Registro Digital Prisma

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN CPS

Código:	AD-DO-02
Versión:	6
Fecha de la versión:	15-04-2021
Nivel de confidencialidad:	0

Declaración de Prácticas de Certificación – CPS – de REGISTRO DIGITAL PRISMA

Impreso en la ciudad de Guatemala
Fecha de revisión: Abril 2021

Avenida Reforma 3-48 zona 9, Edificio Anel, Nivel 5 - Oficina 503

Attn: Desarrollos de Prácticas. Tel: (502) 2506-7070

Agradecimiento

REGISTRO DIGITAL PRISMA reconoce la ayuda de las personas especializadas en diversas áreas de negocios, derecho, política y tecnología, que revisaron el presente documento.

Tabla de contenido

CONSIDERACIONES PRELIMINARES:

PRIMERO: Que REGISTRO DIGITAL PRISMA, SOCIEDAD ANÓNIMA es una entidad constituida y organizada de conformidad con el ordenamiento jurídico de Guatemala y cuenta con los recursos económicos, financieros, la infraestructura técnica y administrativa, así como ha cumplido con todos los requisitos establecidos en el ordenamiento jurídico de Guatemala para proveer servicios de Certificación y por ende actuar legalmente como Autoridad de Certificación en Guatemala.

SEGUNDO: REGISTRO DIGITAL PRISMA SOCIEDAD ANÓNIMA se constituyó de conformidad con la escritura pública número treinta y uno (31) autorizada el quince de febrero del año dos mil ocho, por el Notario Manolo José Enríquez Rosales, la cual quedó debidamente inscrita en el Registro Mercantil General de la República de Guatemala al número 76460, folio 121 del libro 170 de Sociedades Mercantiles, la cual fue modificada mediante: **a)** la escritura Pública número doscientos dieciséis (216) autorizada en la ciudad de Guatemala, el 17 de noviembre del año 2008 por el Notario Manolo José Enríquez Rosales y **b)** mediante escritura Pública número ciento treinta (130) autorizada en la ciudad de Guatemala, el día veintitrés de agosto del año dos mil trece (2013) por el Notario Juan Carlos Díaz Monroy. Conforme a esta última escritura pública, su objeto social consiste en prestar de manera principal los siguientes servicios: *"…A) Proveer servicios de soluciones y de administración de seguridad de información para redes (incluyendo Internet) servidores, aplicaciones y computadoras de todo tipo; B) Proveer servicios de valuación de seguridad y vulnerabilidad, cumplimiento de políticas y detección de intruso; C) Actividades de los prestadores de servicios de certificación y seguridad en redes electrónicas incluyendo pero no limitando Internet, intranets, entre otras; emitir certificados en relación con las firmas electrónicas avanzadas de personas naturales o jurídicas, ya sea públicas o privadas, sean estas firmas electrónicas o digitales o cualquier otra índole (…)"*

TERCERO: REGISTRO DIGITAL PRISMA ha tomado la decisión de actuar como Prestador de Servicios de Certificación en Guatemala y se constituye como tercero en confianza, emitiendo, administrando y renovando certificados de firma electrónica avanzada, de acuerdo a las presentes normas y en estricto apego a la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala, su reglamento y sus actualizaciones, cumpliendo con lo establecido el ordenamiento jurídico de Guatemala, Guías de Evaluación, Inspecciones Periódicas, Políticas, parámetros establecidos en los principios de ISO 9001:2015, ISO 27001:2013 y otros estándares internacionales aplicables.

CUARTO: REGISTRO DIGITAL PRISMA, SOCIEDAD ANÓNIMA cuenta con las acreditaciones necesarias por los órganos o entidades correspondientes, según la normativa vigente.

QUINTO: REGISTRO DIGITAL PRISMA, SOCIEDAD ANÓNIMA es una entidad que ha cumplido con los requisitos y cuenta con la autorización por el Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía, según Resolución No. PSC-01-2014 de fecha 13 de agosto de 2014.

POR LO TANTO, se emiten las presentes normas de certificación en la versión vigente, las cuales una vez sean aprobadas por el Registro de Prestadores de Servicios de Certificación y luego publicadas en el sitio web www.prisma.gt entrarán en vigor de acuerdo a las siguientes disposiciones:

1. Introducción

La infraestructura de llave pública, conocida también por sus siglas en inglés PKI (Public Key Infraestructure) de REGISTRO DIGITAL PRISMA, es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas. REGISTRO DIGITAL PRISMA, como Prestador de Servicios de Certificación, ha delegado a su red de Distribuidores Autorizados, única y exclusivamente las funciones de comercialización y promoción de los certificados para firma electrónica avanzada, quedando vigentes e intactas, las responsabilidades y funciones de REGISTRO DIGITAL PRISMA como Autoridad de Registro y como Autoridad de Certificación. La identificación de los Distribuidores Autorizados por REGISTRO DIGITAL PRISMA, está publicada en el sitio web www.prisma.gt.

Este documento, establece las normas básicas que rigen la infraestructura de REGISTRO DIGITAL PRISMA, en adelante: "PKI de REGISTRO DIGITAL PRISMA "o simplemente "PKI". La Declaración de Prácticas de Certificación CPS establece los requerimientos del negocio, legales y técnicos para aprobar, emitir, administrar, utilizar, revocar y renovar los certificados de firma electrónica avanzada, dentro de la PKI de REGISTRO DIGITAL PRISMA y proporcionar servicios de confiabilidad asociados para todos sus participantes. Cualquier cambio y/o modificación a este documento, será notificado al Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía. Estos requerimientos protegen la seguridad e integridad y comprenden las reglas que se aplican a la PKI de REGISTRO DIGITAL PRISMA proporcionado con ellos la seguridad en niveles de confianza la cual es uniforme.

Estas CPS no consisten en un contrato legal entre REGISTRO DIGITAL PRISMA y los participantes de la PKI de REGISTRO DIGITAL PRISMA. Por lo tanto, REGISTRO DIGITAL PRISMA y los participantes de la PKI de REGISTRO DIGITAL PRISMA deberán suscribir sus propios contratos a fin de establecer sus propias condiciones, derechos y obligaciones.

Este documento está dirigido a:

- REGISTRO DIGITAL PRISMA, como prestador de servicios de certificación, quien deberá operar en los términos de las presentes Declaraciones de Prácticas de Certificación (CPS *por su siglas en inglés*) mismas que cumplen con los requerimientos establecidos por las CP.

- REGISTRO DIGITAL PRISMA, actuando como Autoridad de Registro -AR-; cuenta con sus propias prácticas o políticas de registro, así como sus propios procedimientos en la autenticación previa de los usuarios de certificados de las PKI de REGISTRO DIGITAL PRISMA, cuando sea aplicable.
- Los Suscriptores de certificados de REGISTRO DIGITAL PRISMA deberán entender; de qué manera están autenticados sus datos y documentos acreditativos y cuáles son sus obligaciones al respecto y como se protegen conforme las PKI de REGISTRO DIGITAL PRISMA.
- LA PARTE QUE CONFÍA son las personas quienes deberán estar conscientes sobre qué tanta confianza puede tener en un certificado de firma electrónica avanzada emitido con base a las PKI de REGISTRO DIGITAL PRISMA.

1.1. Presentación

Este documento constituye las normas para el proceso de certificación de REGISTRO DIGITAL PRISMA, al cual se hará referencia mediante el acrónimo de su denominación en inglés "*Certificate Practice Statement*" CPS, las cuales recogen los procedimientos en los que se basa REGISTRO DIGITAL PRISMA para la provisión de servicios de certificación en la emisión, renovación y revocación, así como en el mantenimiento de una PKI.

Las CPS son las disposiciones principales que regulan a REGISTRO DIGITAL PRISMA y establecen los requerimientos legales, técnicos y de negocio para la aprobación, emisión, uso, renovación y revocación de certificados de Firma Electrónica Avanzada. Asimismo, este documento detalla y concreta el proceso de certificación desde la instauración de REGISTRO DIGITAL PRISMA como Prestador de Servicios de Certificación, denominada en el presente documento indistintamente REGISTRO DIGITAL PRISMA o Autoridad de Certificación (AC); así como normar su actuar como Autoridad de Registro (AR) y la admisión de SUSCRIPTORES. En general, los servicios de certificación se refieren a la emisión, uso, renovación y revocación de certificados para Firma Electrónica Avanzada.

En las presentes CPS se asume que el lector conoce los conceptos de certificado, firma electrónica avanzada y PKI de REGISTRO DIGITAL PRISMA. En caso contrario, se recomienda al lector que consulte el glosario al final de este documento en el que se encuentran una serie de definiciones y conceptos, los cuales podrán servir tanto para la interpretación de las presentes normas como para la comprensión de los contratos que incluyen estas normas por referencia o que se relacionan con las mismas. Asimismo, el lector podrá encontrar información adicional relacionada con la PKI, Certificados de Firmas Electrónicas

Avanzadas e información relevante en la página de www.prisma.gt, o podrá solicitar una copia en soporte papel presentándose personalmente o por medio de una persona autorizada a REGISTRO DIGITAL PRISMA en sus oficinas ubicadas en Avenida Reforma, 3-48 zona 9, Edificio Anel 5to. Nivel Oficina 503, Ciudad de Guatemala, Guatemala; teléfono: (502) 2506-7070 (servicio al cliente) o al correo electrónico suscriptor@prisma.gt. REGISTRO DIGITAL PRISMA, notificará al Registro de Prestadores de Servicios de Certificación, cualquier cambio y/o modificación en la dirección de sus oficinas. EL LECTOR expresamente manifiesta que se le ha aconsejado recibir información adecuada en el uso de las técnicas de clave pública previamente a la solicitud de un certificado.

1.2. Ámbito de aplicación:

Estas CPS se aplican específicamente a:

1. REGISTRO DIGITAL PRISMA.
2. Certificados de Suscriptores.
3. Partes que confían

En general, las CPS también rigen el uso de los servicios de certificación provistos por REGISTRO DIGITAL PRISMA y todas las personas físicas y jurídicas que utilicen dichos servicios (quienes en conjunto podrán ser denominados los "PARTICIPANTES DE LA PKI DE REGISTRO DIGITAL PRISMA"). Por consiguiente, las CPS, como un solo documento, cubren las prácticas y procedimientos relativos a la emisión y administración de certificados de firma electrónica avanzada.

A. Papel de las CPS de REGISTRO DIGITAL PRISMA y otros documentos de prácticas

Las prácticas de certificación describen la infraestructura global del negocio, legal y técnica de la cadena de certificados que administra REGISTRO DIGITAL PRISMA. Estas CPS explican entonces las normas de las prácticas de certificación a los participantes de la PKI de REGISTRO DIGITAL PRISMA y explica las prácticas específicas de REGISTRO DIGITAL PRISMA en respuesta a las CP.

Específicamente, las CPS describen, entre otros:

1. Las obligaciones de las Autoridades de Registro, los SUSCRIPTORES dentro de la Infraestructura de Llave Pública –PKI- de REGISTRO DIGITAL PRISMA.
2. Las condiciones legales que se cubren en el contrato de los SUSCRIPTORES dentro de la PKI de REGISTRO DIGITAL PRISMA.

3. Auditorías internas y revisiones relacionadas en materia de seguridad y prácticas que se realicen por parte de REGISTRO DIGITAL PRISMA y sus participantes como PKI.
4. Métodos usados dentro de la PKI de REGISTRO DIGITAL PRISMA para confirmar la identidad de los solicitantes de cada tipo de certificado.
5. Procedimientos operativos para los servicios de ciclo de vida de cada certificado que se emiten en la PKI de REGISTRO DIGITAL PRISMA: solicitudes, emisión, aceptación, renovación y revocación de certificados.
6. Lineamientos de seguridad operativa para registro de auditorías internas, retención de registros y recuperación de desastres que se usan dentro de la PKI de REGISTRO DIGITAL PRISMA.
7. Manejo de seguridad física, de personal, de administración de la clave y logística de los participantes de la PKI de REGISTRO DIGITAL PRISMA.

B. Antecedentes relativos a Certificados Digitales de REGISTRO DIGITAL PRISMA

Este documento asume que el lector conoce de los temas relacionados con criptografía de clave pública, certificados, firmas electrónicas avanzadas en general; y en particular con la PKI de REGISTRO DIGITAL PRISMA. De lo contrario REGISTRO DIGITAL PRISMA aconseja que el lector obtenga capacitación en el uso de la criptografía de claves públicas y de la PKI y la forma en la que lo implementa REGISTRO DIGITAL PRISMA.

C. Cumplimiento con las normas aplicables

Las prácticas que se indican en estas CPS tienen el propósito de cumplir o superar los requisitos de las normas industriales generalmente aceptadas y en desarrollo, incluyendo el Programa WebTrust AICPA/CICA WebTrust o ISO 27001 para las Autoridades de Certificación, ANS X9.79:2001 PKI Practices and Policy Framework (Marco General de Prácticas y Políticas de la Infraestructura de Claves Públicas 2001) y otras normas de la industria relacionadas con la operación de La Autoridad de Certificación.

1.2.1 Compendio de política

REGISTRO DIGITAL PRISMA ofrecerá los certificados cuyos estándares y políticas basado en lo descrito en las CP. Los certificados ofrecen una función de seguridad y corresponden a un nivel específico de confianza.

Los Certificados que emite REGISTRO DIGITAL PRISMA ofrecen el nivel más alto de garantías dentro de la PKI de REGISTRO DIGITAL PRISMA. Los Certificados de Firma Electrónica Avanzada se emiten a Personas Jurídicas y Personas Individuales, éstas últimas se subdividen en: Certificados para persona individual, representantes legales de entidades privadas, persona individual relacionada con una entidad, persona individual profesional titulada y persona individual que es funcionario público.

