Registro de Prestadores de Servicios de Certificación para la Firma Electrónica

Guía de Evaluación

Ministerio de Economía
GUATEMALA

Descriptor del Documento:	**GUA-RPSC-Guía de Evaluación**
Versión:	**1.2**
Estado :	**Final**
Fecha de Emisión:	**08/07/2009**
Contacto:	**mskarlette@mineco.gob.gt**

CONTENIDO

RESUMEN

Considerando que, entre otros, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónica, Decreto 47-2008 del Congreso de la República de Guatemala, tiene por objeto la promoción del comercio electrónico, la validación, fomento y estimulo de las operaciones efectuadas por medio de las nuevas tecnologías de la información, y especialmente el otorgamiento de seguridad jurídica y técnica a las contrataciones, comunicaciones y firmas electrónicas; este documento especifica los procedimientos de evaluación al que serán sometidos las entidades que soliciten su incorporación al Registro de Prestadores de Servicios de Certificación (RPSC), y complementa las regulaciones aplicables para este efecto, con el fin de establecer el nivel mínimo de confiabilidad que requiere el sistema global en su operación.

Dichas regulaciones se basan en criterios establecidos en estándares internacionales, homologados en la medida de lo posible por el organismo normalizador guatemalteco, COGUANOR, como una forma de generar compatibilidad con organizaciones equivalentes en otros países, y poner al alcance de la población en general documentos escritos en idioma español.

Esta Guía de Evaluación debe ser usada por las entidades que busquen su inscripción en el Registro de Prestadores de Servicios de Certificación para identificar los requisitos y estándares que deben cumplir sus procesos de negocios, políticas, recursos, procedimientos, tecnologías, etc.; para obtener la autorización que los habilite para emitir certificados de firma electrónica avanzada y prestar otros servicios que se amparen en el Decreto Número 47-2008.

En adelante, el documento se estructura en dos partes. La primera de ellas define los criterios para ingresar a una entidad al RPSC, define el procedimiento de evaluación de dichas entidades, y explica el tipo de evaluación que se llevará a cabo. La segunda parte del documento ahonda para cada uno de los requisitos identificados anteriormente, respecto del procedimiento de evaluación, los requerimientos que deben ser cumplidos por la entidad solicitante, y los aspectos específicos a evaluar. Finalmente este documento incluye un anexo con información bibliográfica.

PRIMERA PARTE

1 GENERALIDADES EN LA OPERACIÓN DEL SISTEMA

Son aplicables a la presente Guía de Evaluación todas las definiciones contenidas en la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala, y aquellos incluidos en su Reglamento.

Adicionalmente se deben considerar las siguientes definiciones y abreviaturas:

AC: Sigla usada normalmente para referirse a la Autoridad de Certificación.

AR: Sigla usada normalmente para referirse a la Autoridad de Registro.

CP: Sigla en inglés usada normalmente para referirse a la Política de Certificado (Certificate Policy).

CPS: Sigla en inglés usada normalmente para referirse a Declaración de Prácticas de Certificación (Certification Practice Statements).

CRL: Sigla en inglés usada normalmente para referirse a la Lista de Certificados Revocados, o Certificate Revocation List.

Entidad Autorizadora: Se refiere al Registro de Prestadores de Servicios de Certificación, adscrito al Ministerio de Economía

Guía de Evaluación o Guía: Denominación del presente documento, en el cual se indican los requisitos específicos que serán evaluados en una entidad prestadora de servicios de certificación que desee ser incluida en el registro de prestadores autorizados.

Ley: Se refiere a la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala.

PKI: Sigla en inglés usada normalmente para referirse a la Infraestructura de llave Pública (Public Key Infraestructure).

PSC: Sigla usada para referirse a un Prestador de Servicios de Certificación.

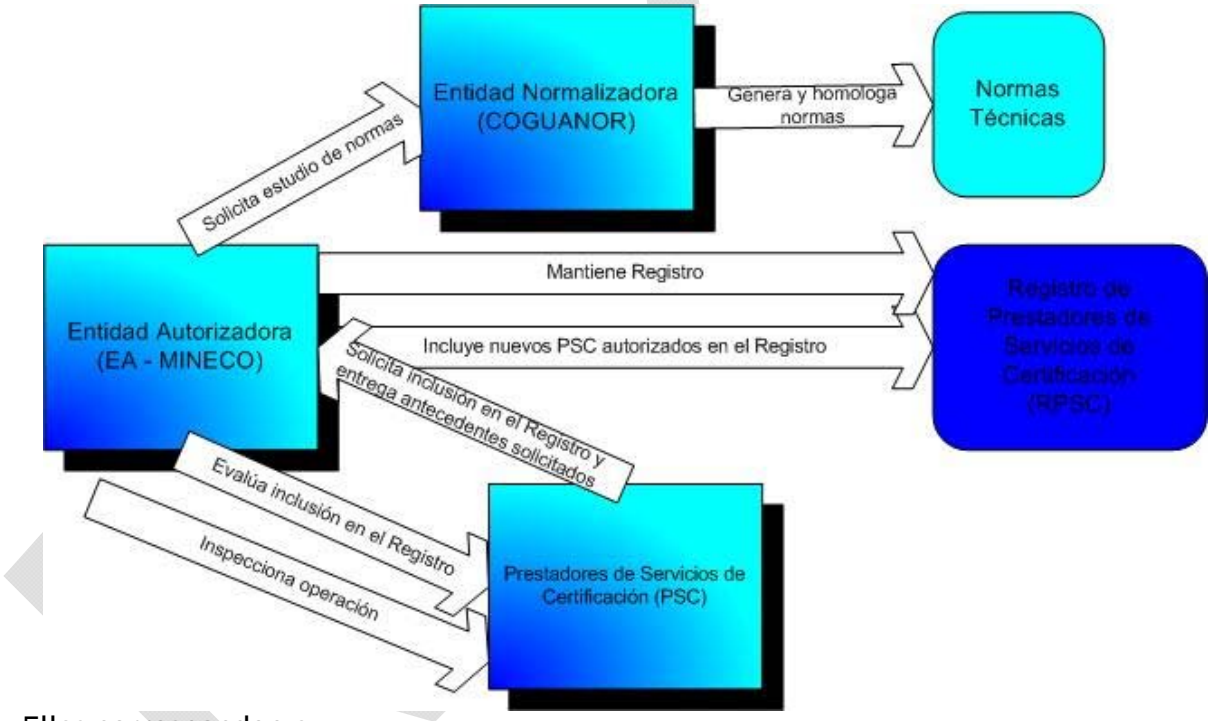
RPSC: El Registro de Prestadores de Servicios de Certificación.

Reglamento: Se refiere al Reglamente asociado a la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

TSA: Sigla en inglés usada normalmente para referirse a autoridades de sellado de tiempo o estampado cronológico (Time-Stamping Authorities).

1.1 Participantes del Sistema de Registro de Prestadores de Servicios de Certificación

La Ley y su Reglamento determinan un sistema de autorización de Prestadores de Servicios de Certificación que involucra a distintos participantes. En la siguiente figura se presenta el esquema general de interacción de las entidades que intervienen en el proceso.



Ellas corresponden a:

Entidad Autorizadora (EA) - Corresponde a la autoridad administrativa, o Registro de Prestadores de Servicios de Certificación adscrito al Ministerio de Economía (Art. 49 de la Ley), responsable del registro y autorización para operar de los prestadores de servicios de certificación.

Entidad de Normalización (EN) - A solicitud de la Entidad Autorizadora, la Comisión Guatemalteca de Normas (COGUANOR) actuará para la generación u homologación de normas, regulaciones, criterios o principios internacionales reconocidos (literal j del Art. 49 de la Ley), las que pasarán a ser parte del conjunto de normas técnicas vigentes aplicables en el contexto de la Ley, el Reglamento y sus regulaciones.

Prestadores de Servicios de Certificación (PSC) - Corresponde a la entidad prestadora de servicios de certificación que solicita ser ingresada al RPSC para actuar como un prestador autorizado.

Registro de Prestadores de Servicios de Certificación (RPSC) - Es un registro público que mantiene la Entidad Autorizadora, en el cual están identificados los PSC cuya operación cumple plenamente con los requisitos establecidos por la Ley, su Reglamento y sus regulaciones, incluyendo esta Guía.

Normas Técnicas (NT) - Es el conjunto de estándares vigentes en los cuales se basa la Entidad Autorizadora para realizar el procedimiento de evaluación.

1.2 Rol de Registro de Prestadores de Servicios de Certificación – RPSC - o Entidad Autorizadora

La autorización de las actividades de las entidades prestadoras de servicios de certificación será desarrollada por el Registro de Prestadores de Servicios de Certificación, quién se puede apoyar en funcionarios o peritos especialmente contratados y habilitados para realizar la evaluación de los PSC (Art. 26 del Reglamento). Debido a este rol que le corresponde cumplir, también se le llama Entidad Autorizadora.

La Entidad Autorizadora evaluará el cumplimiento de cada uno de los requisitos y obligaciones especificadas para los prestadores que quieren ser autorizados, sobre la base de la Ley, su Reglamento, y los estándares internacionalmente aceptados para dichos efectos, los cuales quedan establecidos en esta Guía de Evaluación, y en las Guías de Inspección Periódica.

No es parte de la función de la Entidad Autorizadora el recomendar o diseñar las medidas correctivas, o proponer los planes para subsanar el incumplimiento de requisitos por parte de los prestadores de servicios de certificación que busquen ser autorizados e incluidos en el Registro.

1.2.1 Criterios generales del Registro

Son criterios generales para la operación del Registro de Prestadores de Servicios de Certificación los siguientes:

A. **Transparencia -** El RPSC pondrá a disposición pública toda la información necesaria, requerida para conocer el estado del sistema de certificación de conformidad con las leyes de la República de Guatemala, con el propósito de proveer confianza a los usuarios y generar las condiciones y los acuerdos necesarios para el desarrollo de la actividad, en conformidad a las normas y acuerdos internacionales que se celebren.

B. **Interoperabilidad Internacional -** Los requerimientos del proceso de evaluación para otorgar o rechazar una solicitud de ingreso al registro deberán fomentar la compatibilidad del sistema nacional con los estándares internacionales, en la medida que ello sea posible, permitiendo así la interoperabilidad internacional del sistema.

C. **Gradualidad -** Los niveles de exigencia del proceso de evaluación serán graduales y se irán adaptando desde un estado inicial en el que las exigencias apuntarán a cumplir estándares suficientes que provean confianza en el sistema y compatibles con la realidad nacional, hasta el cumplimiento estricto de los estándares internacionales a medida que el desarrollo de la actividad lo requiera.

D. **Independencia -** Como una forma de asegurar la independencia de los entes reguladores, la Entidad Autorizadora, y los profesionales que para su efecto sean contratados, no podrán ser participes directos del proceso de generación de servicios de certificación ni tener vínculos contractuales de ningún tipo con dichas organizaciones.

E. **Neutralidad Tecnológica -** No existirá preferencia hacia una tecnología en particular.

F. **Privacidad -** Para la realización de un proceso de evaluación riguroso se requiere la entrega de información estratégica o altamente sensible de parte de las empresas que soliciten su inclusión en el registro. Por lo anterior, la Entidad Autorizadora se compromete a no usar ni divulgar la información entregada por el Prestador que sea clasificada explícitamente como confidencial, más que para los fines propios del procedimiento de autorización. Este compromiso se hace extensible a todo organismo y/o persona que intervenga en el proceso de autorización en nombre de la Entidad Autorizadora.

