. La **parte confiante** asumirá los perjuicios que sufra como consecuencia de eventos de caso fortuito o fuerza mayor.

13. Garantías que ofrece CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e para el cumplimiento de sus obligaciones

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, ha suscrito una póliza de seguro con una entidad aseguradora autorizada de acuerdo con la legislación guatemalteca, que ampara los perjuicios contractuales y extracontractuales de los suscriptores y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e en el desarrollo de sus actividades.

14. Política de confidencialidad

La AC Raíz y AC Subordinada, se compromete a proteger todos los datos a los que tenga acceso como consecuencia de su actividad como entidad de certificación.

No obstante, AC Raíz y AC Subordinada se reserva el derecho a revelar a los empleados y consultores, externos o internos, los datos confidenciales necesarios para realizar sus actividades como AC Raíz y AC Subordinada. En este caso los empleados y/o consultores son informados sobre las obligaciones de confidencialidad.

Estas obligaciones no se aplican si la información calificada como “confidencial” es requerida por los Tribunales u órganos administrativos competentes o impuesta por una ley Guatemalteca.

14.1. Información confidencial

Se considera información confidencial:

- Información de registro, todos los datos relativos al registro de firmas electrónicas son considerados confidenciales.
- La información de negocio suministrada por sus proveedores y otras personas con las que Cámara de Comercio tiene el deber de guardar secreto establecida legal o convencionalmente.
- Información sobre la vida de los certificados, todos los datos relativos a la emisión y revocación (salvo su publicación en la CRL) de certificados de la ENTIDAD SUBORDINADA.
- Toda la información clasificada como “Confidencial”.

14.2. Información no confidencial

Se considera información no confidencial:

- Contenido de las firmas electrónicas
- Lista de Certificados Revocados (CRL)
- La clave pública de la AC Raíz y AC Subordinada
- Las versiones de la ESPECIFICACIÓN TÉCNICA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN ET-FE-01

15. Sedes

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e cuenta con sede el la ciudad de Guatemala - Guatemala

Guatemala

Dirección: 10 ma. Calle 3-80 Zona 1
Teléfonos: 2417 2700
Fax: 2220 9393
Correo Electrónico: info@firma-e.com.gt

16. Peticiones, quejas y reclamos

Si Usted o cualquier persona tiene alguna petición, queja o reclamo frente a cualquiera de los servicios o actividades de CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, puede dirigirse a cualquiera de nuestras Entidades de Registro e informar que desea hacer una petición, queja o reclamo, o comunicarse con la persona a cargo de la absolución de los mismos:

Dirección: 10 ma. Calle 3-80 Zona 1
Teléfonos: 2417 2700 Ext.803
Fax: 2220 9393
Dirección de correo electrónico: servicioalcliente@firma-e.com.gt
Responsable: Coordinador de Servicio al Cliente

CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e brinda soporte técnico a través de

Línea Nacional: 2417 2700 Ext.732

La página www.firma-e.com.gt brinda:

- Manuales de Instalación
- Soporte técnico en línea
- Soporte técnico vía correo electrónico info@firma-e.com.gt
- Preguntas frecuentes

17. Procedimientos de resolución de Conflictos.

Todas las diferencias que se presenten entre las partes con ocasión de la celebración del contrato, durante su ejecución o por su interpretación, serán resueltas de manera amigable entre el Titular de la Firma Electrónica y CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e, si transcurridos quince (15) días, a partir de la primera reclamación no se ha llegado a ningún acuerdo, la diferencia se someterá al PROCEDIMIENTO PARA LA RESOLUCIÓN DE CONFLICTOS PR-FE-05 con el Método Alternativo de Solución de Conflictos de Conciliación, en

el Centro de Arbitraje y Conciliación designado por la CÁMARA DE COMERCIO DE GUATEMALA a través de su instancia Firma-e en dicho procedimiento, de acuerdo con las normas establecidas por este.

18. DEFINICIONES:

- **CA:** Autoridad de Certificación. Sigla usada normalmente para referirse a la Autoridad de Certificación. En la presente DPC ejercerá como Autoridad de Certificación CERTICAMARA.
- **CRL:** Sigla en inglés usada normalmente para referirse a la Lista de Certificados Revocados, o Certificate Revocation List.
- **DPC. DECLARACION DE PRACTICAS DE CERTIFICACION:** Documento que comprende y por el que se dan a conocer las políticas y procedimientos generales del servicio de certificación digital.
- **OID:** Definición de los diferentes campos del certificado digital, de conformidad con las prácticas de certificación que se encuentren asociadas al servicio y éstas serán definidas por la Cámara de Comercio de Guatemala bajo la asesoría de Certicámara.
- **PKI: Infraestructura de Llave Pública** (en inglés, PKI, *Public Key Infrastructure*) aplicada a la criptografía es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas para la firma electrónica como la Integridad, Autenticidad, No repudio y Confidencialidad.
- **RA:** Término correspondiente a Autoridad de Registro que dentro del Sistema de Certificación Digital aplicado a una infraestructura de clave pública, es una entidad de confianza que:
 - Registra solicitudes de personas individuales o jurídicas para obtener una firma electrónica.
 - Comprueba la veracidad de los datos que aportan los solicitantes.
 - Remite solicitudes a una CA o Autoridad de Certificación para su proceso.
 - La función de la Autoridad de Registro es controlar la generación de firmas electrónicas autorizada por la regulación Guatemalteca. Previa identificación, la Autoridad de Registro se encarga de realizar la petición del certificado y de guardar los datos correspondientes. En el presente contrato ejercerá como Autoridad de Registro Cámara de Comercio de Guatemala dentro de la República de Guatemala.
- **Revocación:** Procedimiento por medio del cual la **firma electrónica** deja de tener eficacia jurídica.
- **Token:** soporte físico la firma electrónica que a través de un conector USB con tarjeta inteligente, permite el almacenamiento de documentos digitales, los cuales se resguardan mediante un proceso de autenticación, que incluye contraseña y encriptación. Este dispositivo puede ser sustituido por una smart card que cumpla con los requisitos técnicos
- definidos en la Guía de Evaluación del registro de Prestadores de Servicios de Certificación de Firma Electrónica y en concordancia con la Declaración de Prácticas de Certificación de E-Certguatemala.
- **V.P.N:** Virtual Private Network por sus siglas en Inglés (VPN), es una Red Privada Virtual que conecta los componentes de una red con otra red.

19. ANEXO

Anexo A:

CÓDIGO	NOMBRE
ET-FE-02	Especificación Técnica Políticas de Certificación
PR-FE-05	Procedimiento para la Resolución de Conflictos
PR-FE-09	Procedimiento para el cese de Actividades de Cámara de Comercio de Guatemala
PR-FE-15	Procedimiento de Seguridad de la Información

Anexo B: Control de cambios

FECHA	SECCIÓN AFECTADA	RAZON DEL CAMBIO	NO. DE REVISIÓN
25/07/2011	Todas	Se realizaron cambios en la estructura de este documento, entre ellos: se asignaron responsabilidades a la AC Raíz y AC Subordinada, ya que se cambio el Proveedor de Firma Electrónica.	1
25/07/2011	18	Se modificó la sección de Definiciones.	1
3/10/2011	9	Se adaptaron los requisitos según la ET-FE-04.	1

Copia No Controlada