Los certificados de firma electrónica avanzada de persona jurídica y persona individual (persona individual simple, profesional titulado, en relación con entidad, funcionario público, representante legal), se pueden usar no solo para firmar, sino también para encripción y control de acceso, incluyendo como prueba de identidad, en las transacciones de alto valor, entre otras. Los Certificados de Persona Individual ofrecen garantías de la identidad del SUSCRIPTOR porque el proceso de autenticación que lleva a cabo REGISTRO DIGITAL PRISMA como Autoridad de Registro, utilizará como base de criterio de seguridad la presencia personal (física) del SUSCRIPTOR ante sí o ante notario, por medio de una sesión de videoconferencia asistida con el Operador PKI para realizar la correspondencia de la información o por medio de una validación no asistida por medio de la aplicación proveída por REGISTRO DIGITAL PRISMA además de que el propio SUSCRIPTOR deba presentar en el proceso de autenticación, una forma bien reconocida de identificación expedida por el gobierno de la República de Guatemala y otro documento con el cual se acredite su identidad o calidad. El SUSCRIPTOR tiene derecho de usar el nombre de dominio que está anotado en la Solicitud de Certificado.

Los certificados de persona jurídica ofrecen garantías de la identidad de los SUSCRIPTORES con base a la comprobación de que el SUSCRIPTOR existe en realidad, es decir que la persona jurídica se encuentra válidamente constituida y registrada de conformidad con el ordenamiento jurídico de Guatemala, y que el representante legal se encuentra plenamente facultado y autorizado por la persona jurídica para solicitar el certificado de firma electrónica avanzada. Para las personas jurídicas legalmente constituidas en el extranjero podrán obtener certificados para personas jurídicas, dichos certificados únicamente ofrecen garantía de que el suscriptor o persona jurídica constituida en el extranjero cuenta con un representante legal o apoderado debidamente acreditado en la República de Guatemala y que dicha entidad se encuentra inscrita en el Registro Mercantil de la República de Guatemala –en los casos que la ley así lo exija-; y que cuenta con los documentos que pasaron los pases de ley en la República de Guatemala y mediante los cuales se acredita que la persona está legalmente constituida en el extranjero y que los documentos con los que acredita dicho extremo pasaron por los trámites de ley para surtir efectos en la República de Guatemala .

Las especificaciones de certificados en las CP, como se resumen en estas CPS, establecen el nivel mínimo de garantías necesarias con las cuales debe de contar un Certificado. Por ejemplo, cualquier Certificado emitido conforme a la PKI de REGISTRO DIGITAL PRISMA puede usarse para firmas electrónicas avanzadas, así como la encripción y control de acceso, cuando es necesario comprobar la identidad; es decir, para solicitudes que requieren un alto nivel de garantía. No obstante, por contrato o dentro de ambientes específicos (como el ambiente entre personas jurídicas), los participantes de la PKI de REGISTRO DIGITAL PRISMA pueden usar los procedimientos de validación más fuertes de los regulados o establecidos dentro de las CP y de estas CPS. Sin embargo, dicho uso estará limitado a las personas jurídicas y estas serán las únicas responsables por daños, perjuicios o cualquier responsabilidad que cause dicho uso.

i. Programa afiliado de CA

REGISTRO DIGITAL PRISMA es un prestador de servicios de certificación, lo cual significa que puede aprobar o rechazar solicitudes de Certificados. Estos prestadores de servicios llevan a cabo funciones de validación para aprobar o rechazar solicitudes de certificados de firma electrónica avanzada, para identificación de personas físicas o jurídicas. REGISTRO DIGITAL PRISMA como AC, ha establecido un alojamiento seguro para sus instalaciones, incluyendo éstas, los sistemas de AC/AR, así como los módulos criptográficos que tienen las claves privadas que se usan para la emisión de certificados. REGISTRO DIGITAL PRISMA funge a la vez, con los roles de una AC y de una AR y por tanto, lleva a cabo todos los servicios de ciclo de vida del certificado: emisión, renovación y revocación de los mismos.

1.3. Comunidad y aplicabilidad

La comunidad que rige estas CPS en la PKI de REGISTRO DIGITAL PRISMA, aloja un gran número de participantes con diversas necesidades de comunicaciones e información segura. La PKI de REGISTRO DIGITAL PRISMA está regida por estas CPS.

1.3.1.Prestadores de servicios de certificación

El término PRESTADOR DE SERVICIOS DE CERTIFICACIÓN -PSC-, es un término general que se refiere a todas las entidades que emiten certificados y pueden prestar otros servicios relacionados con las firmas electrónicas avanzadas comprendidos en la ley guatemalteca.

Cada Prestador de Servicios de Certificación es una entidad que tiene autorización para emitir Certificados. Los Prestadores de Servicios de Certificación que emiten Certificados a SUSCRIPTORES deberán cumplir con las disposiciones de las CP. Los recipientes de certificados dentro de la PKI de REGISTRO DIGITAL PRISMA, caen en cuatro categorías: (1) REGISTRO DIGITAL PRISMA mismo, (2) Autoridad de Registro (AR) de REGISTRO DIGITAL PRISMA, (3) Autoridad Certificadora (AC) de REGISTRO DIGITAL PRISMA y (4) los Suscriptores de REGISTRO DIGITAL PRISMA .

REGISTRO DIGITAL PRISMA lleva a cabo todas las funciones de la AC y AR dentro de la PKI.

1.3.2.Autoridad de Registro

Dentro de la PKI de REGISTRO DIGITAL PRISMA, la Autoridad de Registro es la propia REGISTRO DIGITAL PRISMA.

La Autoridad de Registro AR ayuda a la AC al realizar funciones de confirmación de la identidad, aprobación o rechazo de Solicitudes de Certificados, aprobación o rechazo de solicitudes de renovación y solicitudes de revocación de Certificados.

1.3.3.Suscriptores

El cuadro a continuación muestra los tipos de SUSCRIPTORES para cada tipo de Certificado que ofrece REGISTRO DIGITAL PRISMA, como Prestador de Servicios de Certificación.

SUJETO	***TIPO DE CERTIFICADO***
PERSONAS INDIVIDUALES	INDIVIDUAL PROFESIONAL TITULADO FUNCIONARIO PÚBLICO EN RELACIÓN CON ENTIDAD REPRESENTANTE LEGAL
PERSONAS JURÍDICAS	LA PERSONA JURÍDICA -ENTIDAD- A QUIEN SE EMITE EL CERTIFICADO.

1.3.4.Aplicabilidad

Estas CPS se aplican a todos los participantes de la PKI de REGISTRO DIGITAL PRISMA, incluyendo a REGISTRO DIGITAL PRISMA propiamente dicha, SUSCRIPTORES Y PARTES QUE CONFÍAN.

Estas CPS se aplican a la PKI de REGISTRO DIGITAL PRISMA y describe las prácticas que rigen el uso de sus certificados.

i. Aplicaciones adecuadas

Los certificados de persona individual y los certificados de persona jurídica, permiten que LAS PARTES QUE CONFÍAN verifiquen las firmas electrónicas avanzadas correspondientes a cada certificado. Los participantes de la PKI de REGISTRO DIGITAL PRISMA reconocen y aceptan que, en la medida en que lo permitan las leyes, cuando se necesite que una transacción sea por escrito, mensaje de datos u otro registro que lleve una firma electrónica avanzada verificable mediante un certificado, es válido, efectivo y exigible en un grado no inferior al grado que tendría si dicho mensaje o registro hubiera sido escrito y firmado en papel. Sujeta a las leyes aplicables, la firma electrónica avanzada, cuando se utiliza en una transacción que se lleve a cabo con referencia a un certificado, será efectiva no importa la ubicación geográfica en la que se emita el certificado o se cree o use la firma electrónica avanzada, y no importa la ubicación geográfica del domicilio social de la AC o del SUSCRIPTOR.

1.4. Uso de Certificado

1.4.1.Usos apropiados del Certificado

i. **Certificados expedidos a personas individuales:**

Los Certificados extendidos a personas individuales, son emitidos para ser utilizados por las personas naturales o individuales para firmar –mediante firma electrónica avanzada-, utilizar firma electrónica avanzada desde token o HSM en la nube y encriptar documentos; así como correos electrónicos que permitan la utilización de certificados y para autenticar las solicitudes (autenticación de clientes). La PARTE QUE CONFÍA puede razonablemente confiar en el certificado de persona individual y en que el uso de este no esté prohibido por la ley, por estas CPS, por la CP conforme a la cual el certificado haya sido expedido y de conformidad con el contrato del suscriptor vigente.

ii. **Certificados expedidos a personas jurídicas:**

Los Certificados de Personas Jurídicas, son expedidos después de que se verifica y se comprueba que la entidad se encuentra legalmente constituida ya sea en la República de Guatemala o el extranjero mediante los documentos acreditativos y que las características incluidas en el certificado son verídicas excluyendo información del Suscriptor no verificado, como por ejemplo: la titularidad de un dominio de Internet o correo electrónico. No es la intención de estas CPS limitar los tipos de usos de los certificados

de personas jurídicas. La PARTE QUE CONFÍA puede razonablemente confiar en que los certificados de personas jurídicas, siempre y cuando su uso no esté prohibido por la ley, por estas CPS, por cualquier CP bajo la cual el Certificado haya sido expedido y conforme a cualquier contrato con Suscriptores que esté vigente.

1.4.2.Usos prohibidos del Certificado

Los certificados se utilizarán únicamente en la medida en que el uso sea permitido de conformidad con el ordenamiento jurídico de la República de Guatemala o el que le sea aplicable si es utilizado en el extranjero.

Todos los tipos y clases de certificado emitidos de conformidad con la PKI de REGISTRO DIGITAL PRISMA, no están diseñados, no tienen el propósito, no están autorizados y por ende no podrán ser utilizados para su utilización como equipo de control en circunstancias peligrosas, para usos que requieran desempeño de error-seguridad, tales como las operaciones de instalaciones nucleares, navegación aérea o sistemas de comunicación, sistemas de control de tráfico aéreo o sistemas de control de armas, donde una falla podría llevar directamente a la muerte, lesiones corporales o a daño ambiental grave. Los certificados de persona individual son para las aplicaciones de los usuarios individuales o personas naturales y no se utilizarán como de personas jurídicas (certificados de persona jurídica) ni certificados que tengan otros propósitos, como certificados de AC o AR. Los certificados AC no podrán ser utilizados para ninguna función excepto funciones de AC y los certificados AR podrán ser únicamente utilizados para funciones de AR.

i. Solicitudes restringidas

En general, los certificados emitidos por REGISTRO DIGITAL PRISMA son certificados para fines múltiples. Los certificados pueden usarse globalmente y para interactuar con diversas partes que confían en todo el mundo. Este uso es permitido y los clientes que utilizan certificados dentro de su ambiente laboral o para los fines que fueron obtenidos los certificados, pueden ponerle más restricciones al uso del certificado dentro de estos ambientes o situaciones especiales. Sin embargo, REGISTRO DIGITAL PRISMA y otros participantes de la PKI de REGISTRO DIGITAL PRISMA no son responsables de supervisar ni de hacer cumplir esas restricciones en estos ambientes.

Asimismo, los certificados del SUSCRIPTOR o usuario final no se usarán como certificados de AC y en consecuencia, el SUSCRIPTOR o usuario final, no podrá atribuirse en el uso de tal certificado, facultades

como Prestador de Servicios de Certificación sin la autorización previa del RPSC. En forma general, se puede indicar que los certificados se usarán sólo en la medida en que el uso sea congruente con las leyes aplicables.

ii. Aplicaciones prohibidas

Los certificados no están diseñados, destinados ni autorizados para utilizarse o revenderse como un equipo de control en circunstancias peligrosas, ni para usos que requieran desempeño a prueba de fallas, en donde una falla podría dar como resultado directamente la muerte, una lesión personal o un grave daño al ambiente.

1.5. Detalles del contacto

1.5.1.Persona Jurídica de la administración de especificaciones

La persona jurídica que administra estas CPS es REGISTRO DIGITAL PRISMA, SOCIEDAD ANÓNIMA, mediante su propio grupo de Desarrollo de Prácticas de REGISTRO DIGITAL PRISMA. Las preguntas al grupo de Desarrollo de Prácticas de REGISTRO DIGITAL PRISMA deben dirigirse a los siguientes datos de contacto:
REGISTRO DIGITAL PRISMA, SOCIEDAD ANÓNIMA.
DIRECCIÓN DE EMAIL – suscriptor@prisma.gt

1.5.2.Persona de contacto

Desarrollo de Prácticas – CPS dirección. suscriptor@prisma.gt

1.5.3.Persona que determina la adecuación de las CPS a la política

El Gerente General de REGISTRO DIGITAL PRISMA determina la adecuación y la aplicabilidad de estas CPS.

1.5.4.Procedimiento de aprobación de CPS

La aprobación de estas CPS, así como cualquier cambio y/o modificación posterior, serán notificadas al Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía y se harán mediante el procedimiento establecido en estas CPS, para su aprobación final. Las modificaciones se harán, ya sea en el formato de un documento que contenga la versión modificada de las CPS, o mediante un aviso de actualización. Las versiones modificadas o las actualizaciones serán asociadas a la sección de actualizaciones de prácticas y avisos de la biblioteca de REGISTRO DIGITAL PRISMA ubicado en la página www.prisma.gt. Las actualizaciones reemplazan cualquier disposición designada o en conflicto de la

versión referenciada de la CPS.

1.6. Definición de acrónimos

Véase el anexo que contiene el glosario y los acrónimos en el punto 9 de este documento.

2. Disposiciones generales

2.1. Obligaciones

REGISTRO DIGITAL PRISMA es responsable de mantener un sitio centralizado donde se almacena y mantiene información digital, bases de datos o archivos informáticos en línea, públicamente accesible, relacionada a sus certificados incluyendo la revocación de certificados.