1.2.2 INCLUSIÓN DE UN PRESTADOR DE SERVICIOS DE CERTIFICACIÓN EN EL RPSC

Un Prestador de Servicios de Certificación será ingresado al RPSC en los siguientes casos:

A. Si cumple plenamente los requisitos establecidos, de acuerdo a los criterios de evaluación definidos en la Ley, su Reglamento, y esta Guía.

B. Cuando presentando incumplimientos, la Entidad Autorizadora los califique como subsanables y evalúe que no ponen en riesgo la seguridad global del sistema. En dicho caso, la Entidad Autorizadora deberá haber aprobado previamente el plan de medidas correctivas propuesto por el Prestador de

Servicios de Certificación, el cual le permitirá subsanar plenamente los incumplimientos en un plazo definido y considerado razonable.

No se otorgará la autorización al Prestador de Servicios de Certificación solicitante en el siguiente caso:

C. Cuando no cumple alguno de los requisitos definidos, poniendo en riesgo la seguridad global del sistema.

1.2.3 CUMPLIMIENTO DE REQUISITOS

El Prestador de Servicios de Certificación que solicite su ingreso al Registro de Prestadores de Servicios de Certificación deberá demostrar el cumplimiento de los requisitos mediante los siguientes medios:

A. Acompañando los antecedentes que exige la Ley, su Reglamento y esta Guía, al momento de presentar la solicitud de evaluación.

B. Presentando la documentación e información adicional solicitada por la Entidad Autorizadora, en la forma y dentro de los plazos establecidos por ella en cada caso.

C. Permitiendo el libre acceso a los expertos nombrados por la Entidad Autorizadora para la realización de inspecciones en terreno.

D. Entregando cualquier información adicional pertinente solicitada por la Entidad Autorizadora durante el proceso de evaluación.

Adicionalmente el Prestador de Servicios de Certificación podrá entregar, si lo desea, información adicional no solicitada que permita reforzar su postulación, la cual podrá ser del siguiente tipo:

E. Documentos descriptivos generados por el PSC que permitan apoyar la comprobación de un requisito.

F. En los casos que sea pertinente, y que la Entidad Autorizadora lo permita o solicite, mediante la presentación de una auditoría externa realizada por una empresa consultora independiente.

La presentación de uno o varios de estos medios de prueba dependerá del requisito en particular al que se esté haciendo alusión. La Entidad Autorizadora entregará guías y documentos modelo para orientar el cumplimiento de cada requisito.

1.2.4 PRELACIÓN DE REQUISITOS

En caso de que existan en esta Guía criterios de evaluación discrepantes o contrapuestos con los requerimientos que se establecen en la Ley, su Reglamento, o las normas técnicas aplicables, prevalecerán los primeros por sobre los siguientes.

En aquellos casos en que la norma técnica definida no especifique aspectos que deban ser evaluados, la Entidad Autorizadora podrá utilizar referencias o especificaciones que estén reconocidas por la industria. En los casos en que esto ocurra, se incorporará en la Guía de Evaluación la individualización del documento utilizado.

2 PROCEDIMIENTO DE EVALUACIÓN

La autorización es el resultado de un procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Entidad Autorizadora que cuenta con las instalaciones, sistemas, programas informáticos y recursos humanos necesarios para otorgar los certificados en los términos que se establecen en la Ley y su Reglamento, permitiendo su inscripción en el RPSC (Art. 23 del Reglamento).

A continuación se describe el procedimiento de evaluación.

2.1 PASO 1 – SOLICITUD

A. Para solicitar su inscripción en el RPSC, la entidad solicitante deberá presentar ante la Entidad Autorizadora una solicitud por escrito dirigida al Director Ejecutivo, individualizándose mediante los documentos indicados en el Requisito 1 Admisibilidad de esta Guía.

B. A dicha solicitud deberá ir acompañada por el comprobante de pago de los costos de la autorización (Art. 24 del Reglamento y su arancel).

C. Además se deberán incluir todos los documentos y antecedentes especificados en el Requisito 1 Admisibilidad, definido en el punto 3. Ellos incluyen documentos legales y comerciales, técnicos, de seguridad física, lógica y de la plataforma tecnológica utilizada, de la operación de la autoridad certificadora y de la(s) autoridad(es) de registro, de los tipos de certificados y servicios prestados, etc.

2.2 PASO 2 – VERIFICACIÓN DE ADMISIBILIDAD

A. Recibida la solicitud, la Entidad Autorizadora procederá a revisar y declarar la admisibilidad de la misma mediante la verificación de la completitud de los antecedentes requeridos, dentro de un plazo de cinco (5) días hábiles.

B. De ser inadmisible la solicitud, dentro del plazo indicado se procederá a comunicar al interesado tal situación y que podrá completar los antecedentes dentro del plazo de quince (15) días hábiles, bajo apercibimiento de ser rechazada la solicitud (Art. 24 del Reglamento).

2.3 PASO 3 – EVALUACIÓN DE LA AUTORIZACIÓN

A. Si la solicitud es declarada admisible será admitida a trámite. La Entidad Autorizadora procederá dentro del plazo de 90 días calendario a un examen sobre el cumplimiento de los requisitos y obligaciones exigidas por la Ley, su Reglamento y esta Guía de Evaluación, para determinar si autoriza o no la inscripción en el RPSC de la entidad solicitante. Dicho plazo será contado desde la fecha de declaración de admisibilidad de la solicitud, y podrá ser prorrogado por una vez, en igual período, y por motivos fundados.

   Para llevar a cabo esta tarea, el PSC solicitante deberá facilitar el acceso de los funcionarios o expertos que la Entidad Autorizadora designe para realizar las evaluaciones, además de proporcionar cualquier información adicional solicitada.

   La evaluación se llevará a cabo sobre criterios objetivos, y cada requisito podrá alcanzar las siguientes calificaciones.

Nota	Interpretación
C	Se asignará una calificación **C** a cada uno de los requisitos exigidos que el PSC **CUMPLE totalmente**.
S	Se asignará una calificación **S** a cada uno de los requisitos exigidos en que: • el PSC no cumple totalmente, • se determina un apego **SUFICIENTE** de requisito exigido, y • se evalúa que el incumplimiento es subsanable en tiempos razonables y no afecta el correcto funcionamiento del sistema ni los fines previstos en la Ley, su Reglamento y esta Guía.
I	Se asignará una calificación **I** a cada uno de los requisitos exigidos en que: • el PSC no cumple, • se determina un apego **INSUFICIENTE** del requisito exigido, y/o • se determina que no es subsanable en tiempos razonables, o afecta el correcto funcionamiento del sistema o los fines previstos en la Ley, su Reglamento y/o esta Guía.

B. Realizada la evaluación, la Entidad Autorizadora se pronunciará sobre el cumplimiento de los requisitos y obligaciones necesarias para ser un PSC autorizado. Dicha declaración será emitida cuando un PSC sea evaluado con una calificación **C** (CUMPLE) en cada uno de los requisitos evaluados. Una vez declarada la autorización, el interesado dispone de un plazo de treinta (30)

días calendario para presentar la póliza de seguros que exige el artículo 16 del Reglamento, bajo apercibimiento de ser rechazada la solicitud si no lo cumple.

C. Si la Entidad Autorizadora determina, como resultado de la evaluación de los antecedentes e inspecciones, que los incumplimientos que presenta el PSC solicitante son s**ubsanables en tiempos razona**bles, y no afectan el correcto funcionamiento del sistema ni los fines previstos en la Ley, su Re**g**lamento y esta Guía, esto es, que **exista al menos un requisito** que como resultado de la evaluación se califique con nota **S** (SUFICIENTE), procederá a comunicar al PSC por escrito de el o los requisitos incumplidos que se deben subsanar, y dará un plazo para entregar por escrito un plan de medidas correctivas.

   i. Una vez recibido el plan de medidas correctivas propuesto por el PSC, la Entidad Autorizadora procederá a evaluar su factibilidad, la solución propuesta, y los plazos para ello. En caso de no ser satisfactorio, la Entidad Autorizadora procederá a dictar una resolución en la que rechaza la solicitud de registro mencionando los requisitos que se consideran no subsanables mediante la propuesta entregada.
   ii. En caso de ser favorable la evaluación del plan de medidas correctivas, la Entidad Autorizadora procederá a informar al interesado que dispone de un plazo de treinta (30) días calendario para presentar la póliza de seguros que exige el artículo 16 del Reglamento, bajo apercibimiento de ser rechazada la solicitud si no lo cumple. Esta condición obliga al PSC a dar cumplimiento fiel al plan de medidas correctivas propuesto y aceptado, cuyo incumplimiento dará lugar a las sanciones que el RPSC determine en su momento.

D. Si el PSC no cumple con los requisitos y obligaciones de autorización definidos por la Ley, su Reglamento y las regulaciones asociadas incluida esta Guía, esto es, que exista al menos un requisito que como resultado de la evaluación se determine que no sea subsanable y sea calificado con una I (INSUFICIENTE), la Entidad Autorizadora procederá a dictar una resolución en la que rechaza la solicitud de inscripción en el RPSC mencionando el o los requisitos que están en dicha condición.

SEGUNDA PARTE

3 REQUISITOS PARA AUTORIZAR LA INSCRIPCIÓN DE UN PSC EN EL REGISTRO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

El objetivo general de la evaluación es verificar el cumplimiento de los requisitos y obligaciones que impone la Ley, su Reglamento y esta Guía, al Prestador de Servicios de Certificación que solicita su inscripción en el Registro de Prestadores de Servicios de Certificación adscrito al Ministerio de Economía.

Por ello, en este documento cada requisito se acompaña de una Guía de Evaluación para permitir al PSC conocer los requisitos mínimos que deberá cumplir y demostrar ante la Entidad Autorizadora.

A su vez, la Entidad Autorizadora realizará revisiones periódicas de la operación de los PSC autorizados para asegurar la conservación en el tiempo de las condiciones presentadas al momento de su autorización, así como el cumplimiento de los planes de medidas correctivas, cuando fuere el caso, y contará para ello con profesionales calificados.

El contenido de estos criterios puede cambiar en el tiempo, dependiendo de los avances de la tecnología y consideraciones de seguridad nacional. Si existiera alguna duda respecto a la actualización de estos criterios, debe contactarse con el Registro de Prestadores de Servicios de Certificación adscrito al Ministerio de Economía. No obstante, todo PSC autorizado será notificado de los cambios de este documento.

Tipología de los requisitos de autorización

Los tipos de requisitos necesarios para que un Prestador de Servicios de Certificación sea incluido en el registro de prestadores autorizados son los siguientes:

R1 Admisibilidad – Se refiere a la verificación de la entrega de toda la información solicitada para dar inicio al procedimiento de evaluación del PSC.

R2 Aspectos Legales y Comerciales – Se refiere a la verificación y validación de todos los aspectos relacionados con la documentación legal y comercial solicitada.

R3 Servicios Ofrecidos – Se refiere a la verificación y validación de todos los tipos de servicios ofrecidos por el PSC, cuya autorización será sometida a evaluación de la Entidad Autorizadora.

R4 Estándares – Se refiere a la verificación del apego a estándares internacionales que permiten determinar los niveles de seguridad lógica, física y de plataformas tecnológicas que dispone el PSC para prestar sus servicios, tanto a nivel de autoridad de certificación, como de autoridad de registro, data center, etc., los cuales deben ser demostrados a través de certificados emitidos por terceras partes independientes, reconocidas internacionalmente o autorizadas en el país para prestar dicho servicio por los organismos pertinentes.

R5 Políticas y Prácticas del PSC – Se refiere a la verificación y validación de la declaración de prácticas de certificación y de la(s) política(s) de certificado(s).

R6 Administración del PSC – Se refiere a la verificación y validación de los requisitos relacionados con la especificación de las operaciones y gestión de certificación y registro, la asignación de funciones y responsabilidades del personal, los planes de entrenamiento, etc.

Interpretación y aplicación de los requisitos

En lo sucesivo, las partes entenderán el documento y sus requisitos aplicables según se corresponda con los tipos de servicios que éstos ofrezcan y con su modelo de operación definido. Sin embargo se especifican explícitamente las siguientes interpretaciones.

A. Si un PSC ha decidido no ofrecer servicios de almacenamiento de comunicaciones electrónicas, entonces no le son aplicables los requisitos de un data center.

B. Si un PSC tiene externalizadas las funciones de Autoridad Certificadora o Autoridad de Estampado Cronológico, por tratarse de funciones sensibles, las empresas en que estén externalizadas dichas tareas deberán cumplir con los requisitos de operación, estandarización y certificaciones, como si se tratase de empresas instaladas en Guatemala, y deberán demostrar dicho cumplimiento por la vía de certificados entregados por entidad internacionales pertinentes y reconocidas, quedando además establecido en los contratos de externalización de servicios la obligación de mantener el cumplimiento de dichos requisitos.

3.1 REQUISITO 1. ADMISIBILIDAD

El objetivo de este requisito es determinar si la solicitud de autorización en el registro de prestadores de servicios de certificación está completa. Es decir, si se acompañó de todos los antecedentes individualizados en el formulario Solicitud de Antecedentes para iniciar el procedimiento de evaluación del PSC.

3.1.1 DOCUMENTACIÓN Y/O EVIDENCIA SOLICITADA

A. Para solicitar su inscripción en el RPSC, la entidad solicitante deberá presentar ante la Entidad Autorizadora una solicitud por escrito dirigida al Director Ejecutivo, individualizándose mediante los siguientes documentos:
   i. Nombre o razón social
   ii. Copia autenticada por un Notario de la constancia de actualización al Registro Tributario Unificado (RTU)
   iii. Nombre del (de los) representante(s) legal(es)
   iv. Para el o los representantes legales de la empresa y administradores que posean título profesional, entregar constancia del (los) colegio(s) profesional(es) que señale que ninguno ha sido suspendido en el ejercicio de su profesión por falta grave contra la ética, y que ninguno ha sido excluido de ellos
   v. Antecedentes comerciales, penales y policiacos del representante legal y de los administradores
   vi. Copia autenticada por un Notario del documento de identificación del (de los) representante(s) legal(es) de la entidad
   vii. Domicilio social, domicilio fiscal y domicilios comerciales, más una declaración indicando el domicilio para recibir las notificaciones, en papel membretado a nombre de la empresa, con firma y sello de alguno de los representantes legales de la empresa
   viii. Dirección de dominio electrónico de la empresa
   ix. Dirección de correo electrónico del representante legal
   x. Número telefónico
   xi. Declaración expresa del representante legal aceptando el correo electrónico como forma de comunicación.

B. Dicha solicitud deberá ir acompañada por el comprobante de pago de los costos de la autorización, girado a nombre del Registro de Prestadores de Servicios de Certificación, según los datos publicados en la página web del RPSC http://www.rpsc.gob.gt/.

C. Además se deberán incluir los siguientes documentos y antecedentes legales y comerciales:
   i. Definición de un procedimiento interno del PSC previsto para asegurar el acceso a los auditores designados por el RPSC.
   ii. Copia de todos los contratos de servicios externalizados relevantes y sensibles en la operación del sistema, si los hay. O en

su defecto, una declaración por escrito, firmada por el representante legal, indicando que no existen servicios relevantes y sensibles en la operación del sistema que estén externalizados.

iii. Copia autenticada por un Notario de la escritura de constitución de la sociedad con extractos debidamente inscritos y publicados, incluyendo la vigencia
iv. Poderes de él o los representantes legales de la entidad solicitante
v. Copia autenticada por un Notario del Carnet de Identificación Tributaria (NIT)
vi. Copia de la política de privacidad del PSC
vii. Copia de la patente de comercio y de sociedad legalizada mediante un Notario
viii. Para empresas con historial comercial, entrega de los últimos 3 balances auditados de la Persona Jurídica del PSC. Para empresas nuevas, declaración patrimonial de la entidad solicitante.

D. Además se deberán incluir los siguientes documentos y antecedentes técnicos:
   i. Ejemplos de todos los tipos de servicios ofrecidos por el PSC
   ii. Certificado de firma electrónica de la Autoridad Certificadora emisora, con la cual se firmará como raíz, en formato binario
   iii. Lista(s) tipo de certificados revocados vigente(s) (CRL)
   iv. Descripción del sitio de acceso público vía web, que contenga al menos: Dirección URL del sitio Web, descripción de la tecnología usada para prestar los servicios antes declarados, tipo de conectividad usada, niveles y formas de accesibilidad ofrecidas, medidas de seguridad;
   v. Descripción del modelo de confianza utilizado por el PSC para lograr el objetivo o, alternativamente, la Declaración de Prácticas de Certificación, si contiene dicho punto
   vi. Manual técnico de los dispositivos seguros de firma electrónica ofrecidos y/o utilizados

E. Además se deberán entregar los siguientes documentos y antecedentes relativos a la seguridad física, lógica y de la plataforma tecnológica utilizada:

   i. Para la operación en el rol de Autoridad Certificadora, y para la Autoridad de Estampado Cronológico:
   Copia validada ante Notario del **certificado** emitido por una tercera parte independiente (entidad certificadora reconocida) del cumplimiento de **uno** de los siguientes estándares internacionales:
   - ISO/IEC 27001 Information Technology – Security Techniques. Information Security Management Systems. Requirements. O la respectiva normal guatemalteca que la homologue.

- WebTrust for Certificate Authorities. O la respectiva normal guatemalteca que la homologue.

ii. Para la verificación del registro público en línea:
Certificación de un auditor independiente del uso de protocolo OCSP según el siguiente estándar:

- RFC 2560 X.509 Internet PKI Online Certificate Status Protocol - OCSP. June 1999. O la respectiva normal guatemalteca que la homologue.

iii. Para el hardware criptográfico de la raíz de la Autoridad Certificadora, y para la Autoridad de Estampado Cronológico:
Copia validada ante Notario del **certificado** emitido por una tercera parte independiente (entidad certificadora reconocida) del cumplimiento de uno de los dos estándares internacionales siguientes:

- FIPS PUB 140-1: Security Requirements for Cryptographic Modules, (Mayo 2001) Nivel 3. O la respectiva norma guatemalteca que la homologue.
- FIPS PUB 140-2: Security Requirements for Cryptographic Modules (Mayo 2002) Nivel 3. O la respectiva norma guatemalteca que la homologue.

iv. Para la operación de la Autoridad de Registro, y de todas las delegadas que existan en ese rol:

Medida transitoria:
Copia validada ante Notario del certificado emitido por una tercera parte independiente (entidad certificadora reconocida) del cumplimiento del estándar internacional ISO 9001, en el cual se consigne a su vez que dentro de los compromisos asumidos por la entidad está el apego al estándar ISO/IEC 27001 Information Technology – Security Techniques. Information Security Management Systems. Requirements. O las respectivas normas guatemaltecas que las homologuen, respectivamente.

A contar del 31 de marzo de 2014, todas las empresas, nuevas y autorizadas, deberán cumplir con lo siguiente en reemplazo de la medida transitoria:
Copia validada ante Notario de los certificados emitidos por una tercera parte independiente (entidad certificadora reconocida) del cumplimiento de los estándares internacionales ISO 9001 e ISO/IEC 27001. O las respectivas normas guatemaltecas que las homologuen, respectivamente.

v. **Para la prestación del servicio de estampado cronológico (time-stamping):**
Copia validada ante Notario del certificado emitido por una tercera parte independiente (entidad certificadora reconocida) del cumplimiento del estándar internacional ISO/IEC 27001 (o la respectiva norma guatemalteca que la homologue), en el cual se consigne a su vez que dentro de los compromisos asumidos por la entidad está el apego a los siguientes tres estándares:
- ETSI TS 102 023 V1.2.1 (2003-01) Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities. O la respectiva norma guatemalteca que la homologue. En dicho estándar se hace exigible el uso del algoritmo de hash SHA-1 con RSA y largos de llave de al menos 2048 bits con RSA.
- ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services. O la respectiva norma guatemalteca que la homologue.
- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol. O la respectiva norma guatemalteca que la homologue.

vi. **Para el dispositivo en el cual se entregarán los certificados y datos privados de firma electrónica ofrecidos por el PSC a sus clientes (smart card, token, etc.):**
Copia validada ante Notario del certificado emitido por una tercera parte independiente (entidad certificadora internacional reconocida) del cumplimiento de uno de los dos estándares internacionales siguientes:
- FIPS PUB 140-1: Security Requirements for Cryptographic Modules, (Mayo 2001) Nivel 2 ó 3. O la respectiva norma guatemalteca que la homologue.
- FIPS PUB 140-2: Security Requirements for Cryptographic Modules (Mayo 2002) Nivel 2 ó 3. O la respectiva norma guatemalteca que la homologue.

vii. **Para la operación del Data Center, cuando se ofrezca la prestación de servicios de almacenamiento de comunicaciones electrónicas y otro tipo de documentos electrónicos:**
Copia validada ante Notario del **certificado** emitido por una tercera parte independiente (entidad certificadora reconocida) del cumplimiento del estándar internacional ISO/IEC 27001 Information Technology – Security Techniques. Information Security Management Systems. Requirements. Donde se consigne el apego del Data Center al estándar TIA-942 Telecommunications Infrastructure Standard for Data Centers (Abril 2005), en TIER III o TIER IV. O las respectivas normas guatemaltecas que las homologuen respectivamente.