2.1.1.Obligaciones de REGISTRO DIGITAL PRISMA, como Autoridad de Certificación (AC)

- Cumplir con la Declaración de Prácticas de Certificación y con los contratos realizados con los Suscriptores y partes que confían.
- Informar al Suscriptor las características de la prestación del servicio, los límites de responsabilidad, y las obligaciones que asume como interviniente en el proceso de certificación. En particular REGISTRO DIGITAL PRISMA deberá informar al suscriptor o terceras personas que lo soliciten, sobre el tiempo y recursos computacionales requeridos para validar la firma electrónica avanzada que se efectúa con los certificados que emite a sus suscriptores.
- Comprobar la información definida en esta Declaración de Prácticas de Certificación como verificable para la emisión de certificados.
- Abstenerse de acceder o almacenar la clave privada del Suscriptor.
- Permitir y facilitar la realización de las auditorías por parte del Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía.
- Emitir certificados de conformidad con lo establecido en la sección de procedimiento de emisión de certificados de estas CPS, y las especificaciones acordadas por el Suscriptor en el contrato de suscripción.
- Publicar en su Repositorio o base de datos de certificados electrónicos expedidos y llevar el Registro de Firmas electrónicas avanzadas.

- Informar al Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía de cualquier evento establecido en las CPS, que comprometa la prestación del servicio.
- Mantener el control y confidencialidad de su clave privada y establecer las seguridades razonables para que no se divulgue o comprometa.
- Procurar diligentemente la prestación permanente e ininterrumpida de los servicios de certificación.
- Permitir el acceso de los Suscriptores y de terceros a esta Declaración de Prácticas de Certificación y al repositorio de REGISTRO DIGITAL PRISMA.
- Actualizar la Base de datos de certificados revocados contenida en el repositorio en los términos establecidos en estas CPS y efectuar los avisos y publicaciones que se establezcan por ley en ésta.
- Revocar los certificados que se requiera de conformidad con lo establecido en estas CPS.
- Informar al Suscriptor, dentro de las 24 horas hábiles siguientes, la revocación de su certificado de acuerdo con la normativa vigente.
- Disponer de una línea telefónica de atención a Suscriptores y terceros, que permita las consultas y la pronta solicitud de revocación de certificados por los Suscriptores.
- Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con los certificados de las firmas electrónicas avanzadas emitidas y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración.
- Conservar física o electrónicamente la documentación que respalda los certificados emitidos, por el término previsto en la ley con el objeto de garantizar la integridad y la confidencialidad que le sean propias.
- Atender las peticiones, quejas y reclamos hechas por los suscriptores, de conformidad con lo establecido en estas CPS.
- Cumplir con las instrucciones que establezca el Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía a través de sus disposiciones en la guía de evaluación del Registro de Prestadores de Servicios de Certificación (RPSC) para la firma electrónica avanzada, en su versión vigente.
- Advertir, sobre las medidas de seguridad que deben observar los suscriptores de firmas electrónicas para la utilización de estos mecanismos.

De conformidad con la normativa guatemalteca vigente, REGISTRO DIGITAL PRISMA cuenta con una línea telefónica y sistemas que permiten la atención al cliente con relación a las peticiones, quejas y reclamos de los suscriptores, de las PARTES QUE CONFÍAN y de los terceros.

El cumplimiento de todas o parte de las obligaciones o procedimientos de emisión de certificados, o de la prestación en general del servicio de certificación, será realizado en forma directa por REGISTRO DIGITAL PRISMA como AC.

REGISTRO DIGITAL PRISMA, en su calidad de AC, lleva a cabo las obligaciones específicas para tal rol que aparecen a través de estas CPS.

Asimismo, REGISTRO DIGITAL PRISMA hace un esfuerzo razonable para garantizar que los contratos del SUSCRIPTOR y los contratos de la PARTE QUE CONFÍA obliguen a los SUSCRIPTORES y a LAS PARTES QUE CONFÍAN dentro de las PKI del REGISTRO DIGITAL PRISMA. Ejemplos de este empeño son, de manera enunciativa y no limitativa, la exigencia de la aceptación de un contrato del SUSCRIPTOR como condición de la inscripción o la exigencia de la aceptación mediante la visita al sitio www.prisma.gt o la simple lectura del contrato de la PARTE QUE CONFÍA, como condición para recibir la información del estado del certificado.

2.1.2.Obligaciones de REGISTRO DIGITAL PRISMA como AR

REGISTRO DIGITAL PRISMA, actúa como AR, realizando funciones de validación, aprobando o rechazando solicitudes de Certificado, aprobando solicitudes de renovación y solicitando la revocación de Certificados presentadas por el solicitante Suscriptor, a través de los Distribuidores Autorizados por REGISTRO DIGITAL PRISMA, a quienes se ha delegado, única y exclusivamente, las funciones de comercialización y promoción de los certificados para firma electrónica avanzada, quedando vigentes e intactas, las responsabilidades y funciones de REGISTRO DIGITAL PRISMA como Autoridad de Registro y como Autoridad de Certificación. Las anteriores, son funciones que no han sido delegadas a los Distribuidores Autorizados. Por lo anteriormente mencionado, ningún Distribuidor Autorizado podrá atribuirse a sí mismo, las funciones que como AC y AR corresponden a REGISTRO DIGITAL PRISMA.

Asimismo, REGISTRO DIGITAL PRISMA, actuando como AR, garantiza que el contrato del SUSCRIPTOR y el contrato de la PARTE QUE CONFÍA obliguen a todos los SUSCRIPTORES y a todas las PARTES QUE CONFÍAN dentro la PKI de REGISTRO DIGITAL PRISMA, de acuerdo con el apartado 2.1.1 de la CPS.

REGISTRO DIGITAL PRISMA, en su calidad de AR, lleva a cabo las obligaciones específicas para tal rol que aparecen a través de estas CPS.

2.1.3.Obligaciones del suscriptor

Las obligaciones del SUSCRIPTOR en las CP se aplican a los SUSCRIPTORES dentro de la PKI de REGISTRO DIGITAL PRISMA, a través de estas CPS, mediante los Contratos del SUSCRIPTOR –"CONTRATO DEL SOLICITANTE SUSCRIPTOR"- aprobados por REGISTRO DIGITAL PRISMA. El contrato del SUSCRIPTOR en vigor dentro de la PKI de REGISTRO DIGITAL PRISMA aparece publicado en www.prisma.gt. Dentro de la PKI de REGISTRO DIGITAL PRISMA, el contrato del SUSCRIPTOR requiere que los Solicitantes del Certificado ofrezcan información completa y precisa sobre sus solicitudes de certificado y manifiesten su consentimiento al contrato del SUSCRIPTOR aplicable, como condición para obtener un certificado. Al Contrato del SUSCRIPTOR serán aplicables las obligaciones específicas que aparecen en las CP y en las CPS a los SUSCRIPTORES de la PKI de REGISTRO DIGITAL PRISMA. El contrato de SUSCRIPTOR establece como obligación que la misma persona del suscriptor, sea quien exclusivamente use su certificado.

También exige que los SUSCRIPTORES protejan sus claves privadas de acuerdo con lo establecido a estas CPS. Conforme a al contrato de SUSCRIPTOR, si un SUSCRIPTOR descubre o tiene motivos para creer que ha habido un compromiso de la clave privada del SUSCRIPTOR o de los datos de activación que protegen dicha clave privada (si fuera aplicable, cuando cuente con los datos de activación de la clave privada), o la información del certificado es incorrecta o ha cambiado, el SUSCRIPTOR de inmediato debe:

1. Notificar a la entidad que aprobó la solicitud del certificado del SUSCRIPTOR, es decir, a REGISTRO DIGITAL PRISMA.
2. Acudir a REGISTRO DIGITAL PRISMA para recibir apoyo y la asesoría necesaria.

El contrato del SUSCRIPTOR exige que los SUSCRIPTORES dejen de usar sus claves privadas al final de sus períodos de uso de la clave.

Los SUSCRIPTORES además de las obligaciones ya mencionadas se obligan a lo siguiente:

- Utilizar la clave privada y el certificado emitido, única y exclusivamente para los fines establecidos y de acuerdo con las condiciones establecidas en el contrato; así como conforme a las condiciones del contrato celebrado con él de manera individual y en estas CPS.

- Usar el certificado para firmar mensajes de datos, explicando a las partes que confían bajo qué calidad se está firmando.
- El mensaje de datos o documento electrónico que el SUSCRIPTOR firma con su firma electrónica avanzada mediante el uso de un certificado emitido por REGISTRO DIGITAL PRISMA determina el contexto de la calidad en que está firmando.
- Responder por la custodia de la clave privada y de su soporte físico (si aplica) evitando su pérdida, revelación, modificación o uso no autorizado. Especialmente, el suscriptor deberá abstenerse, sin importar la circunstancia, de anotar en el soporte físico del certificado el código de activación de claves (si fuere aplicable el código de activación o las claves privadas, ni tampoco en cualquier otro documento que el suscriptor conserve o transporte consigo o con el soporte físico.
- Solicitar la revocación del certificado que le ha sido entregado cuando se cumpla alguno de los supuestos previstos para la revocación del certificado.
- Abstenerse de revelar la clave privada o el código de activación del certificado así como abstenerse de delegar su uso a terceras personas.
- Asegurarse de que toda la información contenida en el certificado es verdadera y notificar inmediatamente a REGISTRO DIGITAL PRISMA en caso de que se haya incluido cualquier información incorrecta o inexacta o en caso de que por alguna circunstancia posterior la información del certificado no corresponda con la realidad.
- Asimismo, deberá comunicar de manera inmediata el cambio o variación que haya sufrido cualquiera de los datos que el Suscriptor proporcionó a REGISTRO DIGITAL PRISMA, para la emisión del certificado.
- Informar inmediatamente a REGISTRO DIGITAL PRISMA a la cuenta de correo electrónico suscriptor@prisma.gt o cualquier medio escrito, acerca de cualquier situación que pueda afectar la confiabilidad del certificado e iniciar el procedimiento de revocación del certificado cuando sea necesario. Especialmente, deberá notificar de inmediato la pérdida, robo o falsificación del soporte físico y cualquier intento de realizar estos actos sobre el mismo, así como el conocimiento por otras personas del código de activación o de las claves privadas, solicitando la revocación del certificado de conformidad con el procedimiento que se establece en las CPS.
- Destruir el soporte físico cuando así lo exija REGISTRO DIGITAL PRISMA en el momento en que haya sido sustituido por otro con los mismos fines o cuando termine el período del servicio adquirido del certificado con REGISTRO DIGITAL PRISMA siguiendo en todo caso las instrucciones de éste.

- Respetar los derechos de propiedad industrial e intelectual de REGISTRO DIGITAL PRISMA y de terceras personas en la solicitud y en el uso del certificado.
- REGISTRO DIGITAL PRISMA, a su leal saber y entender y siempre y cuando no haya sido incluido por el propio SUSCRIPTOR, no incluirá información del certificado cuya inserción pueda constituirse de alguna forma, en violación de los derechos de propiedad intelectual o industrial de REGISTRO DIGITAL PRISMA y/o de terceras personas.
- Cualquier otra que se derive de la ley, del contenido de estas CPS, Política de Certificación CP o cualquier otro documento relacionado.
- Abstenerse de monitorear, alterar, realizar ingeniería inversa o interferir en cualquier otra forma la prestación de servicios de certificación.

2.1.4.Obligaciones de la parte que confía

Cuando una tercera persona confía en un certificado está aceptando usar el sistema de PKI en su integridad y por tanto acepta regirse por las normas establecidas para el mismo, las cuales se encuentran contenidas en estas CPS y en las CP.

Las obligaciones de LA PARTE QUE CONFÍA son enunciativas, pero no limitativas las siguientes:

- Verificar la confiabilidad del certificado revisando especialmente que éste no se encuentre en la base de datos de certificados revocados de REGISTRO DIGITAL PRISMA. La confiabilidad de certificado deberá en todo caso ceñirse a lo establecido en la sección de confiabilidad de las firmas y los certificados.
- Aceptar y reconocer a los certificados solamente el uso que se permite darles de conformidad con lo establecido en la sección de uso de los certificados.
- Conocer con detenimiento y cumplir en todo momento las presentes CPS en la utilización de las firmas electrónicas avanzadas y los certificados de REGISTRO DIGITAL PRISMA.
- En especial la PARTE QUE CONFÍA deberá tener presente y actuar en todo momento de acuerdo con las limitaciones de responsabilidad y garantías que ofrece REGISTRO DIGITAL PRISMA.
- Informar a REGISTRO DIGITAL PRISMA de cualquier irregularidad o sospecha de la misma que se presente en la utilización de los certificados de las PKI de REGISTRO DIGITAL PRISMA.
- Abstenerse de monitorear, alterar, realizar ingeniería inversa o interferir en cualquier otra forma la prestación de servicios de certificación.

El contrato de la PARTE QUE CONFÍA dentro de la PKI de REGISTRO DIGITAL PRISMA incluirá una declaración en la que se establece: "*que antes de cualquier acto de confianza, LAS PARTES QUE CONFÍAN deben evaluar independientemente la conveniencia de uso de un certificado para cualquier fin determinado y decidir que el certificado, de hecho, se usará para este fin*". Asimismo, en ese contrato se incluirá una cláusula en la que se establece que REGISTRO DIGITAL PRISMA, como AC, ni como AR, es responsable de evaluar la conveniencia de uso de un certificado.

El contrato de la PARTE QUE CONFÍA incluye una cláusula en la que se establece que específicamente LAS PARTES QUE CONFÍAN no les darán otro uso a los certificados, más allá de lo especificado dentro de las presentes CPS.

En el contrato de la PARTE QUE CONFÍA se establece que LAS PARTES QUE CONFÍAN deben utilizar el software y/o hardware apropiado para llevar a cabo la autentificación de la firma electrónica avanzada y otras operaciones de código (criptográficas) que desee llevar a cabo. Dichas operaciones comprenden la identificación y verificación de la jerarquía de la cadena de certificados. Conforme a éste contrato, LAS PARTES QUE CONFÍAN no deben confiar en un certificado, a menos que estos procedimientos de verificación tengan éxito.

El contrato de la PARTE QUE CONFÍA también exige que LAS PARTES QUE CONFÍAN comprueben el estado de un certificado en el que desean confiar, al igual que todos los certificados de su cadena de certificados. Si alguno de los certificados de la cadena de certificados fue revocado de acuerdo con el contrato de la PARTE QUE CONFÍA, la PARTE QUE CONFÍA no debe confiar en el certificado que fue revocado; ni en ninguno otro que fuere revocado de la cadena de certificados.