F. Además incluir los siguientes documentos y antecedentes relativos a la operación de la autoridad certificadora y de la(s) autoridad(es) de registro:
   i. Declaración de Prácticas de Certificación (CPS) del prestador de servicios de certificación
   ii. Política de Certificado (CP) para todos los tipos de servicios ofrecidos, en cuanto tengan variaciones respecto de la política de certificado más general
   iii. Manual de operación de la autoridad certificadora
   iv. Manual de operación de la autoridad de estampado cronológico
   v. Manual de operación de la autoridad de registro
   vi. Manual de operación del data center
   vii. Perfiles de los cargos que manejan información o sistemas sensibles
   viii. Currículos de las personas que ocupan los cargos y funciones sensibles. Cómo mínimo deberán contar con un profesional jurídico, un profesional de sistemas y un oficial de seguridad
   ix. Procedimientos de seguridad aplicados en la contratación y seguimiento de los antecedentes comerciales, penales y policiacos del personal de la empresa
   x. En particular respecto del Oficial de Seguridad, entregar currículo que incluya, como mínimo, dos (2) referencias profesionales y una (1) referencia personal; más copia autenticada ante Notario de los certificados que acrediten el perfil profesional del Oficial de Seguridad emitidos por entidades reconocidas u homologadas por las autoridades respectivas, y por referentes de la industria para el caso de las certificaciones técnicas.
   xi. También respecto del Oficial de Seguridad, incluir la evidencia que permita verificar su entrenamiento en los siguientes conceptos:
      - Prácticas de Gestión de la Seguridad
      - Arquitectura y Modelos de Seguridad
      - Sistemas y Metodología de Control de Acceso
      - Seguridad en el Desarrollo de Aplicaciones y Sistemas
      - Seguridad de las Operaciones
      - Criptografía
      - Seguridad Física
      - Seguridad en Internet, Redes y Telecomunicaciones
      - Recuperación ante Desastres y Planificación de la Continuidad del Negocio
      - Leyes, investigaciones y Ética
   xii. Respecto del Oficial de Seguridad, incluir evidencia que permita verificar su adhesión al Código de Ética de la ISC2 (http://www.isc2.org).

3.1.2 *Caracterización del evaluador*

El perfil mínimo para ser evaluador de este requisito es 3 años de experiencia laboral profesional, capacitado en la Ley, su Reglamento, esta Guía, y en conceptos de seguridad, estándares, firma y certificación electrónica.

3.1.3 *Aspectos Específicos a Evaluar*

Aspecto	Evaluación	C	S	I
1. Entrega de documentación solicitada.	Verificación de los antecedentes requeridos en un plazo de cinco (5) días hábiles, donde se comprueba que el PSC entregó, al momento de la solicitud, toda la documentación requerida.	Si los antecedentes están completos y en la forma requerida. En general no se evaluará el contenido de ella, lo que es tarea de los siguientes requisitos.	Si los antecedentes no están completos o en la forma requerida.	Si falta al menos un dato o documento solicitado, y no es posible que sea entregada dentro del plazo de quince (15) días hábiles, se calificará con nota I.
2. Pago del costo de evaluación.	Se verificará que ha sido debidamente pagado el costo de realizar la evaluación de la autorización.	Se verifica el comprobante de pago por el monto y en la forma indicada en esta Guía.	No Aplica.	No se ha realizado el pago o existe algún error respecto de alguna de las condiciones expuestas en esta Guía.
3. Relación con el PSC.	Se verificará la existencia de un Procedimiento Interno del PSC previsto para asegurar el acceso a los auditores designados por el RPSC.	Se verifica que dicho procedimiento existe y es razonable de ser seguido por el RPSC para interactuar con el PSC, y en el cual el representante legal del PSC declara expresamente que acepta el correo electrónico como forma de comunicación.	(El procedimiento no está definido en términos razonables para interactuar con el PSC. O Falta o está incorrecta la declaración expresa del representante legal aceptando el correo electrónico como forma de comunicación.) Y Puede ser resuelto en plazos razonables.	(El procedimiento no está definido en términos razonables para interactuar con el PSC. O Falta o está incorrecta la declaración expresa del representante legal aceptando el correo electrónico como forma de comunicación.) Y El PSC se niega a dar solución en plazos razonables.

Si los tres aspectos han sido calificados con una C la solicitud será declarada admisible y será admitida a trámite.

Si la evaluación de los tres aspectos contiene calificaciones C y S, o sólo S, la solicitud será declarada momentáneamente inadmisible, lo que será comunicado al interesado en un plazo de tres (3) días hábiles. El PSC podrá completar los antecedentes dentro

del plazo de quince (15) días hábiles, bajo apercibimiento de ser rechazada la solicitud si incumple el plazo.

Si existe al menos un aspecto evaluado con I, la solicitud será declarada inadmisible, y el PSC deberá presentar una nueva solicitud si desea ser reevaluado.

3.2 REQUISITO 2. ASPECTOS LEGALES Y COMERCIALES

El objetivo de este requisito es comprobar que el PSC que solicita su inscripción en el registro de prestadores de servicios de certificación cumple con los requisitos legales y comerciales establecidos en la Ley, su Reglamento y en otras normativas complementarias aplicables, incluyendo esta Guía.

3.2.1 DOCUMENTACIÓN Y/O EVIDENCIA SOLICITADA

A. Nombre o razón social de la empresa solicitante
B. Constancia actualizada autenticada por un Notario del Registro Tributario Unificado, RTU
C. Nombre del (de los) representante(s) legal(es)
D. Constancia del (los) colegio(s) profesional(es) que señale que tanto el representante legal como los administradores no han sido suspendidos en el ejercicio de su profesión por falta grave contra la ética, y que no han sido excluidos de ellos
E. Antecedentes comerciales, penales y policiacos del representante legal y de los administradores
F. Copia autenticada por un Notario del documento de identificación del (de los) representante(s) legal(es) de la entidad
G. Domicilio social
H. Dirección de correo electrónico del representante legal
I. Declaración expresa del representante legal aceptando el correo electrónico como forma de comunicación, en formato de carta membretada con los datos de la empresa interesada, firmada y sellada por su representante legal.
J. Copia del contrato de todos los servicios externalizados relevantes y sensibles en la operación del sistema, si los hay.
K. Copia fiel de la escritura de constitución de la sociedad con extractos debidamente inscritos y publicados, incluyendo la vigencia
L. Poderes de él o los representantes legales de la entidad solicitante
M. Copia autenticada por un Notario del Carnet de Identificación Tributaria (NIT)
N. Documento con una Política de Privacidad de la empresa solicitante
O. Copia de la patente de comercio y de sociedad, legalizadas mediante un Notario
P. Para empresas con historial comercial, entrega de los últimos 3 balances auditados de la Persona Jurídica del PSC. Para empresas nuevas, declaración patrimonial de la entidad solicitante.

3.2.2 CARACTERIZACIÓN DEL EVALUADOR

El perfil mínimo para ser evaluador de este requisito es título profesional de abogado y 3 años de experiencia laboral profesional. Familiarizado con contratos, legislación relacionada con privacidad de la información y protección

al consumidor, capacitado en la Ley, su Reglamento, esta Guía, y en conceptos de seguridad, estándares, firma y certificación electrónica.

3.2.3 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación	C	S	I
1. Identificación completa del PSC	Se verificará la identificación del PSC: • Nombre o razón social de la empresa solicitante • Constancia actualizada autenticada por un Notario de RTU • Nombre del (los) representante(s) legal(es) • Documento(s) de identificación del (los) representante(s) legal(es) • Domicilio social • Dirección de correo electrónico del representante legal • Declaración expresa del representante legal aceptando el correo electrónico como forma de comunicación, en formato indicado.	Toda la información de identificación se encuentra completa y en la forma solicitada.	Alguno de los documentos entregados no cumple con la forma requerida pero es posible hacerlo llegar como es debido en plazos razonables.	Alguno de los documentos entregados no cumple con la forma requerida y existe alguna imposibilidad de hacerlo llegar como es debido en plazos razonables.
2. Personalidad jurídica	Se verificará la validez y vigencia de la personalidad jurídica del solicitante, mediante la revisión y comprobación de la escritura presentada y sus certificados.	Está la solicitud debidamente individualizada y toda la documentación solicitada.	Si los antecedentes están en la forma requerida, o presentan algún problema resoluble en plazos razonables.	Alguno de los documentos solicitados no está en la forma requerida, y no es posible resolverlo en plazos razonables.
3. Domicilio	Se verificará que el solicitante tenga	El interesado tiene domicilio en	No Aplica.	El interesado no tiene domicilio en

Aspecto	Evaluación	C	S	I
	domicilio en el país.	Guatemala.		Guatemala.
4. Idoneidad de la administración del PSC	Se verificarán los antecedentes comerciales, penales, policiacos, y las constancias en los colegios profesionales del representante legal y de los administradores del PSC. Además se verificarán los siguientes documentos: • Copia autenticada por un notario de la escritura de constitución de la sociedad con extractos debidamente inscritos y publicados, incluyendo la vigencia • Poderes de él o los representantes legales de la entidad solicitante	Ninguno(a) de ello(a)s tiene anotaciones comerciales, penales o policiacas, o ha sido suspendido(a)s en el ejercicio de su profesión por falta grave contra la ética, y tampoco se encuentran excluido(a)s de los respectivos colegios profesionales. Además la escritura de la sociedad y la delegación de poderes expresa convenientemente su responsabilidad respecto de la empresa.	No Aplica.	Alguno(a) de ello(a)s tiene anotaciones comerciales, penales o policiacas, o está suspendido(a) en el ejercicio de su profesión por falta grave contra la ética, o se encuentra excluido(a) de su colegio profesional. o La escritura de la sociedad o la delegación de poderes deja dudas respecto de la responsabilidad que tienen respecto del quehacer de la empresa.
5. Capacidad económica	Se verificarán las autorizaciones de operación de la empresa, con base en los siguientes documentos: • Copia autenticada por un Notario del Carnet de Identificación Tributaria (NIT) • Copia de la patente de comercio legalizada mediante un Notario Además se verificará su capacidad económica con base en los	La empresa cuenta con los permisos necesarios para operar en el país en un rubro compatible con los servicios de certificación; y además muestra solvencia económica suficiente para prestar el servicio, y cumplir con las obligaciones requeridas en la Ley, su Reglamento y esta Guía.	La empresa no cuenta con los permisos necesarios para operar en el país en un rubro compatible con los servicios de certificación, pero puede llevar a cabo la tramitación necesaria para ello en un plazo razonable.	La empresa no muestra solvencia económica suficiente para prestar el servicio, y cumplir con las obligaciones requeridas en la Ley, su Reglamento y esta Guía.

Aspecto	Evaluación	C	S	I
	siguientes documentos: • Para empresas con historia, entrega de los últimos 3 balances auditados de la Persona Jurídica del PSC. Para empresas sin historia, declaración patrimonial de la entidad solicitante.			
6. Declaración de la importancia de la privacidad en su rol de PSC.	Se verificará la existencia y el contenido de la Política de Privacidad de la empresa solicitante.	La política de privacidad aborda los aspectos requeridos en la legislación nacional, la Ley, su Reglamento, y esta Guía.	La política de privacidad está incompleta, pero puede ser subsanado en plazos razonables.	El PSC se niega a modificar su Política de Privacidad en los plazos establecidos, o a cumplir con lo requerido en la Ley, su Reglamento, y esta Guía.
7. Delegación responsable de parte de la actividad del PSC.	Se verificarán todos los contratos en que el PSC delega parte de su actividad a terceros, empresas o personas, externalizando alguna parte sensible de su operación.	Se verifica que el PSC ha hecho entrega de una copia de todos los contratos externalizados. Dichos contratos establecen condiciones que dan seguridad al sistema estableciendo, cuando corresponda, la obligación de la tercera parte de mantener las certificaciones o estándares que le serían exigidos en esta Guía al PSC si prestase dichos servicios. Dichos contratos incluyen además cláusulas de privacidad y confidencialidad respecto de la información que los terceros reciban de parte del PSC.	(Se verifica que el PSC no ha hecho entrega de una copia de todos los contratos externalizados. o Dichos contratos no cubren las condiciones mínimas para dar seguridad al sistema, como si se tratase de una operación interna del PSC. o Dichos contratos no incluyen cláusulas de privacidad y confidencialidad respecto de la información que los terceros reciban de parte del PSC.) Y Alguna o todas las anteriores se pueden resolver en plazos razonables.	(Se verifica que el PSC no ha hecho entrega de una copia de todos los contratos externalizados. o Dichos contratos no cubren las condiciones mínimas para dar seguridad al sistema, como si se tratase de una operación interna del PSC. o Dichos contratos no incluyen cláusulas de privacidad y confidencialidad respecto de la información que los terceros reciban de parte del PSC.) Y Alguna o todas las anteriores no se puede resolver en plazos razonables.