El contrato de la PARTE QUE CONFÍA incluye una declaración en la que se establece que la aceptación de sus términos es condición para usar o de otro modo confiar en los certificados. Las PARTES QUE CONFÍAN que también son SUSCRIPTORES convienen en estar obligadas por los términos del contrato de la PARTE QUE CONFÍA.

El contrato de la PARTE QUE CONFÍA contiene una declaración que indica que si todas las verificaciones tienen éxito, la PARTE QUE CONFÍA tiene derecho de confiar en el certificado, siempre y cuando la confianza en el certificado sea razonable de acuerdo con las circunstancias. Si las circunstancias indican la necesidad de garantías adicionales, la PARTE QUE CONFÍA debe obtener dichas garantías para que la citada

confianza se considere razonable.

El contrato de la PARTE QUE CONFÍA establece una declaración en el que LAS PARTES QUE CONFÍAN no deben supervisar, invertir, ni interferir con la ingeniería de la implementación técnica del sistema de certificados de REGISTRO DIGITAL PRISMA, salvo mediante previa aprobación por escrito de REGISTRO DIGITAL PRISMA.

2.1.5.Obligaciones de repositorio

REGISTRO DIGITAL PRISMA es el responsable de las funciones de repositorio. REGISTRO DIGITAL PRISMA publica los certificados que emite en el repositorio que se establece y de acuerdo con el artículo 2.6 de éstas CPS.

A la revocación del Certificado del SUSCRIPTOR de un usuario final, REGISTRO DIGITAL PRISMA publica el aviso de dicha revocación en el repositorio y emitirá CRL dentro de su PKI. Asimismo, los clientes pueden usar el protocolo del estado del certificado en línea ("OCSP", por sus siglas en inglés) de REGISTRO DIGITAL PRISMA.

2.2. Responsabilidad

2.2.1.Responsabilidad de la Autoridad de Certificación

Las disposiciones que establecen responsabilidad, las cláusulas de exclusión y limitación de responsabilidad entre REGISTRO DIGITAL PRISMA, y los participantes de la PKI de REGISTRO DIGITAL PRISMA, se establecen en los contratos celebrados entre ellos respectivamente.

Las prácticas de REGISTRO DIGITAL PRISMA relativas a las garantías, cláusulas de exclusión de garantía y limitaciones en el contrato de la PARTE QUE CONFÍA, se aplican a REGISTRO DIGITAL PRISMA. Es importante que los términos aplicables a LAS PARTES QUE CONFÍAN también se incluyan en el contrato del SUSCRIPTOR, además del contrato de la PARTE QUE CONFÍA, pues los SUSCRIPTORES a menudo fungen también como PARTES QUE CONFÍAN.

i. Garantías de la Autoridad de Certificación para los suscriptores y las partes que confían

Los contratos celebrados con REGISTRO DIGITAL PRISMA comprenderán una serie de derechos y obligaciones orientadas a garantizar a LOS SUSCRIPTORES Y LAS PARTES QUE CONFIAN, como son entre otras las siguientes:

- Que el SUSCRIPTOR proporcionará información verdadera y válida, por ende el certificado no contiene declaraciones falsas, que se conozcan o se deriven de las entidades que aprueban la solicitud del certificado o emitan el certificado;
- Que no hay errores en la información del certificado que introdujeron las entidades que aprueban la solicitud de certificado o que emiten el certificado, debido a que no se puso el debido cuidado en el manejo de la solicitud del certificado o la creación del certificado;
- Que sus certificados cubren todos los requisitos de estas CPS;
- Que los servicios de revocación y el uso de un repositorio se conforman con estas CPS en todos los aspectos;
- Los contratos de la LA PARTE QUE CONFIA de REGISTRO DIGITAL PRISMA contienen una garantía para las PARTES QUE CONFIAN razonablemente en un certificado, de que:
    - Toda la información que contiene dicho certificado o que se incorpora en él mediante referencia, salvo por la información del SUSCRIPTOR no verificada, es exacta;
    - Con respecto a los certificados que aparecen en el repositorio de REGISTRO DIGITAL PRISMA, que el certificado fue emitido a la persona individual o persona jurídica que se nombre en el certificado como SUSCRIPTOR, y que el SUSCRIPTOR ha aceptado el certificado, de acuerdo con el apartado 4.3 de la CPS, y que las entidades que aprueban la solicitud de certificado y emiten el certificado han cumplido sustancialmente con estas CPS cuando emiten el certificado.

ii. Cláusulas de exclusión de garantías de la Autoridad de Certificación

El contrato del SUSCRIPTOR de REGISTRO DIGITAL PRISMA como el contrato de la PARTE QUE CONFÍA publicado en la página web de Registro Digital Prisma www.prisma.gt , incluirá cláusulas en las que no se harán responsables y por lo tanto no garantizarán la comerciabilidad o conveniencia para un fin en particular de los servicios que preste.

iii. Limitaciones de responsabilidad de la Autoridad de Certificación

En la medida en que lo permitan las leyes aplicables, en el contrato del SUSCRIPTOR de REGISTRO DIGITAL PRISMA se establecen los límites de responsabilidad aplicables a sus servicios. Las

limitaciones de responsabilidad incluyen pero no se limitan a daños indirectos, especiales, incidentales y consecuenciales. REGISTRO DIGITAL PRISMA, S.A., cumpliendo con lo requerido por la ley, ha contratado un Seguro de Responsabilidad Civil solicitado por el Registro de Prestadores de Servicio de Certificación (RPSC) del Ministerio de Economía de Guatemala.

iv. Fuerza mayor

De conformidad con la ley aplicable, el contrato del SUSCRIPTOR de REGISTRO DIGITAL PRISMA y el contrato de las PARTES QUE CONFÍAN comprenderán una cláusula que regula las causas de fuerza mayor y eximentes de responsabilidad, por las cuales REGISTRO DIGITAL PRISMA quedará exenta de toda responsabilidad y liberada de todas sus obligaciones cuando por razones de fuerza mayor no pueda emitir, revocar o consultar la lista de los certificados revocados.

2.2.2.Responsabilidad de la Autoridad de Registro

Las responsabilidades, exclusiones y limitaciones de responsabilidad aplicables a REGISTRO DIGITAL PRISMA, en sus roles de AR y AC, se encuentran regidas por la ley, los reglamentos y disposiciones aplicables emanadas por el Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía.

2.2.3.Responsabilidad del Suscriptor

i. Garantías del Suscriptor

El contrato del SUSCRIPTOR de REGISTRO DIGITAL PRISMA establece cláusulas en las que se exigen que los SUSCRIPTORES garanticen que:

- Cada firma electrónica avanzada creada que usa la clave privada que corresponde a la clave pública que se anota en el certificado, es la firma electrónica avanzada del propio SUSCRIPTOR y que el certificado ha sido aceptado y está funcionando (no está vencido ni revocado), en el momento en que se creó la firma electrónica avanzada.
- Que ninguna persona no autorizada ha tenido acceso a la clave privada del SUSCRIPTOR.
- Todas las declaraciones que haga el SUSCRIPTOR en la solicitud de certificado que presentó son verdaderas.
- Toda la información proporcionada por el SUSCRIPTOR y que se incluye en el certificado, es verdadera.

- El Certificado se utiliza exclusivamente para los fines autorizados y legales, congruentes con estas CPS, las CP y otros documentos relacionados con éstas.

El SUSCRIPTOR es un usuario final y no es una AUTORIDAD DE CERTIFICACIÓN y está usando la clave privada correspondiente a la clave pública anotada en el certificado, para fines de firmar electrónicamente un certificado (o cualquier otro formato de clave pública certificada) o CRL. El Suscriptor es responsable de guardar y custodiar su clave privada y por ende, debe de generar su clave privada confidencialmente en dispositivo seguro. No se permiten herramientas centralizadas de generación de claves privadas ni el respaldo centralizado de los mismos.

ii. Compromiso de la clave privada

Las CP y las CPS establecen normas básicas de la PKI de REGISTRO DIGITAL PRISMA para la protección de las claves privadas de los SUSCRIPTORES. En el contrato de SUSCRIPTOR se establecen una serie de declaraciones que obligan a los SUSCRIPTORES a cumplir con estas normas y puntualizan que los únicos responsables por las pérdidas o daños que se originen de esa falta de cumplimiento son los propios SUSCRIPTORES.

2.2.4.Confiabilidad de la Parte que Confía

El contrato del SUSCRIPTOR y el contrato de la PARTE QUE CONFÍA correspondientemente exigen cada uno, que LAS PARTES QUE CONFÍAN reconozcan que cuentan con información suficiente para tomar una decisión informada con respecto a la medida en que optan por confiar en la información de un certificado, que son responsables únicamente por decidir si confían o no en esa información, y que se harán cargo de las consecuencias legales de su incumplimiento con las obligaciones de la PARTE QUE CONFÍA.

2.3. Responsabilidad financiera

2.3.1.Responsabilidad financiera hacia los Suscriptores y las Partes que Confían

i. Responsabilidad financiera hacia los Suscriptores

En la medida en que lo permitan las leyes aplicables, el contrato de SOLICITANTE SUSCRIPTOR DE REGISTRO DIGITAL PRISMA exige, REGISTRO DIGITAL PRISMA, no se responsabilizará, ni responderá; y por lo tanto, no indemnizará al solicitante suscriptor, a alguna parte o tercero alguno que pretendiere resarcimiento por la utilización de los Certificados emitidos por REGISTRO DIGITAL PRISMA, en las siguientes circunstancias:

- Falsedad o declaración de hecho falsa por el SUSCRIPTOR sobre la Solicitud de Certificado del SUSCRIPTOR, que lleve a la denegatoria para la emisión del Certificado;
- Que el SUSCRIPTOR no haya protegido su clave privada, usado un sistema confiable, o de otro modo, tomado las debidas precauciones para evitar el compromiso, pérdida,-divulgación, modificación o uso autorizado de la clave privada del SUSCRIPTOR.

ii. Responsabilidad financiera hacia las partes que confían

En la medida en que lo permitan las leyes aplicables, el contrato entre la PARTE QUE CONFÍA y REGISTRO DIGITAL PRISMA exige, que REGISTRO DIGITAL PRISMA, no se responsabilizará, ni responderá a LA PARTE QUE CONFÍA por:

- El incumplimiento de la PARTE QUE CONFÍA con las obligaciones que le atañen, conforme al CONTRATO DE LA PARTE QUE CONFÍA, que está en sitio web: www.prisma.gt; el cual debe de aceptar antes de utilizar los servicios ofrecidos en el mencionado sitio.
- La confianza de una PARTE QUE CONFÍA en un certificado que razonablemente no sea acorde a las circunstancias, o
- El incumplimiento de la PARTE QUE CONFÍA con la verificación de la condición de dicho certificado, para determinar si el certificado está vencido o revocado.

2.3.2.Relaciones accesorias

En la medida en que lo permitan las leyes aplicables, el contrato del SUSCRIPTOR y el contrato de la PARTE QUE CONFÍA de REGISTRO DIGITAL PRISMA, respectivamente desconocen los acuerdos o contratos de la AC o las AR que no formen parte de la PKI de REGISTRO DIGITAL PRISMA.

2.3.3.Procesos Administrativos

REGISTRO DIGITAL PRISMA contará con los recursos financieros suficientes para mantener sus operaciones y llevar a cabo sus deberes y obligaciones, así como será capaz de enfrentar el riesgo de la responsabilidad para con los SUSCRIPTORES y LAS PARTES QUE CONFÍAN, contratando y manteniendo vigente el seguro de responsabilidad civil, así como los seguros que establezca la ley y el reglamento correspondiente.

2.3.4.Algunas responsabilidades adicionales a las partes

La presente cláusula establecerá de manera enunciativa más no limitativa algunas obligaciones adicionales relativas a las partes, e incluso de terceros que pudieran verse involucrados con el certificado, solicitado para su emisión por parte de REGISTRO DIGITAL PRISMA y constituyen disposiciones que deberán regir los contratos correspondientes y que describen en las siguientes literales:

i. Obligaciones de REGISTRO DIGITAL PRISMA como Autoridad de Registro (AR)

REGISTRO DIGITAL PRISMA, en su calidad de AR, lleva a cabo funciones de validación, aprobando o rechazando solicitudes de certificado, solicitando la revocación de certificados y aprobando solicitudes de renovación.

ii. Obligaciones del Suscriptor

- Las obligaciones del SUSCRIPTOR serán aplicables a todos aquellos SUSCRIPTORES dentro de la PKI de REGISTRO DIGITAL PRISMA, mediante el contrato del SUSCRIPTOR aprobado por REGISTRO DIGITAL PRISMA.

- Dentro de la PKI de REGISTRO DIGITAL PRISMA, el contrato del SUSCRIPTOR establece como requisito, que los solicitantes del certificado ofrezcan información completa y precisa a través de su formulario de solicitud de certificado y manifiesten su consentimiento al suscribir el CONTRATO de SUSCRIPTOR, como condición para obtener un certificado.

- Al contrato del SUSCRIPTOR y a los SUSCRIPTORES que soliciten la emisión de un certificado al amparo de la PKI de REGISTRO DIGITAL PRISMA, les son aplicables las obligaciones específicas que aparecen en estas CPS de REGISTRO DIGITAL PRISMA.

- El contrato del SUSCRIPTOR exige que los SUSCRIPTORES usen sus Certificados de acuerdo con lo establecido a las CPS y entre otras obligaciones, se exige que los SUSCRIPTORES tengan bajo su guarda y custodia, protejan, resguarden y no publiquen o revelen a terceros sus claves privadas. Conforme al contrato del SUSCRIPTOR, si un SUSCRIPTOR descubre o tiene motivos para creer que su clave privada de SUSCRIPTOR o de los datos de activación que protegen dicha Clave Privada (si fuera aplicable) ha sido comprometida, o si la información del certificado es incorrecta o ha cambiado, el SUSCRIPTOR de inmediato deberá:

- Notificar por correo electrónico a la dirección suscriptor@prisma.gt o por cualquier medio escrito a REGISTRO DIGITAL PRISMA y solicitar la revocación del certificado.

- El contrato del SUSCRIPTOR incluye una cláusula en la que se exige que los SUSCRIPTORES dejen de usar sus claves privadas al finalizar sus períodos de vigencia.

- Los Contratos del SUSCRIPTOR declaran que los SUSCRIPTORES no supervisarán, interferirán ni harán algún tipo de ingeniería inversa a la PKI de REGISTRO DIGITAL PRISMA ni comprometerán intencionalmente la seguridad de ésta.

iii. Obligaciones de la Parte que Confía

- Todos aquellos terceros que se involucren con los SUSCRIPTORES que obtengan un certificado y que en virtud de dicho certificado consoliden una relación basada en la confiabilidad que representa dicho certificado serán denominados para efectos de la presente CPS como " PARTE QUE CONFÍA".

- La PARTE QUE CONFÍA dentro de las PKI de REGISTRO DIGITAL PRISMA, antes de cualquier acto de confianza, deberá evaluar independientemente la conveniencia de uso de un certificado para cualquier fin determinado y decidir que el certificado, de hecho, se usará para un fin adecuado. Dichos terceros deberán estar conscientes de que las Autoridades de Registro que hayan estado involucradas en la autenticación de datos, Autoridades Certificadoras (cuando sea aplicable) y REGISTRO DIGITAL PRISMA, no son responsables de evaluar la conveniencia del uso de un certificado.

- A fin de allegarse de información correcta, veraz, atribuible y susceptible de verificarse, las PARTES QUE CONFÍAN deben de utilizar aplicaciones y hardware apropiado para realizar la verificación de la firma electrónica avanzada u otras operaciones criptográficas que desean realizar, como condición para confiar en los certificados con respecto a cada una de estas operaciones. Dichas operaciones comprenden la identificación de una cadena de certificados y la verificación de las firmas electrónicas avanzadas de todos los certificados de la cadena de certificados conforme a estos contratos, las PARTES QUE CONFÍAN no deben confiar en un certificado, a menos que estos procedimientos de verificación tengan éxito.

- Las PARTES QUE CONFÍAN deberán comprobar el estado de un certificado en el que desean confiar, al igual que todos los certificados de su cadena de certificados. Si alguno de los certificados de la cadena de certificados fue revocado, no deberán confiar en el certificado del SUSCRIPTOR del usuario final o en otro certificado revocado de la cadena de certificados.

- LAS PARTES QUE CONFÍAN tienen derecho de confiar en el certificado, siempre y cuando la confianza en el certificado sea razonable en las circunstancias. Si las circunstancias indican la necesidad de garantías adicionales, la PARTE QUE CONFÍA debe obtener dichas garantías para que la citada confianza se considere razonable.

iv. Garantías de la Autoridad de Certificación para los suscriptores y las partes que confían

El contrato del SUSCRIPTOR de REGISTRO DIGITAL PRISMA comprende una serie de garantías para los SUSCRIPTORES dentro de las que se incluyen:

- No hay falsas declaraciones sustanciales en el certificado que conozcan o se deriven de las entidades que aprueban la solicitud del certificado o emitan el certificado.

- No hay errores en la información del certificado, introducida por REGISTRO DIGITAL PRISMA al aprobar la solicitud de emisión de certificado, o en la emisión de este.

- Toda la información que contiene el certificado o que se incorpora en él mediante referencia, salvo por la información del SUSCRIPTOR no verificada, es exacta;

- Con respecto a los certificados que aparecen en el repositorio de REGISTRO DIGITAL PRISMA, que el certificado fue emitido a la persona individual o persona jurídica que se nombre en el certificado como SUSCRIPTOR, y que el SUSCRIPTOR ha aceptado el certificado.

v. Límites de responsabilidad

Esta cláusula se aplica a la responsabilidad de conformidad con el convenio (incluyendo la trasgresión de la garantía), agravio (incluyendo negligencia y/o estricta responsabilidad) y cualquier otra forma de reclamación legal o equitativa. Si se entabla alguna demanda, acción, litigio, arbitraje u otro tipo de proceso relativo a los servicios materia del presente documento del SUSCRIPTOR, la responsabilidad total de las Partes estará limitada en el contrato correspondiente.

2.4. Interpretación y exigibilidad

2.4.1.Leyes que rigen

Las presentes CPS se encuentran sujetas a la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas - Decreto número 47-2008 del Congreso de la República, sus Reglamentos vigentes; así como a las Guías de Evaluación y las Inspecciones Periódicas del Registro de Prestadores de Servicios de Certificación; siendo todas las anteriores, la normativa que regirá su exigibilidad, interpretación y validez.

2.4.2.Divisibilidad, supervivencia, fusión, aviso

En la medida en que lo permitan las leyes aplicables, el contrato del SUSCRIPTOR y el de la PARTE QUE CONFÍA de REGISTRO DIGITAL PRISMA contienen cláusulas de divisibilidad, supervivencia, fusión y aviso. Una cláusula de divisibilidad en un contrato evita que la determinación de invalidez o inexigibilidad de una cláusula del mismo deteriore el resto del contrato. Una cláusula de supervivencia especifica que las disposiciones de un contrato pueden continuar en vigor a pesar de la rescisión o vencimiento del contrato. Una cláusula de fusión manifiesta que todos los entendimientos relativos al objeto de un contrato están incorporados en el mismo. Una cláusula de aviso de un contrato, estipula la forma en que las partes se van a dar avisos entre sí.

2.4.3.Procedimientos de resolución de conflictos

i. Conflictos con los Suscriptores Usuarios Finales y las partes que Confían

En la medida en que lo permitan las leyes aplicables, los Contratos del SUSCRIPTOR y los Contratos de la PARTE QUE CONFÍA de REGISTRO DIGITAL PRISMA contienen, una cláusula de resolución de conflictos. La cláusula manifiesta que los procedimientos de resolución de conflictos exigen de un periodo de negociación mínimo de sesenta (60) días calendario, por lo que las partes harán lo posible por llegar a una solución amigable de todas las controversias relativas a la aplicación, interpretación, contravención, terminación, ejecución o invalidez de los contratos de los Suscriptores y LAS PARTES QUE CONFÍAN. Si las partes no pudieran resolver amigablemente la controversia dentro de los sesenta (60) días calendario siguientes a la recepción por una de ellas del pedido de solución amigable, presentado por la otra, la solución de las controversias a la aplicación,

interpretación, contravención, terminación, ejecución o invalidez de dichos contratos serán sometidas a arbitraje de equidad, de conformidad con el reglamento de conciliación y arbitraje del centro de arbitraje y conciliación de la Cámara de la Industria el cual, las partes declaran que conocen y aceptan desde ya en forma irrevocable. Al surgir cualquier conflicto, disputa o reclamación, las partes designarán cada una un árbitro para su nombramiento por la Junta Directiva del centro y la autorizan para que nombre al tercer árbitro, de conformidad con dicho reglamento, en todo caso, el centro será la institución encargada de administrar el procedimiento arbitral y de cumplir con todas las funciones que le designa el citado reglamento de arbitraje. Aquellas controversias, que por razón de su naturaleza jurídica no sean materia arbitrable o no pudieran ser resueltas mediante Arbitraje u otro Mecanismo Alternativo de Solución de Controversias se resolverán por los tribunales de Guatemala.

2.5.Tarifas

2.5.1.Tarifa de emisión de Certificado o tarifa de renovación

REGISTRO DIGITAL PRISMA tiene derecho de cobrar por los servicios que presta, incluyendo, pero no limitando la emisión y renovación de los Certificados, de acuerdo con las tarifas que establezca para cada tipo de servicio. Dicho cobro, se formalizará a través de la intervención de un Distribuidor Autorizado, quien establecerá la tarifa a fijar al solicitante suscriptor.

2.5.2. Acceso gratuito a publicidad del Certificado

Ni REGISTRO DIGITAL PRISMA ni los Solicitantes Suscriptores, cobrarán tarifa alguna como condición para poner un Certificado a disposición de los usuarios o LAS PARTES QUE CONFÍAN en el repositorio.

2.5.3.Tarifas de otros servicios de valor agregado y acceso de información de revocación

REGISTRO DIGITAL PRISMA no cobra tarifa como condición para hacer que las CRL estén disponibles en el repositorio o, de otro modo, estén disponibles para LAS PARTES QUE CONFÍAN.

2.5.4. Tarifas para otros servicios, como la información de política

REGISTRO DIGITAL PRISMA no cobra tarifas por el acceso a las CP ni a estas CPS. El uso que se haga para

fines que no sean simplemente ver el documento, como su reproducción, redistribución, modificación o creación de trabajos derivados, está sujeto a un contrato de licencia con la entidad que posea el derecho de autor del documento.

2.6. Publicación y repositorio

2.6.1.Publicación de información de la AC

REGISTRO DIGITAL PRISMA es responsable del funcionamiento del repositorio, tanto respecto a la infraestructura tecnológica como los procesos administrativos de actividades que lleve a cabo como Autoridad de Certificación. REGISTRO DIGITAL PRISMA publica cierta información de la AC en la sección de repositorio del sitio Web de REGISTRO DIGITAL PRISMA en: www.prisma.gt. REGISTRO DIGITAL PRISMA publica las CP, estas CPS, el contrato del SUSCRIPTOR y el contrato de la PARTE QUE CONFÍA en el sitio Web de REGISTRO DIGITAL PRISMA, publicando la información del Estado de los Certificados.

2.6.2.Frecuencia de la publicación

Las actualizaciones de estas CPS se publican de acuerdo con el punto 8 de las CPS. Las actualizaciones del contrato del SUSCRIPTOR y del contrato de la PARTE QUE CONFÍA, se publicarán en el sitio de web de REGISTRO DIGITAL PRISMA, cuando sean emitidos.

2.6.3.Controles de acceso

La información que se publica en la parte del repositorio del sitio Web de REGISTRO DIGITAL PRISMA es información de libre acceso al público. El acceso de sólo lectura a dicha información no tiene restricción. REGISTRO DIGITAL PRISMA exige que las personas convengan en un Contrato de la PARTE QUE CONFÍA como condición para acceder a los Certificados, la información del estado del Certificado o las CRL. REGISTRO DIGITAL PRISMA ha implementado medidas de seguridad lógicas y físicas para evitar que las personas malintencionadas, sin autorización, agreguen, supriman o modifiquen datos.

2.6.4.Repositorios

Ver el apartado 2.1.5 de estas CPS

2.7. Auditoría de cumplimiento

Según apego a la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala, su reglamento y sus Guías de Evaluación; el Registro de Prestadores de Servicio de Certificación (RPSC) del Ministerio de Economía de Guatemala podrá llevar a cabo como mínimo una visita anual para llevar a cabo auditoría de cumplimiento de las obligaciones de REGISTRO DIGITAL PRISMA.

REGISTRO DIGITAL PRISMA, tendrá derecho de efectuar "Revisiones Suplementarias de la Administración de Riesgos" de sí mismo, después de haber descubierto que no se ha cumplido a cabalidad o en forma total con todo según lo indicado por una Auditoría de Cumplimiento.

REGISTRO DIGITAL PRISMA tendrá derecho de delegar la realización de estas auditorías internas, revisiones e investigaciones a un tercero independiente. Las entidades que están sujetas a una auditoría, revisión o investigación, colaborarán en forma razonable con REGISTRO DIGITAL PRISMA y el personal que lleva a cabo la auditoría, revisión o investigación.

2.7.1.Frecuencia de la auditoría de cumplimiento de la entidad

Las auditorías de cumplimiento que realiza el Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía de Guatemala, se llevan a cabo anualmente para garantizar una operación continua y confiable, de conformidad con lo establecido en la Ley.

2.7.2.Requisitos de la identidad del auditor

Para las auditorías a la AC de REGISTRO DIGITAL PRISMA, S.A., que lleve a cabo el Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía de Guatemala; será éste el encargado de definir los requisitos de sus auditores apegándose a la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala, su reglamento y sus Guías de Evaluación.

Para las auditorías internas que REGISTRO DIGITAL PRISMA, S.A. considere conveniente efectuar a sí mismo; o las que considere pertinente efectuar a los demás actores dentro de las PKI de REGISTRO DIGITAL PRISMA, ésta determinará los requisitos y competencias para el auditor interno o

independiente o la institución que se contrate y entre las competencias básicas, estarán la debida pericia en tecnología de PKI, herramientas y técnicas de seguridad de la información, auditoria de seguridad y estar acreditado para realizar esta función, la cual exige la posesión de una cierta serie de aptitudes, medidas de garantía de la calidad como la revisión, las pruebas de competencia, las normas con respecto a la debida asignación del personal a los compromisos y los requisitos para la educación profesional continua.

2.7.3.Medidas que se toman en virtud de deficiencias

REGISTRO DIGITAL PRISMA y su órgano de administración es el responsable de desarrollar e implementar las acciones correctivas según apego a la Ley para el Reconocimiento de las comunicaciones y firmas electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala, su reglamento, las Guías de Evaluación y las propias Inspecciones Periódicas.

Para las auditorías que REGISTRO DIGITAL PRISMA, S.A. considere conveniente efectuar a sí misma; si en caso llegara a determinar que los hallazgos plantean una amenaza grave e inmediata a la seguridad o integridad de las PKI DE REGISTRO DIGITAL PRISMA, se desarrollarán las acciones correctivas en 30 días y se implementarán dentro de un período razonable. Con respecto a excepciones o deficiencias menos graves, la Dirección de REGISTRO DIGITAL PRISMA evaluará la importancia de dichos asuntos y determinará el curso de acción adecuado.

2.7.4.Comunicaciones de los resultados

Los resultados de la auditoría de cumplimiento de las operaciones de REGISTRO DIGITAL PRISMA pueden darse a conocer a discreción de la Dirección de REGISTRO DIGITAL PRISMA.

2.8. Confidencialidad y privacidad

REGISTRO DIGITAL PRISMA ha implantado una política de privacidad, que se encuentra disponible en www.prisma.gt.