Si los siete aspectos han sido calificados con una C el requisito sobre Aspectos Legales y Comerciales se entenderá como aprobado.

Si la evaluación de los siete aspectos contiene calificaciones C y S, o sólo S, el requisito será entendido como parcialmente aprobado. El PSC exigirá resolución a las observaciones planteadas, y fijará plazos, bajo apercibimiento de ser rechazada la solicitud si se incumple el plazo.

Si existe al menos un aspecto evaluado con I, el requisito se entenderá como incumplido, lo que habilitará a la Entidad Autorizadora para rechazar la solicitud de inscripción en el RPSC, y el PSC deberá presentar una nueva solicitud si desea ser reevaluado.

3.3 *REQUISITO 3 – SERVICIOS OFRECIDOS*

El objetivo de este requisito es comprobar los aspectos mínimos que disponen la Ley, su Reglamento y esta Guía, en relación a la conformidad con estándares, contenidos mínimos, límites y atributos de los distintos tipos de servicios ofrecidos por el PSC.

3.3.1 *DOCUMENTACIÓN Y/O EVIDENCIA SOLICITADA*

A. Ejemplos de todos los tipos de servicios ofrecidos por el PSC (en caso de certificados, entregar archivos con extensión .cer), entre otros (Art. 41 de la Ley):

- Certificado de firma electrónica avanzada de personas naturales o jurídicas, ya sean éstas digitales o de cualquier otra índole;
- Certificado sobre la verificación respecto de la alteración entre envío y recepción de las comunicaciones electrónicas;
- Facilitación del servicio de creación de firmas electrónicas avanzadas certificadas, ya sean éstas digitales o de cualquier otra índole;
- Certificados en relación con la persona que posea un derecho u obligación con respecto a documentos de concesión, adquisición, renuncia, restitución, transferencia o negociación de algún derecho sobre mercancías (literal f del Art. 31 de la Ley);
- Certificados en relación con la persona que posea un derecho u obligación con respecto a documentos de adquisición o transferencia de derechos y obligaciones con arreglo al contrato (literal g del Art. 31 de la Ley);
- Servicio y facilitación del servicio de registro y estampado cronológico en la generación, transmisión y recepción de comunicaciones electrónicas;
- Descripción de servicio de archivo y conservación de comunicaciones electrónicas;
- Certificados en los que certifiquen las condiciones profesionales del titular de la firma para efectos de constituir prueba frente a cualquier entidad pública o privada;
- Otros no especificados.

B. Certificado de firma electrónica de la Autoridad Certificadora emisora, con la cual se firmará como raíz, en formato de extensión .cer

C. Lista(s) de certificado de firma electrónica avanzada revocados (CRL tipo) emitido por el PSC en formato de extensión .crl.

D. Descripción del sitio de acceso público vía web, que contenga al menos: Dirección URL del sitio Web, descripción de la tecnología usada para prestar los servicios antes declarados, tipo de conectividad usada, niveles y formas de accesibilidad ofrecidas, medidas de seguridad;

E. Descripción del modelo de confianza utilizado por el PSC para lograr el objetivo o, alternativamente, la Declaración de Prácticas de Certificación, si contiene dicho punto

F. Manual técnico de los dispositivos seguros de firma electrónica ofrecidos y/o utilizados

G. Dirección electrónica (URL) de la entidad certificadora, para acceder a toda su oferta pública de servicios y productos.

H. Política de certificado (CP – Certificate Policy) de cada uno de los servicios ofrecidos.

3.3.2 CARACTERIZACIÓN DEL EVALUADOR

El perfil mínimo para ser evaluador de este requisito es título profesional de ingeniero en computación, informática, telecomunicaciones, electricidad, electrónica, o afín, con experiencia demostrable en uso de estándares de seguridad de la información mínima de 3 años, capacitado en la Ley, su Reglamento, esta Guía, y en conceptos específicos de los estándares aplicables a firma y certificación electrónica.

3.3.3 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación	C	S	I
1. Conformidad de los certificados digitales con el estándar ISO/IEC 9594-8	Verificar, para todos los tipos de certificados digitales emitidos, que la estructura básica del certificado esté en conformidad a la norma y que la gramática utilizada puede ser leída por cualquier aplicación que cumpla dicho estándar.	La estructura está de acuerdo al estándar, por lo que puede ser visualizado utilizando los navegadores más usados.	No Aplica.	Presenta alguna incompatibilidad con el estándar.
2. Contenido básico del certificado de firma electrónica avanzada emitido por el PSC	Para todos los tipos de certificados emitidos, se verificará que el certificado contiene la siguiente información: a) Un código de	Para todos los tipos de certificados emitidos, se ha verificado que contiene todos los datos requeridos.	Al menos uno de los tipos de certificados emitidos contiene todos los datos requeridos. Y Existen otros en que no	Ninguno de los tipos de certificados emitidos cumple con el contenido básico exigido, y no es factible subsanar las faltas en plazos razonables.

Aspecto	Evaluación	C	S	I
	identificación único y/o número de serie del certificado; b) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección y domicilio, dirección de correo electrónico y alguno de los siguientes: número de identificación tributaria, cédula de vecindad, código único de identificación, o pasaporte; según corresponda. c) Identificación del prestador de servicio de certificación, con indicación de su nombre comercial y/o razón social, número de identificación tributaria, dirección de correo electrónico, dirección y lugar donde realiza actividades. d) La metodología para verificar la firma electrónica del firmante. e) Fecha de emisión y expiración del certificado. f) Los antecedentes de autorización del PSC, otorgados por el RPSC. g) La firma		es así, pero puede ser corregido en plazos razonables para ser autorizados.	

Aspecto	Evaluación	C	S	I
	electrónica del PSC.			
3. Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado de firma electrónica avanzada emitido por el PSC	Se verificará que el PSC estructure sus certificados de firma electrónica avanzada de forma que los atributos adicionales que introduzca con el fin de incorporar límites al uso del certificado, si los hay, no impidan la lectura del contenido básico exigido, ni su reconocimiento por terceros.	No incorpora atributos que impidan su lectura a terceros, ni impidan visualizar el contenido básico exigido. O Los atributos incorporados pueden ser leídos sin problema y no impiden visualizar el contenido mínimo exigido.	No aplica.	Incorpora atributos que impiden su lectura a terceros o impiden visualizar el contenido básico exigido.
4. Reconocimiento de límites de uso del certificado de firma electrónica avanzada por terceros	Se verificará que el PSC estructure sus certificados de firma electrónica avanzada de forma que los límites de uso, si los hay, sean reconocibles por terceros.	Para cada tipo de certificado ofrecido, es posible verificar sus límites en el certificado, según se indica en su política (CP).	Los límites de uso no son reconocibles por terceros pero es subsanable en plazos razonables antes de empezar a operar.	Los límites de uso no son reconocibles por terceros, y/o no puede ser subsanado en plazos razonables para empezar a operar.
5. Uso de clave pública autorizada	Se verificará que los datos de creación de firma del PSC autorizado para emitir certificados de firma electrónica avanzada no son utilizados para certificados emitidos bajo otras políticas (CP).	Verificar en la oferta pública del PSC que no se ofrecen otros tipos de servicios que usen los datos de creación de firma electrónica avanzada del PSC.	No aplica.	Los datos de creación de firma electrónica avanzada autorizados se usan para otros servicios no autorizados.
6. Algoritmos de firma	Se verificará que el PSC utilice algoritmos de firma estándares de la industria que provean el adecuado nivel de seguridad tanto para su propia firma como para la firma del titular.	Está en conformidad a estándar vigente de la industria RSA, en su formato nacional, o en formato internacional: RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	El algoritmo no es el requerido pero se puede modificar en plazos razonables antes de empezar a operar como entidad autorizada.	El algoritmo no es el requerido y se puede modificar en plazos razonables antes de empezar a operar como entidad autorizada.
7. Largos de llaves	Se verificará que el PSC utilice largos de llave pública y privada tales que provean el nivel de	Largo de llave para firma del PSC y para firma del titular, en ambos casos, igual o	El largo de llave de PSC o del titular de la firma, o ambos, es menor a lo requerido pero el PSC	El PSC no cumple con uno o ambos largos de llave requeridos, y no tiene mecanismos para

Aspecto	Evaluación	C	S	I
	seguridad prevaleciente en la industria tanto para su propia firma como para la firma del titular.	superior a: 2048 bits (en RSA)	va a modificar el largo de las llaves bajo el estándar requerido antes de comenzar a operar.	modificar el largo de llave de firma antes de comenzar a operar como entidad autorizada.
8. Funciones Hash	Se verifica que el PSC utilice funciones de hash estándares de la industria, para el proceso de firma, que provean el adecuado nivel de seguridad tanto para su propia firma como para la firma del titular.	Las funciones de hash utilizadas están en conformidad a estándar vigente de la industria SHA-1, en su formato nacional, o en formato internacional: RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	El PSC puede hacer los cambios para ajustarse al estándar en tiempos razonables antes de comenzar a operar como entidad autorizada.	El PSC no puede hacer los cambios para ajustarse al estándar en tiempos razonables antes de comenzar a operar como entidad autorizada.
9. Seguridad del archivo y conservación de comunicaciones electrónicas	Se verifica que el servicio ofrecido incluye un nivel de seguridad adecuado para el riesgo asumido	La descripción del servicio incluye una oferta de seguridad del Data Center en conformidad a estándar vigente de la industria en su formato nacional, o en formato internacional: TIA-942 (April 2005) Telecommunications Infrastructure Standard for Data Centers en el cual se distingue claramente la seguridad y disponibilidad ofrecida, con un mínimo de TIER 2, y un razonable de TIER 3 o TIER 4 para las comunicaciones y archivos más importantes	La descripción del servicio no entrega claridad de los niveles de seguridad y disponibilidad ofrecidos, sin embargo, estos corresponden como mínimo al nivel exigido, y la información entregada al usuario del servicio puede ser actualizada y completada en plazos razonables, antes de comenzar a operar como entidad autorizada.	La descripción del servicio no entrega claridad de los niveles de seguridad y disponibilidad ofrecidos, y/o ella no alcanza al nivel mínimo exigido, lo que no puede ser modificado en plazos razonables, antes de comenzar a operar como entidad autorizada.
10. Contenido mínimo de la(s) lista(s) de certificados revocados (CRL)	Verificar que la(s) CRL contenga(n) al menos la siguiente información: • Versión 2. • Algoritmo de firma. Este campo debe contener la	La CRL contiene todo lo exigido como mínimo, y su estructura está en conformidad a estándar vigente de la industria en su formato nacional, o en formato internacional: RFC 5280 Internet X.509	La CRL carece de ciertos atributos exigidos o su estructura no está en conformidad a estándar requerido pero puede ser solucionado en un plazo razonable antes de empezar a operar como	La estructura presenta alguna incompatibilidad con el estándar y no puede ser solucionada en un plazo razonable antes de empezar a operar como entidad autorizada.