2.8.1.Tipos de Información que debe mantenerse confidencial y privada

Los siguientes registros de SUSCRIPTORES, sujetos al apartado 2.8.2 de la CPS, se mantienen confidenciales

y privados, así como los siguientes:

- Registros de Solicitudes de Certificado (sujetas al apartado 2.8.2 de la CPS);
- Registros de Transacciones (tanto registros completos como el rastreo de auditorías de transacciones);
- Los informes de auditoría de REGISTRO DIGITAL PRISMA, creados por REGISTRO DIGITAL PRISMA o sus auditores respectivos (ya sean internos o públicos);
- Planeación de contingencia y planes de recuperación de desastres, y medidas de seguridad que controlan las operaciones del hardware y software de REGISTRO DIGITAL PRISMA y la administración de servicios de Certificados y los servicios de inscripción designados.

2.8.2.Tipos de Información que no se considera confidencial ni privada

Los Participantes de la PKI de REGISTRO DIGITAL PRISMA reconocen que la información pública de los certificados, la revocación de certificados y otra información del estado y la información contenida en el repositorio de REGISTRO DIGITAL PRISMA no se considera información confidencial ni privada. Esta sección, está sujeta a las leyes de privacidad aplicable.

2.8.3.Divulgación de información de revocación de certificados

Ver el apartado 2.8.2 de CPS.

2.8.4.Divulgación de información confidencial – obligatoria

Los Participantes de la PKI de REGISTRO DIGITAL PRISMA reconocen que REGISTRO DIGITAL PRISMA está facultada a divulgar la información confidencial / privada si recibe una notificación de resolución ya sea administrativa o judicial en la que se le requiera la información de un certificado o de un suscriptor de conformidad con la ley y que la divulgación sea necesaria en respuesta a un proceso judicial, administrativo o de otra naturaleza durante el proceso de exhibición de un juicio de cualquier naturaleza, incluyendo citaciones, interrogatorios, solicitudes de admisión y solicitudes de presentación de pruebas y por lo tanto la divulgación en estos casos es obligatoria.

2.9. Derechos de propiedad intelectual

La asignación de Derechos de Propiedad Intelectual entre los participantes de la PKI REGISTRO DIGITAL PRISMA que no sean los SUSCRIPTORES y LAS PARTES QUE CONFÍAN, están regidas por los contratos aplicables entre dichos participantes. Los siguientes incisos del apartado 2.9 de estas CPS se aplican a los derechos de propiedad intelectual con respecto a los SUSCRIPTORES y a LAS PARTES QUE CONFÍAN.

2.9.1.Derechos de propiedad en los Certificados e información de revocación

REGISTRO DIGITAL PRISMA tiene todos los Derechos de Propiedad Intelectual que corresponden y que se incluyen en Certificados y la información de revocación que emiten.

2.9.2.Derechos de propiedad en las CPS

Los Participantes de la PKI de REGISTRO DIGITAL PRISMA reconocen que REGISTRO DIGITAL PRISMA tiene los Derechos de Propiedad Intelectual de estas CPS.

2.9.3.Derechos de propiedad en los nombres

El Solicitante a Suscriptor de un certificado, conservará todos los derechos que tiene (en su caso); si alguna marca registrada, marca de servicio o nombre comercial se incluye en alguna solicitud de Certificado y nombre distinguido dentro de cualquier Certificado emitido a dicho Solicitante.

2.9.4.Derechos de propiedad en las claves y el material clave

Los pares de claves que corresponden a los Certificados de REGISTRO DIGITAL PRISMA y a los SUSCRIPTORES, son propiedad de REGISTRO DIGITAL PRISMA y los SUSCRIPTORES que son los Sujetos respectivos de estos Certificados, respectivamente; no importa el medio físico dentro del cual están almacenados y protegidos, y dichas personas retienen todos los Derechos de Propiedad Intelectual en estos pares de claves. No obstante, lo anteriormente expuesto, las claves públicas Raíz de AC y los Certificados Raíz que las contienen, incluyendo todas las claves públicas de la AC y los Certificados auto firmados, son propiedad de REGISTRO DIGITAL PRISMA. Finalmente, sin limitar la generalidad de lo anterior, la clave privada de la AC es propiedad de REGISTRO DIGITAL PRISMA; y ésta retiene el Derecho de Propiedad Intelectual de las mismas.

3. Identificación y autenticación

3.1. Registro Inicial

3.1.1.Tipos de nombres

Los Certificados de la AC de REGISTRO DIGITAL PRISMA contienen Nombres Distinguidos X.509 versión 3 en los campos del Emisor y el Sujeto.

Los Certificados del SUSCRIPTOR usuario final contienen un nombre distinguido X.509 versión 3 en el campo el nombre del Sujeto.

El elemento de Nombre Común (CN=) del nombre distinguido del Sujeto de los Certificados del SUSCRIPTOR usuario final se autentica cuando se trata de los Certificados.

- El valor del nombre común autenticado que se incluye en los nombres distinguidos del sujeto del certificado de persona jurídica, es un nombre de dominio (cuando se trata de identificaciones del servidor seguro e identificaciones del servidor global) o el nombre legal de la persona jurídica o unidad dentro de la persona jurídica.
- Sin embargo, el valor del nombre común autenticado incluido en el nombre distinguido del sujeto del certificado de persona jurídica, es el nombre personal aceptado del representante legal autorizado para usar la clave privada de la entidad y el elemento de la entidad es el nombre legal de la persona jurídica.
- El valor del nombre común que se incluye en el nombre distinguido del sujeto de los certificados de personas individuales representa el nombre personal aceptado generalmente de la persona.

3.1.2.Necesidad de que los nombres sean significativos

Los certificados del SUSCRIPTOR usuario final contienen nombres con semántica que se entiende comúnmente y que permite la determinación de la identidad de la persona individual o la persona jurídica que es el sujeto del certificado. No se permiten los seudónimos de los SUSCRIPTORES (nombres que no sean el nombre verdadero personal o de la persona jurídica) en esos certificados. Los certificados de la AC de REGISTRO DIGITAL PRISMA contienen nombres con semántica que se entiende comúnmente y permite la determinación de la identidad de la AC que es el asunto del certificado.

3.1.3.Singularidad de los nombres

REGISTRO DIGITAL PRISMA garantiza que los nombres distinguidos del asunto son únicos dentro del

dominio de una AC específica a través de elementos automatizados del proceso de inscripción del SUSCRIPTOR.

3.1.4.Procedimiento de resolución de conflictos por reclamaciones de nombres

Se prohíbe que los Solicitantes de Certificado usen nombres en sus Solicitudes de Certificado que infrinjan los Derechos de Propiedad Intelectual de otros. Sin embargo, REGISTRO DIGITAL PRISMA no verifica si un Solicitante del certificado tiene Derechos de Propiedad Intelectual con el nombre que aparece en la Solicitud de Certificado, ni funge como árbitro ni como juez o mediador o de otro modo resuelve algún conflicto relativo a la propiedad de algún nombre de dominio, nombre comercial, marca registrada o marca de servicio. REGISTRO DIGITAL PRISMA tiene derecho, sin responsabilidad ante ningún Solicitante del certificado, de rechazar cualquier Solicitud de Certificado en virtud de tal conflicto.

3.1.5.Registro, autenticación y marcas registradas

Ver el apartado 3.1.4 CPS

3.1.6.Método para solicitar un certificado para firma electrónica avanzada

REGISTRO DIGITAL PRISMA recibe las solicitudes de certificados para firma electrónica avanzada, por medio del sitio web www.prisma.gt, utilizando el estándar de envío de mensajes PKCS #10, a partir del cual se incluye la clave pública y los datos que dan identidad al par de claves; un mecanismo habitual de solicitudes de un servidor web a una CA.

3.1.7.Autenticación de la identidad de la persona jurídica

REGISTRO DIGITAL PRISMA confirma la identidad de los solicitantes SUSCRIPTORES de personas jurídicas y otro tipo de información de inscripción que se le proporcione a los solicitantes de certificado (salvo por la Información del SUSCRIPTOR no verificada), de acuerdo con los procedimientos que se establecen en los incisos que siguen, además de los siguientes procedimientos, el solicitante del certificado debe demostrar que tiene legalmente la clave privada que le corresponde a la clave pública que se va a anotar en el certificado, de acuerdo con el punto 3.1.6 de la CPS.

i. Autenticación de los Certificados de Registro Digital Prisma de persona jurídica

Para confirmar la identidad de un solicitante del certificado para el certificado REGISTRO DIGITAL PRISMA de Persona Jurídica, se requerirá:

- La determinación de que la persona jurídica existe mediante su comprobación en el Registro

Mercantil General de la República, Registro de Personas Jurídicas del Ministerio de Gobernación de la República de Guatemala o alternativamente, mediante documentación de la entidad emitida por oficina privada o de gobierno que tenga la capacidad para comprobarlo.

- La confirmación por teléfono, correo confirmatorio y/o procedimiento comparable para el solicitante del certificado para confirmar cierta información sobre la entidad, confirmar que la persona jurídica ha autorizado la solicitud de certificado, confirmar la designación del representante que presenta la solicitud de certificado en nombre del solicitante del certificado.
- Una confirmación por teléfono, correo confirmatorio y/o procedimiento comparable para verificar que la persona nombrada como representante ha presentado la solicitud de certificado en representación de la persona jurídica.

3.1.8.Autenticación de la Identidad de persona individual

Con respecto a los Certificados de personas individuales, REGISTRO DIGITAL PRISMA, como AC confirma que:

- El solicitante del certificado es la persona identificada en la solicitud del certificado.
- El solicitante del certificado posee legalmente la clave privada que le corresponde a la clave pública que se va a anotar en el certificado, de acuerdo con el apartado 3.1.6 de la CPS, y
- La información que se va a incluir en el certificado es precisa.

Asimismo, REGISTRO DIGITAL PRISMA lleva a cabo los procedimientos más detallados que se describen a continuación para certificados.

i. Certificados de personas individuales

La autenticación de las solicitudes de certificados de personas individuales se basa en la comprobación fehaciente de la identidad del solicitante para lo cual REGISTRO DIGITAL PRISMA requerirá previamente la comparecencia personal y directa del solicitante, ante sí o ante notario, por medio de una sesión de videoconferencia asistida con el Operador PKI para realizar la correspondencia de la información o por medio de una validación no asistida por medio de la aplicación proveída por REGISTRO DIGITAL PRISMA. Se verificará la identidad del solicitante del certificado, comprobándola por medio del Documento Personal de Identificación emitido por el Registro Nacional de las Personas (RENAP), el pasaporte cuando aplique y la constancia de inscripción y modificación en el Registro Tributario Unificado (RTU) emitido en el año en curso.

3.2. Solicitud de revocación

Antes de la revocación de un certificado, REGISTRO DIGITAL PRISMA verifica que dicha solicitud de revocación haya sido requerida por el SUSCRIPTOR del certificado.

Entre los procedimientos aceptables para autenticar las solicitudes de revocación del SUSCRIPTOR, se encuentran los siguientes:

- Hacer que el suscriptor presente en el Sitio Web de REGISTRO DIGITAL PRISMA www.prisma.gt, su clave de anulación y revoque el certificado automáticamente, siempre y cuando el sistema verifique que sí corresponde a la clave que está en el registro.

- Comunicación con el suscriptor en donde se obtengan garantías razonables a la luz de la clase de certificado que la persona individual o persona jurídica que pide la revocación, es en realidad el suscriptor; dependiendo de las circunstancias, dicha comunicación puede comprender uno o más de los medios siguientes: teléfono, correo electrónico, servicio de mensajería, entre otros.

Los Operadores AC de REGISTRO DIGITAL PRISMA pueden realizar la revocación de los certificados digitales del suscriptor usuario final dentro del subdominio de REGISTRO DIGITAL PRISMA. La identidad de los Operadores AC, la auténtica REGISTRO DIGITAL PRISMA mediante el control de acceso, usando SSL y autenticación del cliente antes de permitir que lleven a cabo funciones de revocación.

3.3. Requisitos de documentos presentados

Para la identificación física de los solicitantes de los certificados en presencia física ante REGISTRO DIGITAL PRISMA o ante notario, o para la identificación por medio de una sesión de videoconferencia asistida con el Operador PKI para realizar la correspondencia de la información o por medio de una validación no asistida por medio de la aplicación proveída por REGISTRO DIGITAL PRISMA, deberán presentar la documentación requerida dentro de las Prácticas de Registro para Persona Individual y las Prácticas de Registro para Persona Jurídica establecidas por REGISTRO DIGITAL PRISMA.

4. Requisitos de operación

4.1. Solicitud del Certificado

4.1.1.Solicitudes de Certificado para los Certificados de los Suscriptores usuarios finales

Con respecto a los Certificados de REGISTRO DIGITAL PRISMA, todos los solicitantes de certificado que sean usuarios finales pasarán por un proceso de inscripción, que consiste en:

- Llenar una solicitud de certificado, proporcionando la información requerida;
- Generar o encargarse de que se haya generado un par de claves de acuerdo con el apartado 6.1 de la CPS;
- El Solicitante del certificado entrega su clave pública, directamente o a través de una Autoridad de Certificación subordinada autorizada a REGISTRO DIGITAL PRISMA, de acuerdo con el apartado 6.1.3 de la CPS;
- Demostrar a REGISTRO DIGITAL PRISMA de acuerdo con el apartado 3.1.6 de las CPS que el Solicitante del Certificado posee la clave privada que le corresponde a la clave pública entregada a REGISTRO DIGITAL PRISMA, y
- Manifestar su consentimiento al contrato del SUSCRIPTOR pertinente.

4.1.2.Solicitudes de Certificados de AC, AR, PKI de Registro Digital Prisma y personal autorizado;

i. **Certificados de la Autoridad de Registro**

REGISTRO DIGITAL PRISMA opera una AC administrativa, que puede emitir certificados a las AR y los sistemas de las AR, incluyendo:

- El personal de REGISTRO DIGITAL PRISMA (los Administradores de la AR de REGISTRO DIGITAL PRISMA) que procesa solicitudes de certificado en nombre de la AC de REGISTRO DIGITAL PRISMA.