Aspecto	Evaluación	C	S	I
	identificación del algoritmo de firma utilizado. • Nombre del emisor. Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados. • Fecha actual. Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados (CRL). • Próxima actualización. Se debe incluir en este campo la fecha en que, a más tardar, se emitirá la próxima lista de certificados revocados. • Certificados revocados. En este campo se deben incluir los números de serie de los certificados revocados por el emisor, indicando además la fecha y hora de revocación correspondiente. • Certificados suspendidos. En este campo se deben incluir los números de serie de los certificados suspendidos por el emisor, indicando además la fecha y hora de suspensión correspondiente. • Firma electrónica del PSC emisor.	Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	entidad autorizada.	

Aspecto	Evaluación	C	S	I
11. Existencia y contenido mínimo del sitio de información pública	El PSC debe mantener un sitio en Internet, en el cual mantenga la información relevante para los titulares y las partes que confían. Debe contener al menos los siguientes documentos: • Registro de certificados emitidos, indicando código de identificación único del certificado y su estado (vigente, suspendido o revocado) emitido usando estándar de la industria. • Copia de la Lista de certificados revocados (CRL) actualizada cada 24 horas. • Si es pertinente, indicar si el certificado ha sido traspasado de otro prestador de servicios de certificación autorizado o ha sido homologado. • Acceso seguro a los titulares para realizar la revocación y/o suspensión de certificados vigentes. • Política de certificado (CP) de cada uno de los certificados ofrecidos. • Declaración de sus Prácticas de Certificación (CPS).	El PSC mantiene un sitio en Internet que contiene como mínimo la información exigida. Además para acceder a los certificados emitidos y verificar su estado ofrece un servicio en línea en conformidad a estándar vigente de la industria en su formato nacional, o en formato internacional: RFC 2560 X.509 Internet PKI Online Certificate Status Protocol - OCSP. June 1999	El PSC tiene un sitio en Internet con parte de la información y servicios exigidos en línea, y puede completar lo faltante en un plazo razonable antes de empezar a operar como entidad autorizada.	El PSC tiene un sitio en Internet con parte de la información y servicios exigidos en línea, pero no puede completar lo faltante en un plazo razonable antes de empezar a operar como entidad autorizada.

Aspecto	Evaluación	C	S	I
	• Resoluciones de la Entidad Autorizadora que le afecten, incluyendo sanciones aplicadas. • Mecanismo en línea para consulta de certificados.			

Si los once aspectos han sido calificados con una C el requisito sobre Servicios Ofrecidos se entenderá como aprobado.

Si la evaluación de los once aspectos contiene calificaciones C y S, o sólo S, el requisito será entendido como parcialmente aprobado. El PSC exigirá resolución a las observaciones planteadas, y fijará plazos, bajo apercibimiento de ser rechazada la solicitud si se incumple el plazo.

Si existe al menos un aspecto evaluado con I, el requisito se entenderá como incumplido, lo que habilitará a la Entidad Autorizadora para rechazar la solicitud de inscripción en el RPSC, y el PSC deberá presentar una nueva solicitud si desea ser reevaluado.

3.4 REQUISITO 4 – ESTÁNDARES

El objetivo de este requisito es verificar que el PSC ha sido certificado por terceras partes independientes y pertinentes, ya sea en Guatemala o por entidad extranjeras reconocidas internacionalmente, que cumplen con estándares exigibles dependiendo del tipo de servicio prestado.

Además dichos requisitos de certificación serán extensibles a las empresas en las cuales se haya externalizado el servicio mencionado.

3.4.1 DOCUMENTACIÓN Y/O EVIDENCIA SOLICITADA

A. Para la operación en el rol de Autoridad Certificadora, y para la Autoridad de Estampado Cronológico, uno de los siguientes certificados:
   - ISO/IEC 27001 Information Technology – Security Techniques. Information Security Management Systems. Requirements. O la respectiva normal guatemalteca que la homologue.
   - WebTrust for Certificate Authorities. O la respectiva normal guatemalteca que la homologue.

B. Para el hardware criptográfico de la raíz de la Autoridad Certificadora, y para la Autoridad de Estampado Cronológico, uno de los siguientes certificados:
   - FIPS PUB 140-1: Security Requirements for Cryptographic Modules, (Mayo 2001) Nivel 3. O la respectiva norma guatemalteca que la homologue.
   - FIPS PUB 140-2: Security Requirements for Cryptographic Modules (Mayo 2002) Nivel 3. O la respectiva norma guatemalteca que la homologue.

C. Para la operación de la Autoridad de Registro, y de todas las delegadas que existan en ese rol:

   Medida transitoria:
   Certificado del estándar internacional ISO 9001, en el cual se consigne a su vez que dentro de los compromisos asumidos por la entidad está el apego al estándar ISO/IEC 27001. O las respectivas normas guatemaltecas que las homologuen, respectivamente.

   A contar del 31 de marzo de 2014, todas las empresas, nuevas y autorizadas, deberán cumplir con lo siguiente en reemplazo de la medida transitoria:
   Certificados de los estándares internacionales ISO 9001 e ISO/IEC 27001. O las respectivas normas guatemaltecas que las homologuen, respectivamente.

D. Para la prestación del servicio de estampado cronológico (time-stamping):
   - ISO/IEC 27001 (o la respectiva norma guatemalteca que la homologue), en el cual se consigne el apego a los siguientes tres estándares:
     a. ETSI TS 102 023 V1.2.1 (2003-01) Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities. O la respectiva norma guatemalteca que la homologue.

En dicho estándar se hace exigible el uso del algoritmo de hash SHA-1 con RSA y largos de llave de al menos 2048 bits con RSA.

b. ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services. O la respectiva norma guatemalteca que la homologue.
c. RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol. O la respectiva norma guatemalteca que la homologue.

E. Para el dispositivo en el cual se entregarán los certificados y datos privados de firma electrónica ofrecidos por el PSC a sus clientes (smart card, token, etc.), certificado de uno de los dos estándares internacionales siguientes:
   - FIPS PUB 140-1: Security Requirements for Cryptographic Modules, (Mayo 2001) Nivel 2 ó 3. O la respectiva norma guatemalteca que la homologue.
   - FIPS PUB 140-2: Security Requirements for Cryptographic Modules (Mayo 2002) Nivel 2 ó 3. O la respectiva norma guatemalteca que la homologue.

F. Para la operación del Data Center, cuando se ofrezca la prestación de servicios de almacenamiento de comunicaciones electrónicas y otro tipo de documentos electrónicos:
   - ISO/IEC 27001 Information Technology – Security Techniques. Information Security Management Systems. Requirements. Donde se consigne el apego del Data Center al estándar TIA-942 Telecommunications Infrastructure Standard for Data Centers (Abril 2005), en TIER III o TIER IV. O las respectivas normas guatemaltecas que las homologuen respectivamente.

3.4.2 CARACTERIZACIÓN DEL EVALUADOR

El perfil mínimo para ser evaluador de este requisito es título profesional de ingeniero en sistemas o computación, informática, telecomunicaciones, electrónica, o afín, con experiencia demostrable en uso de estándares de seguridad de la información mínima de 3 años, capacitado en la Ley, su Reglamento, esta Guía, y en conceptos específicos de los estándares aplicables a firma y certificación electrónica.

3.4.3 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación	C	S	I
1. Certificados pare rol de Autoridad Certificadora	Verificar para rol de AC, tener certificado de uno de los siguientes: • ISO/IEC 27001:2005 • WebTrust for Certificate Authorities. O la respectiva normal guatemalteca que la	Se tienen certificados que puede ser validado para demostrar que el PSC, en su rol de Autoridad Certificadora, extensible a quien lo haya delegado cuando sea el caso, cumple con los estándares exigidos.	El PSC, en su rol de Autoridad Certificadora, extensible a quien lo haya delegado cuando sea el caso, está en proceso de alcanzar las certificaciones exigidas según consta en informe de auditoría elaborado por tercera parte independiente	El PSC, en su rol de Autoridad Certificadora, extensible a quien lo haya delegado cuando sea el caso, no cumple con los estándares exigidos.

Aspecto	Evaluación	C	S	I
	homologue. Y para el hardware criptográfico de la AC, tener certificado de uno de los siguientes: • FIPS PUB 140-1Nivel 3. • FIPS PUB 140-2 Nivel 3. O la respectiva norma guatemalteca que la homologue.		pertinente, y validado por los evaluadores del RPSC.	
2. Certificados para rol de autoridad de registro	Para el rol de AR, Provisoriamente, tener certificado ISO 9001, en el cual se consigne el apego al estándar ISO/IEC 27001:2005. A contar del 31 de marzo de 2011, tener certificado ISO 9001, y certificado ISO/IEC 27001. O las respectivas normas guatemaltecas que las homologuen. Para el dispositivo en el cual se entregarán los certificados y datos privados de firma electrónica ofrecidos por el PSC a sus clientes, el certificado de uno de los dos siguientes: • FIPS PUB 140-1Nivel 2 ó 3. • FIPS PUB 140-2 Nivel 2 ó 3. O la respectiva norma guatemalteca que la homologue.	Se tienen certificados que pueden ser validados para demostrar que el PSC, en su rol de Autoridad de Registro, extensible a quien lo haya delegado cuando sea el caso, cumple con los estándares exigidos.	El PSC, en su rol de Autoridad de Registro, extensible a quien lo haya delegado cuando sea el caso, está en proceso de alcanzar las certificaciones exigidas según consta en informe de auditoría elaborado por tercera parte independiente pertinente, y validado por los evaluadores del RPSC.	El PSC, en su rol de Autoridad de Registro, extensible a quien lo haya delegado cuando sea el caso, no cumple con los estándares exigidos.
3. Certificados para rol de autoridad de estampado cronológico	Para el rol de TSA, tener certificado de uno de los siguientes: • ISO/IEC 27001:2005 • WebTrust for Certificate Authorities.	Se tienen certificados que puede ser validado para demostrar que el PSC, en su rol de Autoridad de Estampado Cronológico, extensible a quien lo haya	El PSC, en su rol de Autoridad de Estampado Cronológico, extensible a quien lo haya delegado cuando sea el caso, está en proceso de alcanzar las	El PSC, en su rol de Autoridad de Estampado Cronológico, extensible a quien lo haya delegado cuando sea el caso, no cumple con los estándares exigidos.

Aspecto	Evaluación	C	S	I
	O la respectiva normal guatemalteca que la homologue. Para el hardware criptográfico de la TSA, tener certificado de uno de los siguientes: • FIPS PUB 140-1Nivel 3. • FIPS PUB 140-2 Nivel 3. O la respectiva norma guatemalteca que la homologue. Para la prestación del servicio de estampado cronológico, tener certificado ISO/IEC 27001 (o la respectiva norma guatemalteca que la homologue), en el cual se consigne el apego a los siguientes dos estándares: • ETSI TS 102 023 V1.2.1 (2003-01) con algoritmo de hash SHA-1 con RSA y largos de llave de al menos 2048 bits con RSA. • ISO/IEC 18014-1:2002 • RFC 3161 O las respectivas normas guatemaltecas que las homologuen.	delegado cuando sea el caso, cumple con los estándares exigidos.	certificaciones exigidas según consta en informe de auditoría elaborado por tercera parte independiente pertinente, y validado por los evaluadores del RPSC.	
4. Certificados para rol de almacenamiento de comunicaciones electrónicas	Para la operación del Data Center, tener certificado ISO/IEC 27001:2005 donde se consigne el apego del Data Center al estándar TIA-942 (Abril 2005), en TIER III o TIER IV. O las respectivas normas guatemaltecas que las homologuen respectivamente.	Se tiene un certificado que puede ser validado para demostrar que el PSC, en su oferta de almacenamiento de comunicaciones electrónicas, extensible a quien lo haya delegado cuando sea el caso, cumple con los estándares exigidos.	El PSC, en su oferta de almacenamiento de comunicaciones electrónicas, extensible a quien lo haya delegado cuando sea el caso, está en proceso de alcanzar las certificaciones exigidas según consta en informe de auditoría elaborado por tercera parte independiente pertinente, y validado	El PSC, en su oferta de almacenamiento de comunicaciones electrónicas, extensible a quien lo haya delegado cuando sea el caso, no cumple con los estándares exigidos.

Aspecto	Evaluación	C	S	I
			por los evaluadores del RPSC.	

Si los cuatro aspectos han sido calificados con una C el requisito sobre Estándares se entenderá como aprobado.

Si la evaluación de los cuatro aspectos contiene calificaciones C y S, o sólo S, el requisito será entendido como parcialmente aprobado. El PSC exigirá resolución a las observaciones planteadas, y fijará plazos, bajo apercibimiento de ser rechazada la solicitud si se incumple el plazo.

Si existe al menos un aspecto evaluado con I, el requisito se entenderá como incumplido, lo que habilitará a la Entidad Autorizadora para rechazar la solicitud de inscripción en el RPSC, y el PSC deberá presentar una nueva solicitud si desea ser reevaluado.

3.5 REQUISITO 5 – POLÍTICAS Y PRÁCTICAS DE CERTIFICACIÓN

El objetivo de este requisito es comprobar que tanto la Declaración de Prácticas de Certificación como la(s) Política(s) de Certificado cumplen con los contenidos mínimos exigidos, y están escritos de manera clara y en español.

3.5.1 DOCUMENTACIÓN Y/O EVIDENCIA SOLICITADA

A. Declaración de Prácticas de Certificación (CPS) del PSC.
B. Todas las Políticas de Certificado del PSC.

3.5.2 CARACTERIZACIÓN DEL EVALUADOR

El perfil mínimo para ser evaluador de este requisito es título profesional de ingeniero en sistemas o computación, informática, telecomunicaciones, electrónica, o afín, con experiencia demostrable en uso de estándares de seguridad de la información mínima de 3 años, capacitado en la Ley, su Reglamento, esta Guía, y en conceptos específicos de los estándares aplicables a plataformas o aplicaciones de PKI.

3.5.3 ASPECTOS ESPECÍFICOS A EVALUAR

Aspecto	Evaluación	C	S	I
1. Contenido de la política de certificado (CP)	Para cada una de las CP se deberá considerar el siguiente contenido mínimo: • Titular del certificado. A quién se le puede otorgar el certificado. • Procedimiento de registro. Se verifica el registro del titular, es decir, cómo se verifica su identidad en forma fehaciente para que el certificado pueda ser utilizado para firma electrónica avanzada. • Procedimiento de generación de llave privada del titular, para asegurar que los datos de creación de firma serán generados y entregados por el PSC en presencia	Para todos los tipos de certificados que no compartan política de certificado (CP) existe un documento que contiene al menos la información requerida, de manera clara, completa y en español, lo cual puede ser verificado en su implementación y funcionamiento.	La(s) política(s) de certificado (CP) está(n) incompleta(s) respecto de la información requerida, o no son suficientemente claras, pero puede ser subsanado en plazos razonables antes de empezar a operar como entidad autorizada.	La(s) política(s) de certificado (CP) está(n) incompleta(s) respecto de la información requerida, y no puede ser subsanado en plazos razonables antes de empezar a operar como entidad autorizada.

Aspecto	Evaluación	C	S	I
	física del titular. • Usos. La CP deberá indicar los propósitos para los cuales fue emitido el certificado y sus limitaciones. • Obligaciones. La CP debe contener una descripción de las obligaciones que contraen las entidades involucradas en la emisión y utilización del certificado (autoridad de certificación, autoridad de registro, titular y receptor), incluyendo referencias a garantía y seguros. • Verificación de las políticas de privacidad y protección de datos. Que estas políticas sean las apropiadas para la firma electrónica, y que sean publicadas y de conocimiento del subscriptor. • Indicar bajo qué circunstancias un certificado es suspendido o revocado, los plazos, y quién y cómo puede pedir dichos actos.			
2. Contenido de la Declaración de Prácticas de Certificación (CPS)	Deberá existir una CPS en español con el siguiente contenido mínimo: • Una introducción, que deberá contener un resumen de las	Existe un documento en español que contiene al menos la información requerida, de manera clara y completa, lo que puede ser verificado en su implementación y funcionamiento.	Existe un documento incompleto respecto de la información requerida, o está en un idioma distinto del español, pero cualquiera de los dos casos puede ser	Existe un documento incompleto respecto de la información requerida, o está en un idioma distinto del español, y en alguno de los dos casos no se puede ser subsanar en

Aspecto	Evaluación	C	S	I
	prácticas de certificación, mencionando tanto la entidad que suscribe el documento, como el tipo de usuarios a los que son aplicables. • Consideraciones generales, debiendo contener información sobre obligaciones, responsabilidades, cumplimiento de auditorías, confidencialidad, y derechos de propiedad intelectual, con relación a todas las partes involucradas. • Identificación y autenticación, debiendo describirse tanto los procesos de autenticación aplicados a los solicitantes de certificados, como los procesos para autenticar a los mismos cuando piden suspensión o revocación de certificado. • Requerimientos operacionales, debiendo contener información operacional para los procesos de solicitud de certificado, emisión de certificados, suspensión y revocación de certificados, procesos de		subsanado en plazos razonables antes de empezar a operar como entidad autorizada.	plazos razonables antes de empezar a operar como entidad autorizada.

Aspecto	Evaluación	C	S	I
	auditoría de seguridad, almacenamiento de información relevante, cambio de datos de creación de firma electrónica, superación de situaciones críticas, casos de fuerza mayor y caso fortuito, y procedimiento de término del usuario del servicio de certificación. • Controles de procedimiento, personal y físicos, debiendo describir los controles de seguridad no técnicos utilizados por el prestador de servicios de certificación para asegurar las funciones de generación de datos de creación de firma electrónica, autenticación de usuarios, emisión de certificados, suspensión y revocación de certificados, auditoria y almacenamiento de información relevante. • Controles de seguridad técnica, debiendo señalar las medidas de seguridad adoptadas por el prestador de servicios de certificación para proteger los datos de creación de su			

Aspecto	Evaluación	C	S	I
	propia firma electrónica. • Perfiles de certificados y del registro de acceso público, debiendo especificar el formato del certificado y del registro de acceso público para todos los tipos ofrecidos como servicio. • Especificaciones de administración de la política de certificación, debiendo señalar la forma en que la misma está contenida en la Práctica, los procedimientos para cambiar, publicar y notificar la política. • Verificar que existan procedimientos que definan el ciclo de vida de los certificados. Deberes y procedimientos del PSC para emitir / revocar / suspender / renovar certificados de firma avanzada y definiciones sobre la expiración de los certificados. • Verificar que exista la documentación de procedimientos de finalización del giro del PSC, en el que se incluyan los procedimientos de término y de traspaso a otro PSC u organismo que			

Aspecto	Evaluación	C	S	I
	asuma la responsabilidad de mantener la continuidad de los servicios, en tanto existan certificados vigentes.			
3. Consistencia entre la CPS y la(s) CP(s)	Verificación de consistencia entre todos los documentos.	Se verifica que no existen inconsistencias entre lo establecido en la CPS y lo declarado en la(s) CP(s)	Se identifica alguna inconsistencia entre lo establecido en la CPS y lo declarado en la(s) CP(s), pero ello puede ser subsanado en plazos razonables antes de empezar a operar como entidad autorizada.	Se identifica alguna inconsistencia entre lo establecido en la CPS y lo declarado en la(s) CP(s), y ello no puede ser subsanado en plazos razonables antes de empezar a operar como entidad autorizada.

Si los tres aspectos han sido calificados con una C el requisito sobre Políticas y Prácticas de Certificación se entenderá como aprobado.

Si la evaluación de los tres aspectos contiene calificaciones C y S, o sólo S, el requisito será entendido como parcialmente aprobado. El PSC exigirá resolución a las observaciones planteadas, y fijará plazos, bajo apercibimiento de ser rechazada la solicitud si se incumple el plazo.

Si existe al menos un aspecto evaluado con I, el requisito se entenderá como incumplido, lo que habilitará a la Entidad Autorizadora para rechazar la solicitud de inscripción en el RPSC, y el PSC deberá presentar una nueva solicitud si desea ser reevaluado.

3.6 REQUISITO 6 – ADMINISTRACIÓN DEL PSC

El objetivo de este requisito es comprobar, a través de la documentación presentada y la verificación de su implementación, que el modelo operacional del PSC cumple con los aspectos mínimos necesarios para ofrecer confiabilidad e interoperabilidad en su forma de operar y prestar servicios.

3.6.1 DOCUMENTACIÓN Y/O EVIDENCIA SOLICITADA

A. Modelo operacional de Autoridad Certificadora.
B. Manual de operación de la autoridad de estampado cronológico
C. Modelo operacional de Autoridad de Registro.
D. Manual de operación del data center
E. Perfiles de los cargos que manejan información o sistemas sensibles
F. Currículos de las personas que ocupan los cargos y funciones sensibles. Cómo mínimo deben contar con un profesional jurídico, un profesional de sistemas, y un oficial de seguridad
G. Procedimientos de seguridad aplicados en la contratación y seguimiento de los antecedentes comerciales, penales y policiacos del personal de la empresa
H. En particular respecto del Oficial de Seguridad, entregar currículo que incluya, como mínimo, dos (2) referencias profesionales y una (1) referencia personal; más copia autenticada ante Notario de los certificados que acrediten el perfil profesional del Oficial de Seguridad emitidos por entidades reconocidas u homologadas por las autoridades respectivas, y por referentes de la industria para el caso de las certificaciones técnicas.
I. También respecto del Oficial de Seguridad, incluir la evidencia que permita verificar su entrenamiento en los siguientes conceptos:
    - Prácticas de Gestión de la Seguridad
    - Arquitectura y Modelos de Seguridad
    - Sistemas y Metodología de Control de Acceso
    - Seguridad en el Desarrollo de Aplicaciones y Sistemas
    - Seguridad de las Operaciones
    - Criptografía
    - Seguridad Física
    - Seguridad en Internet, Redes y Telecomunicaciones
    - Recuperación ante Desastres y Planificación de la Continuidad del Negocio
    - Leyes, investigaciones y Ética
J. Respecto del Oficial de Seguridad, incluir evidencia que permita verificar su adhesión al Código de Ética de la ISC2 (http://www.isc2.org).

3.6.2 *CARACTERIZACIÓN DEL EVALUADOR*

El perfil mínimo para ser evaluador de este requisito es título profesional, con un mínimo de 3 años de experiencia laboral, capacitado en la Ley, su Reglamento, esta Guía, y en conceptos de seguridad, estándares, firma y certificación electrónica.