Las AR, como SUSCRIPTORES de la AC Administrativa pertinente, deben contar con la autorización del Registro de Prestadores de Servicios de Certificación (RPSC) y se aplican los requisitos para los Certificados del Administrador indicados en el apartado 4.1.1 de la CPS.

ii. ***Certificados del empleado de Registro Digital Prisma***

REGISTRO DIGITAL PRISMA emite certificados a sus empleados, después de la presentación exitosa y procesamiento de una solicitud de certificado.

4.2. Emisión del Certificado

4.2.1.Emisión de Certificados del Suscriptor

Después de que un solicitante del certificado presenta una solicitud ya sea de manera física, por medio de una sesión de videoconferencia asistida con el Operador PKI para realizar la correspondencia de la información o por medio de una validación no asistida por medio de la aplicación proveída por REGISTRO DIGITAL PRISMA y acepta las condiciones del contrato solicitante suscriptor, REGISTRO DIGITAL PRISMA debe confirmar la información de la solicitud de certificado. Cuando se han llevado a cabo exitosamente todos los procedimientos de autenticación necesarios de acuerdo con el apartado 3.1 de la CPS, REGISTRO DIGITAL PRISMA aprueba la solicitud de certificado. Si la autenticación no tiene éxito, REGISTRO DIGITAL PRISMA rechaza la solicitud del certificado y la notificación de rechazo se manda por correo electrónico a la dirección que especificó el usuario durante su solicitud original indicando la razón del rechazo y dándole un plazo al solicitante para que subsane el error o la falta si fuera aplicable. Si vencido el plazo otorgado por REGISTRO DIGITAL PRISMA o la Autoridad de Registro involucrada en el proceso de verificación al solicitante no subsana el error o la falta, REGISTRO DIGITAL PRISMA o la Autoridad de Registro tendrá por rechazada la solicitud y le notificará al solicitante el rechazo. Con base en la información proporcionada por el solicitante/suscriptor, REGISTRO DIGITAL PRISMA, como AC crea y emite un certificado después de haber aprobado la solicitud de certificado en su calidad de AR.

Cuando REGISTRO DIGITAL PRISMA verifica una solicitud de emisión de certificado y esta es satisfactoria; actuando en su calidad de Autoridad de Registro, procede a aprobar la solicitud y posteriormente, en su calidad de Autoridad de Certificación, genera un certificado, el cual es emitido a favor del solicitante. Los procedimientos de esta sección también se aplican para la emisión de certificados, con relación a la presentación de una solicitud para sustituir certificados anteriormente emitidos y para el procedimiento de renovación de certificados. Los correos de notificación de confirmación, aprobación o rechazo son enviados al correo electrónico que ingresa el cliente en el formulario de solicitud de certificado.

4.2.2.Emisión de Certificados de AR

REGISTRO DIGITAL PRISMA autentica la identidad de las entidades que deseen ser AR, las cuales deben obtener la autorización del Registro de Prestadores de Servicios de Certificación (RPSC) para poder operar. Antes que REGISTRO DIGITAL PRISMA celebre un contrato con el potencial AR solicitante conforme al

apartado 4.1.2 de la CPS, se confirma la autorización obtenida por parte del Registro de Prestadores de Servicios de Certificación (RPSC) y su identidad con base en los documentos de identificación presentados y la presencia física del representante legal. La celebración de dicho contrato indica la aprobación final y total de la solicitud de parte de REGISTRO DIGITAL PRISMA. REGISTRO DIGITAL PRISMA se reserva el derecho de autorizar o rechazar la solicitud de un solicitante proveniente de una AR independiente y no será responsable por las solicitudes rechazadas.

Una vez, REGISTRO DIGITAL PRISMA apruebe a una persona jurídica para ser AR, le emite el Certificado de AR, de acuerdo con el apartado 6.1 de la CPS. Lo anterior con base a los componentes de la infraestructura de REGISTRO DIGITAL PRISMA (por ejemplo, los Responsables OCSP), personal autorizado de REGISTRO DIGITAL PRISMA crea y aprueba las solicitudes de Certificado a través de un proceso controlado que exige la participación de múltiples Personas de Confianza.

4.3. Aceptación del Certificado

Al generar un certificado, REGISTRO DIGITAL PRISMA enviará un mensaje al suscriptor, a la cuenta de correo electrónico (e-mail) proporcionada en el formulario, la cual contendrá las instrucciones para que el solicitante/suscriptor reciba el certificado.

Si el solicitante/suscriptor cambia la dirección de correo electrónico, deberá iniciar un nuevo proceso de certificación, sin que pueda reclamar la devolución de las tarifas ya pagadas y sin que medie responsabilidad alguna por parte de REGISTRO DIGITAL PRISMA.

4.4. Revocación del Certificado

4.4.1.Circunstancias de revocación

i. Circunstancias para revocar los Certificados del Suscriptor usuario final

Se revoca un Certificado del suscriptor usuario final, si:

- REGISTRO DIGITAL PRISMA, o un suscriptor tiene motivos fundamentados para creer que ha habido un compromiso de la clave privada de un SUSCRIPTOR, o lo sospecha firmemente y le comunica este extremo a REGISTRO DIGITAL PRISMA.,
- REGISTRO DIGITAL PRISMA tiene motivos para creer que el suscriptor ha violado sustancialmente una obligación, declaración o garantía substancial al tenor del contrato del suscriptor aplicable.

- Que el contrato con el suscriptor se ha rescindido o su plazo ha vencido y no ha sido renovado.
- La relación entre una persona jurídica que es SUSCRIPTOR de un Certificado de REGISTRO DIGITAL PRISMA de persona jurídica y el representante legal que controla la clave privada del SUSCRIPTOR, se ha rescindido o concluye de alguna forma.
- REGISTRO DIGITAL PRISMA tiene motivos para creer que el Certificado no fue emitido conforme con los procedimientos que exige estas CPS, el Certificado fue emitido a una persona que no es la nombrada como Asunto del Certificado o el Certificado fue emitido sin la autorización de la persona nombrada como Asunto de dicho Certificado;
- REGISTRO DIGITAL PRISMA tiene motivos para creer que un hecho substancial de una Solicitud de Certificado es falsa o no es verdadera.
- REGISTRO DIGITAL PRISMA determina que no se cumplió o no se renunció a un prerrequisito substancial para la emisión del certificado.
- Cuando se trate de certificados de personas jurídicas; cambiar la razón social, denominación o el nombre de la persona jurídica del suscriptor. La información que tiene el certificado, que no sea la información del SUSCRIPTOR, no verificada, es incorrecta o ha cambiado, o El SUSCRIPTOR solicita la revocación del Certificado, de acuerdo con el apartado 3.4 de esta CPS. REGISTRO DIGITAL PRISMA también puede revocar un certificado cuyo suscriptor sea persona jurídica y cuyo plazo se dio por terminado o de otro modo concluyó. Los Contratos del SUSCRIPTOR de REGISTRO DIGITAL PRISMA exigen que los SUSCRIPTORES usuarios finales notifiquen de inmediato a REGISTRO DIGITAL PRISMA que se sabe o se sospecha de un compromiso de su clave privada.

Al revocar un certificado se cambia el estatus del mismo en la lista CRL y con el servicio OCSP. También se manda un correo electrónico al cliente con la confirmación del rechazo y la razón por la cual se rechazó el certificado .

ii. Circunstancias para revocar Certificados de AR

REGISTRO DIGITAL PRISMA revocará los certificados de la AR o de sus administradores, si:

- REGISTRO DIGITAL PRISMA descubre o tiene motivos para creer que se ha comprometido la clave privada de AR o de sus administradores;
- REGISTRO DIGITAL PRISMA descubre o tiene motivos para creer que el Certificado se emitió de manera que no se conforma substancialmente a los procedimientos que exigen estas CPS;

- El certificado se emitió a favor de una persona individual o jurídica que no es la que se nombra como asunto del certificado, o el certificado se emitió sin la autorización de la persona nombrada como el asunto del certificado;
- REGISTRO DIGITAL PRISMA determina que no se cumplió o no se renunció a un prerequisito substancial para la emisión de un Certificado.

4.4.2.¿Quién puede pedir la revocación de un Certificado del Suscriptor usuario final?

Las siguientes personas individuales o jurídicas pueden pedir la revocación de un Certificado del suscriptor usuario final:

- REGISTRO DIGITAL PRISMA, actuando en su calidad de AC que aprobó la Solicitud de Certificado del suscriptor.
- Los usuarios individuales pueden pedir la revocación de sus propios certificados de personas individuales. Cuando se trate de certificados de persona jurídica, sólo un representante debidamente autorizado y expresamente facultado por la entidad tiene derecho de pedir la revocación de certificados emitidos a la persona jurídica.

REGISTRO DIGITAL PRISMA publica los certificados que se expiden, así como si estos han sido revocados; en un repositorio públicamente accesible.

4.4.3.Procedimiento para pedir la revocación

i. Procedimiento para pedir la revocación de un Certificado del Suscriptor usuario final

El suscriptor de un certificado emitido por REGISTRO DIGITAL PRISMA, deberá solicitarle a REGISTRO DIGITAL PRISMA la revocación de su certificado, quien a su vez iniciará la revocación del certificado de forma inmediata.

El Suscriptor también podrá realizar la revocación directamente a través del sitio web de REGISTRO DIGITAL PRISMA www.prisma.gt por medio de la auto revocación, la cual requerirá que ingrese el número de serie de su certificado y la clave de anulación que ingresó en el formulario de solicitud del certificado.

4.4.4.Frecuencia de emisión de las CRL (Listas de Certificados revocados)

REGISTRO DIGITAL PRISMA publica sus CRLs en los cuales muestran la revocación de certificados y ofrece servicios de verificación de su estado. Las CRL de las AC son mantenidas por REGISTRO DIGITAL PRISMA y por ende los certificados AC de REGISTRO DIGITAL PRISMA tienen el punto de distribución –CDP–

(interfaz que representa cómo se debe obtener la información de CRL) de PKI de REGISTRO DIGITAL PRISMA, para que se pueda validar el estatus de estos.

4.4.5.Requisitos de verificación de la lista de revocación de Certificados

LA PARTE QUE CONFÍA debe verificar el estado de los certificados en los que desean confiar. Un método con el que LA PARTE QUE CONFÍA puede verificar el estado del Certificado es consultando la CRL publicada por REGISTRO DIGITAL PRISMA.

Con respecto a la AC de REGISTRO DIGITAL PRISMA, las CRL se divulgan en el repositorio de REGISTRO DIGITAL PRISMA www.prisma.gt.

4.4.6.Disponibilidad de verificación de la revocación/estado en línea

Además de la publicación de las CRL, REGISTRO DIGITAL PRISMA proporciona información del estado del certificado a través de funciones de consulta en el repositorio de REGISTRO DIGITAL PRISMA. La información del estado del certificado se puede obtener a través de funciones de consulta basadas en la web, a través del repositorio de REGISTRO DIGITAL PRISMA en www.prisma.gt y REGISTRO DIGITAL PRISMA también proporciona información sobre el estado del certificado de OCSP. Los clientes que cuentan con el servicio de OCSP pueden revisar el estado del Certificado a través del uso del OCSP.

4.4.7.Requisitos de verificación de la revocación en línea

Si una PARTE QUE CONFÍA no revisa el estado del certificado en que desea confiar consultando la CRL pertinente más reciente, la PARTE QUE CONFÍA debe revisar el estado del Certificado.

4.4.8.Notificaciones especiales relativas al compromiso de la clave

REGISTRO DIGITAL PRISMA emplea métodos razonables para avisar a las PARTES QUE CONFÍAN y a los demás participantes de la PKI de REGISTRO DIGITAL PRISMA, si ésta descubre o tiene motivos para creer que se ha comprometido la clave privada de REGISTRO DIGITAL PRISMA como AC o como AR, como puede ser notificación vía correo electrónico, telefónica o cualesquiera otra que tenga al alcance.

4.4.9.Certificados de prueba

Para el exclusivo efecto de demostración, se podrá emitir certificados de prueba para que los posibles solicitantes a suscriptores puedan comprobar el uso de este. Para ello, el certificado de prueba deberá contener datos ficticios y deberá contener de forma evidente y visible, la mención de que es un certificado

de prueba o demo. Al ser un certificado prueba o demo, este no está vinculado a los datos de un solicitante SUSCRIPTOR real, por lo que la firma electrónica que se estampa por medio de este tipo de certificado es una firma electrónica simple la cual carece de certeza jurídica. Sin embargo, el certificado sí cuenta con las características técnicas que se emplean para los certificados emitidos para firma electrónica avanzada y adicionalmente, figura REGRISTRO DIGITAL PRISMA, como AC que lo emite.

REGISTRO DIGITAL PRISMA divulgará en su repositorio, la emisión y en su caso, la revocación de los certificados de prueba que sean emitidos, mismos que quedarán identificados como tales de manera que no genere dudas.

4.5. Procedimientos de auditoría de seguridad

4.5.1.Tipos de eventos registrados

REGISTRO DIGITAL PRISMA mantiene evidencia de los siguientes eventos importantes:

- Eventos de administración del ciclo de vida del certificado del SUSCRIPTOR, incluyendo:
    - Solicitudes, Renovación y revocación de Certificados
    - Generación y emisión de Certificados y CRLs.

- Eventos relativos a la seguridad, incluyendo
    - Acciones PKI y del sistema de seguridad que lleva a cabo el personal de REGISTRO DIGITAL PRISMA
    - Cambios en el perfil de seguridad
    - Caídas del sistema, fallas en el hardware y otras anomalías; Entrada/salida de visitantes a las instalaciones de la AC.

Entre los datos del registro, se encuentran los siguientes detalles:

- Fecha y hora de registro
- Número de serie o secuencia de registro, cuando se trata de registros diarios automáticos.
- Tipo de registro.

La información de registro de la solicitud del certificado de la AR de REGISTRO DIGITAL PRISMA y de la Autoridad de Certificación subordinada, cuando aplique incluyendo:

- Tipo de documento(s) de identificación presentado(s) por el solicitante del certificado.