3.6.3 *ASPECTOS ESPECÍFICOS A EVALUAR*

Aspecto	Evaluación	C	S	I
1. Modelo de operación: de la autoridad certificadora, de la autoridad de registro, del data center, y de la autoridad de estampado cronológico	Se verificará que los modelos comprendan, al menos, los siguientes aspectos: • La historia de la empresa. • Relaciones comerciales con proveedores de insumos o servicios para sus operaciones. • Interfaces entre la Autoridad Certificadora, la Autoridad de Registro, el data center, y la Autoridad de Estampado Cronológico • Implementación de elementos de seguridad • Descripción de procesos de administración • Procesos de auditoría y respaldo • Políticas de Privacidad Además se verificará que, según corresponda, los modelos consideren la generación de llaves para el titular de acuerdo a las políticas de certificación aplicables.	Para todos los modelos de operación desarrollados por el PSC, se cumplen los requisitos exigidos. Cuando alguna de las operaciones sea subcontratada a terceros, le serán aplicables las mismas obligaciones del PSC, según conste en su documentación, o en los contratos.	Para alguno de los modelos de operación desarrollados por el PSC, se cumplen parcialmente los requisitos exigidos, pero puede ser subsanado en plazos razonables antes de empezar a operar como entidad autorizada.	Para alguno de los modelos de operación desarrollados por el PSC, se cumplen parcialmente (o no se cumplen) los requisitos exigidos, y no puede ser subsanado en plazos razonables antes de empezar a operar como entidad autorizada.

Aspecto	Evaluación	C	S	I
	Además se verificará que los modelos consideren las auditorías siguientes: • Seguridad y dispositivos de seguridad • Restricciones del personal • Interfaces de administración • Procedimientos de recuperación de desastres • Procedimientos de respaldo • Entrenamiento del personal Además se verificará que los modelos incluyan requerimientos de: • Seguridad física de las instalaciones • Seguridad del personal • Nivel de seguridad del módulo criptográfico Además se verificará que los modelos de registro del titular provean una identificación univoca del titular y el modelo de uso de la llave privada provea la confianza requerida en el sistema.			
2. Manual de operación de la Autoridad Certificadora	Se verificará que el manual tenga una descripción detallada de los siguientes procedimientos: • Generación de pares de llaves • Publicación de la CRL • Publicación de la información del certificado	El manual contiene como mínimo todo lo exigido, o hace referencia a la documentación donde se detalla lo exigido, lo cual también fue evaluado por el RPSC.	El manual no contiene como mínimo todo lo exigido, pero puede ser subsanado en plazos razonables.	El manual no contiene como mínimo todo lo exigido, y no puede ser subsanado en plazos razonables.

Aspecto	Evaluación	C	S	I
	• Distribución de llaves y certificados • Renovación de certificados • Renovación de certificados luego de una revocación • Medidas de control de acceso • Procedimientos de respaldo y recuperación • Manejo de contingencias • Actualización de la Declaración de Prácticas de Certificación y Política de certificados Descripción de los servicios de la AC y descripción de la interacción entre la AC y AR			
3. Manual de operación de la Autoridad de Registro	Se verificará que el manual tenga una descripción de los planes de contingencia.	El manual contiene como mínimo todo lo exigido, o hace referencia a la documentación donde se detalla lo exigido, lo cual también fue evaluado por el RPSC.	El manual no contiene como mínimo todo lo exigido, pero puede ser subsanado en plazos razonables.	El manual no contiene como mínimo todo lo exigido, y no puede ser subsanado en plazos razonables.
4. Gestión del personal crítico	Se verificará que el PSC cuenta al menos con el personal mínimo individualizado: jurídico, de sistemas y oficial de seguridad. Se verificará la nómina de los cargos de personal de la Autoridad Certificadora y de la Autoridad de Registro, con la descripción de las responsabilidades y los procedimientos en que los empleados realizan sus funciones	La gestión del personal crítico cumple como mínimo con todo lo exigido.	La gestión del personal crítico no cumple como mínimo con todo lo exigido, pero puede ser subsanado en plazos razonables.	La gestión del personal crítico no cumple como mínimo con todo lo exigido, y no puede ser subsanado en plazos razonables.

Aspecto	Evaluación	C	S	I
	distinguiendo, en particular, a quienes tengan responsabilidad en los planes de continuidad del negocio, y en los planes de recuperación de desastres y emergencia. Se verificarán los antecedentes profesionales y la experiencia del personal crítico que trabaja para el PSC, verificando la concordancia de los perfiles en cada cargo y función, con el análisis de riesgos. Se verificará que el personal crítico esté capacitado en las prácticas de seguridad que debe observar de acuerdo a su cargo y función. Se verificarán los antecedentes comerciales, penales y policiacos del personal crítico. Se evaluará el procedimiento definido por el PSC para la contratación del personal crítico, incluyendo comprobación de los antecedentes.			
5. Gestión del oficial de seguridad (OS)	Se verificará, además de lo estipulado para el personal general, los antecedentes profesionales y curriculares del OS.	La gestión del oficial de seguridad cumple como mínimo con todo lo exigido, y el OS es idóneo para el cargo.	La gestión del oficial de seguridad no cumple como mínimo con todo lo exigido, aunque el OS es idóneo para el cargo, y las faltas pueden ser subsanadas en plazos razonables.	La gestión del oficial de seguridad no cumple como mínimo con todo lo exigido, o el OS no es idóneo para el cargo, y las faltas no pueden ser subsanadas en plazos razonables.
6. Conocimientos del Oficial de	Se verificará la evidencia de los	Existe evidencia de cursos realizados por el	El OS está realizando dichos cursos, o ha	El OS no ha realizado instrucción formal, y no

Aspecto	Evaluación	C	S	I
Seguridad	conocimientos adquiridos por el OS, en comparación con los exigidos.	OS donde se contemplan los 10 conceptos exigidos.	cumplido parcialmente el currículo, pero puede ser subsanable.	lo ha contemplado.
7. Suscripción de código de ética	Se verificará la firma del OS respecto del código de ética de ISC2.	El OS ha suscrito el código de ética de ISC2.	El OP está en proceso de hacerlo.	El OS no está dispuesto a suscribir el código de ética.

Si los siete aspectos han sido calificados con una C el requisito sobre Administración del PSC se entenderá como aprobado.

Si la evaluación de los cinco aspectos contiene calificaciones C y S, o sólo S, el requisito será entendido como parcialmente aprobado. El PSC exigirá resolución a las observaciones planteadas, y fijará plazos, bajo apercibimiento de ser rechazada la solicitud si se incumple el plazo.

Si existe al menos un aspecto evaluado con I, el requisito se entenderá como incumplido, lo que habilitará a la Entidad Autorizadora para rechazar la solicitud de inscripción en el RPSC, y el PSC deberá presentar una nueva solicitud si desea ser reevaluado.

3.7 RESUMEN DE LA EVALUACIÓN

Finalmente, una vez realizada la evaluación descrita en los puntos anteriores, se puede construir el siguiente resumen.

Requisitos y Subrequisitos	Nota
R1 Admisibilidad	
1. Entrega de documentación solicitada.	
2. Pago del costo de evaluación.	
3. Relación con el PSC.	
R2 Aspectos Legales y Comerciales	
1. Identificación completa del PSC	
2. Personalidad jurídica	
3. Domicilio	
4. Idoneidad de la administración del PSC	
5. Capacidad económica	
6. Declaración de la importancia de la privacidad en su rol de PSC.	
7. Delegación responsable de parte de la actividad del PSC.	
R3 Servicios Ofrecidos	
1. Conformidad de los certificados digitales con el estándar ISO/IEC 9594-8	
2. Contenido básico del certificado de firma electrónica avanzada emitido por el PSC	
3. Lectura y reconocimiento del contenido mínimo cuando existen atributos adicionales en el certificado de firma electrónica avanzada emitido por el PSC	
4. Reconocimiento de límites de uso del certificado de firma electrónica avanzada por terceros	
5. Uso de clave pública autorizada	
6. Algoritmos de firma	
7. Largos de llaves	
8. Funciones Hash	
9. Seguridad del archivo y conservación de comunicaciones electrónicas	

Requisitos y Subrequisitos	Nota
10. Contenido mínimo de la(s) lista(s) de certificados revocados (CRL)	
11. Existencia y contenido mínimo del sitio de información pública	
R4 Estándares	
1. Certificados para rol de Autoridad Certificadora	
2. Certificados para rol de autoridad de registro	
3. Certificados para rol de autoridad de estampado cronológico	
4. Certificados para rol de almacenamiento de comunicaciones electrónicas	
R5 Políticas y Prácticas de Certificación	
1. Contenido de la política de certificado (CP)	
2. Contenido de la Declaración de Prácticas de Certificación (CPS)	
3. Consistencia entre la CPS y la(s) CP(s)	
R6 Administración del PSC	
1. Modelo de operación: de la autoridad certificadora, de la autoridad de registro, del data center, y de la autoridad de estampado cronológico	
2. Manual de operación de la Autoridad Certificadora	
3. Manual de operación de la Autoridad de Registro	
4. Gestión del personal crítico	
5. Gestión del oficial de seguridad (OS)	
6. Cuerpo de conocimiento	
7. Suscripción del código de ética de ISC2	

Realizada la evaluación, la Entidad Autorizadora queda en condición de pronunciarse sobre el cumplimiento de los requisitos y obligaciones necesarias para ser un PSC autorizado.

Si el PSC tiene calificaciones individuales C (CUMPLE) o S (SUFICIENTE), puede declararse su autorización, y dispondrá de un plazo de treinta días calendario para presentar la póliza de seguros. Para las calificaciones S, deberá haberse aprobado previamente un plan de medidas correctivas.

Si el PSC tiene alguna calificación I (INSUFICIENTE), la Entidad Autorizadora procederá a dictar una resolución en la que rechaza la solicitud de inscripción en el RPSC mencionando el o los requisitos que están en dicha condición.

BIBLIOGRAFÍA

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 del Congreso de la República de Guatemala.

ETSI TS 102 023 V1.2.1 (2003-01) Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.

FIPS PUB 140-1: Security Requirements for Cryptographic Modules, (Mayo 2001)

FIPS PUB 140-2: Security Requirements for Cryptographic Modules (Mayo 2002)

ISO 9001 Quality management systems – Requirements

ISO/IEC 18014-1:2002 Information technology -- Security techniques -- Time-stamping services.

ISO/IEC 27001:2005 Information Technology – Security Techniques. Information Security Management Systems. Requirements.

RFC 2560 X.509 Internet PKI Online Certificate Status Protocol - OCSP. June 1999.

RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

TIA-942 Telecommunications Infrastructure Standard for Data Centers (Abril 2005)

WebTrust for Certificate Authorities.

Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación (Publicado el 19 de julio del 2004 en el D.O.F.), de la República de México.

Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación (Publicadas el 10 de agosto del 2004 en el D.O.F.), de la República de México.

Ley sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Dicha Firma, Número 19799, de la República de Chile.

Reglamento de la Ley sobre Documentos Electrónicos, firma Electrónica y Servicios de Certificación de Dicha Firma, de la República de Chile.

Guía de Evaluación, Procedimiento de Evaluación de Prestadores de Servicios de Certificación, Ministerio de Economía, Fomento y Reconstrucción, Chile 2002.