- Registro de los datos y números de identificación o la combinación de éstos (por ejemplo, el número del Pasaporte del Solicitante del Certificado) de los documentos de identificación, si se aplica, lugar donde se almacenan las copia de las solicitudes y los documentos de identificación.
- Identidad de la entidad que acepta la solicitud.
- Método usado para validar los documentos de identificación, en su caso.
- Nombre de la AR que presenta, si aplica.

4.5.2.Frecuencia del registro de procesamiento

Los registros de auditoría se examinan por lo menos cada semana, en busca de eventos de seguridad y de operación. Asimismo, REGISTRO DIGITAL PRISMA revisa si en sus registros de auditoría se comprueba la existencia de actividad sospechosa o inusual en respuesta a las alertas que se generan con base en irregularidades e incidentes dentro de los sistemas de AC y AR de REGISTRO DIGITAL PRISMA.

El procesamiento del registro de auditoría consiste en una revisión de los registros y documentos en busca de todos los eventos importantes resultando en un resumen del registro de auditoría. Entre las revisiones del registro de auditoría se encuentran la verificación de que el registro no haya sido alterado, una breve inspección de todos los asientos del registro y una investigación más completa de las alertas o irregularidades de los registros. Las acciones que se lleven a cabo con base en las revisiones del registro de auditoría, también se pueden documentar.

4.5.3.Registro de los archivos de auditoría

Los archivos de registros de auditoría electrónicos y manuales, están protegidos de ser revisados, vistos, modificados o suprimidos sin autorización, o de cualquier otro modo alterado mediante el uso de controles de acceso físico y lógico.

4.5.4.Procedimientos de respaldo (backup) del registro de auditoría

Se crean respaldos de los registros de auditoría y se hacen respaldos completos.

4.5.5.Sistema automático de auditoría

Se generan y registran datos de auditoría automatizados a nivel de solicitud, red y sistema operativo.

4.5.6.Análisis de vulnerabilidades

Los eventos del proceso de auditoría se registran, en parte, para vigilar las vulnerabilidades del sistema. Los análisis de vulnerabilidades ("AV") se llevan a cabo, revisan y enmiendan después de un examen de estos eventos supervisados. Los AV se basan en datos de registro automatizados de tiempo real y se llevan a cabo en forma diaria, mensual y anual, de acuerdo con la Política de vulnerabilidades técnicas.

4.6. Archivo de registros

4.6.1.Tipos de eventos registrados

Además de los registros de auditoría que se especifican en el apartado 4.5 con estas CPS, REGISTRO DIGITAL PRISMA lleva registros que comprenden documentos de:

- El cumplimiento de REGISTRO DIGITAL PRISMA con estas CPS y otras obligaciones conforme al contrato con sus suscriptores, sus acciones e información que son substanciales para cada solicitud de certificado y para la creación, emisión, uso, revocación, vencimiento y reposición de la clave o renovación de todos los certificados que emite desde el centro de procesamiento.

Los registros de los eventos del ciclo de vida del Certificado de REGISTRO DIGITAL PRISMA comprenden:

- La identidad del SUSCRIPTOR nombrado en cada certificado;
- La identidad de las personas que solicitan la revocación del certificado.

Otra información que puede contener el certificado pueden ser ciertos hechos materiales previsibles relacionados con la emisión de certificados incluyendo de manera enunciativa y no limitativa, información pertinente para concluir en forma exitosa una auditoria de cumplimiento conforme al apartado 2.7 de éstas CPS se pueden guardar en los registros en forma electrónica o en impresión, siempre y cuando dichos registros tengan un índice, se almacenen, conserven y reproduzcan en forma precisa y completa.

4.6.2.Período de retención del archivo

Los registros asociados con un Certificado se guardan, en formato digital u otro disponible por lo menos durante el término exigido en la ley que regule el acto o negocio jurídico en particular, o por diez años en caso de no existir dicho término. Si es necesario, REGISTRO DIGITAL PRISMA puede implementar períodos de retención más largos, con el fin de cumplir con otras las leyes y normativas aplicables.

4.6.3.Protección del archivo de Registro Digital Prisma

REGISTRO DIGITAL PRISMA protege sus registros archivados compilados, de modo que sólo Personas de Confianza autorizadas tengan permiso de acceder a los datos archivados. Los datos archivados electrónicamente están protegidos contra el acceso, modificación, supresión u otras alteraciones no autorizadas, a través de la implementación de controles de accesos físicos y lógicos apropiados. Los medios que guardan los datos de los archivos y las aplicaciones necesarias para procesar los datos del archivo, se guardan para garantizar que se puede acceder a los datos archivados durante el período.

4.7. Cambio de situación de la clave

Los pares de claves de REGISTRO DIGITAL PRISMA se retirarán al final de la duración solicitada por el Suscriptor, la cual no podrá exceder de 3 años. Los Certificados de la AC de REGISTRO DIGITAL PRISMA se pueden renovar mientras la vida acumulada del certificado del par de claves de la AC no supere la máxima vida del par de claves de la AC. Se generarán nuevos pares de claves conforme sea necesario, por ejemplo, para sustituir los pares de clave de la AC que se están retirando, para adicionar pares de claves activos, existentes, y soportar nuevos servicios.

4.8. Recuperación de desastres

REGISTRO DIGITAL PRISMA ha implantado una combinación robusta de controles físicos, lógicos y de procedimiento para minimizar el riesgo y el impacto potencial del compromiso de la clave privada en caso de un desastre. Asimismo, REGISTRO DIGITAL PRISMA ha implementado los procedimientos de respuesta para tales situaciones. Los procedimientos de compromiso de clave han sido desarrollados para minimizar el impacto potencial de dicho suceso y restaurar las operaciones dentro de un tiempo razonable.

4.8.1.Corrupción de los recursos de computación, software y/o datos

En caso de corrupción de los recursos de computación, software y/o datos que ocurra en los sistemas de AC se da a conocer la Política seguridad que adopte REGISTRO DIGITAL PRISMA en la que se instituyen los procedimientos de manejo de incidentes. Estos procedimientos exigen el adecuado escalamiento, investigación de incidentes y respuesta de incidentes. Si es necesario, se implementarán dentro de los procedimientos de compromiso de la clave o recuperación de desastres de REGISTRO DIGITAL PRISMA.

4.9. Cese de REGISTRO DIGITAL PRISMA como AC

En caso de que sea necesario que REGISTRO DIGITAL PRISMA deje de funcionar como AC, ésta informará al RPSC con anticipación sobre esta circunstancia. REGISTRO DIGITAL PRISMA llevará a cabo los procedimientos razonables para avisarle a los suscriptores, debiendo de comunicarlo previamente a cada uno de los Suscriptores de firmas electrónicas certificadas por REGISTRO DIGITAL PRISMA, con antelación de al menos quince (15) días hábiles y señalando al titular que de no existir objeción a la transferencia de los certificados a otro prestador de servicios de certificación, dentro del plazo de quince (15) días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos. En este caso, si REGISTRO DIGITAL PRISMA es autorizada, deberá ésta de traspasar los certificados, necesariamente, a un certificador autorizado en la fecha en que el cese se produzca.

En caso de existir oposición, REGISTRO DIGITAL PRISMA dejará sin efecto, revocando los certificados respecto de los cuales el Suscriptor se haya opuesto a la transferencia.

5. Controles de seguridad del personal, de procedimientos y físicos

REGISTRO DIGITAL PRISMA ha implementado la política de seguridad, la cual soporta los requisitos de seguridad de estas CPS.

5.1. Controles físicos

5.1.1.Localización

Las operaciones de la AC de REGISTRO DIGITAL PRISMA se llevan a cabo dentro de un ambiente protegido físicamente, destinado para frenar, prevenir y detectar el ingreso encubierto o abierto de personas no autorizadas. Así mismo, las operaciones de AR de REGISTRO DIGITAL PRISMA cuentan con los elementos necesarios, la debida protección física y cumplen con los estándares internacionales ISO 27001:2013 e ISO 9001:2015.

5.1.2.Acceso físico

Los sistemas de la AC de REGISTRO DIGITAL PRISMA están protegidos con accesos de seguridad biométricos.

5.1.3.Almacenamiento de medios

Todos los medios que contienen software y datos de producción, información de auditoría, archivos o de respaldo, se almacenan dentro de las instalaciones de REGISTRO DIGITAL PRISMA o en otro almacén fuera de éstas, con los controles de acceso físicos y lógicos apropiados, diseñados para limitar el acceso al personal autorizado y proteger a estos medios de daños accidentales (por ejemplo, de agua, fuego y electromagnéticos).

5.1.4.Respaldo fuera de las instalaciones

REGISTRO DIGITAL PRISMA como AC lleva a cabo respaldos de rutina de los datos de sistema críticos, los datos de registro de auditoría y otro tipo de información sensible.

5.1.5.Política y procedimiento para el uso y reciclaje de medios de almacenamiento de información sensible

REGISTRO DIGITAL PRISMA como AC cuenta con un sistema automatizado de respaldo de toda la información sensible y contrata con terceros ya sea en Guatemala o en el extranjero para garantizar este extremo. Estos respaldos se llevan a cabo en formato digital. El sistema de respaldo está configurado para llevar a cabo respaldos que se incrementan diariamente, completos bimensualmente y se transfiere la información respaldada a los medios dispuestos para su almacenamiento. Estos medios permanentes se almacenan de conformidad con los estándares más altos de seguridad provistos por terceros de confianza y que han sido previamente contratados por REGISTRO DIGITAL PRISMA.

5.2. Controles de Procedimiento

5.2.1.Funciones de confianza

Las personas de confianza por lo general comprenden a todos los empleados, contratistas y consultores que tienen acceso o controlan las operaciones de autenticación, así como los sistemas criptográficos que pueden afectar en forma substancial:

- La validación de la información en las solicitudes de certificados, la aceptación, rechazo u otro tipo de procesamiento de las solicitudes de Certificados, solicitudes de revocación o de renovación o información de inscripción;
- La emisión o revocación de Certificados, incluyendo al personal que tiene acceso a partes restringidas de su repositorio;
- El manejo de información o solicitudes del SUSCRIPTOR.

Entre las personas de confianza se encuentran, de manera enunciativa y no limitativa: alta dirección, gerencia, operador PKI, operador AC, personal de seguridad de la información, personal de gestión de calidad, personal de tecnología, personal de recursos humanos, asesor legal y ejecutivos que están destinados a manejar la confiabilidad de la infraestructura de REGISTRO DIGITAL PRISMA. Se toman en consideración las categorías de personal identificado en esta sección como personas de confianza.

5.2.2.Número de personas que se necesitan por tarea:

REGISTRO DIGITAL PRISMA mantiene procedimientos de política y riguroso control para garantizar la distribución de los deberes con base a las obligaciones y responsabilidades que le corresponde a cada puesto. Las tareas más sensibles, como el acceso al hardware criptográfico de la AC (unidad de firma criptográfica o HSM) y al material asociado de la clave, y su administración, se encuentran ubicados en los servicios de Data Center de Amazon Web Services (AWS) que cuenta con todas las certificaciones y seguridad con estándares internacionales, como ISO 27001:2013 y TIER III, que garantizan la seguridad de la información.

5.2.3.Identificación y autentificación de cada función

La verificación de la identidad de todo el personal que quiere ser persona de confianza se lleva a cabo a través de la presencia física de dicho personal ante las personas de confianza que se encargan de los recursos humanos de REGISTRO DIGITAL PRISMA o de las funciones de seguridad y verifican las formas bien reconocidas de identificación (por ejemplo, documento personal de identificación, los pasaportes y las licencias de manejo).

REGISTRO DIGITAL PRISMA garantiza que al PERSONAL se le da la calidad de PERSONAL DE CONFIANZA y una vez adquirida esta calidad garantizará que:

- Se le haya dado de alta en los dispositivos de acceso y se le haya dado acceso a las instalaciones necesarias;
- Se le haya emitido el certificado de firma electrónica avanzada, para autenticarse en los sistemas de AC y AR de REGISTRO DIGITAL PRISMA.
- Se le asigna usuario y contraseña para otros sistemas de tecnología de la información de REGISTRO DIGITAL PRISMA a los que tenga acceso permitido.

5.3. Controles de personal

5.3.1.Requisitos de antecedentes y visto bueno

El personal que quiere ser persona de confianza debe presentar un comprobante de los antecedentes (penales, policiacos, bancarios, entre otros) calificaciones y experiencia que se le piden para llevar a cabo las responsabilidades del empleo potencial en forma competente y satisfactoria, y cualquier acreditación gubernamental, en su caso, que sean necesarios para llevar a cabo servicios de certificación conforme a contratos gubernamentales. El personal que ocupa puestos de confianza deberá renovar cada año y por ende repetir las verificaciones de los antecedentes.

Adicionalmente el personal de REGISTRO DIGITAL PRISMA debe firmar un acuerdo de confidencialidad durante el proceso de contratación y durante su empleo. Cuando un empleado termina su relación laboral con REGISTRO DIGITAL PRISMA se siguen todos los pasos necesarios para revocar sus accesos lógicos y físicos incluyendo el recibo de gafetes, claves criptográficas, bloqueo de cuentas, etc. y la notificación a todos los empleados y guardias de REGISTRO DIGITAL PRISMA del estatus de esa persona.

5.3.2.Procedimientos de verificación de los antecedentes

Antes de iniciar el empleo en un rol de confianza, REGISTRO DIGITAL PRISMA lleva a cabo verificaciones de los antecedentes, que comprenden lo siguiente:

- Confirmación de empleo anterior, verificación de referencia profesional, confirmación del grado educativo más alto o importante obtenido, búsqueda de antecedentes (penales, policiacos, comerciales, bancarios entre otros).
- Verificación de registros o bases de datos en los que consten antecedentes crediticios/financiero.

En la medida en que algunos de los requisitos que impone esta sección no se puedan satisfacer, en virtud de la prohibición o limitación de las leyes aplicables o de otras circunstancias, REGISTRO DIGITAL PRISMA utilizará una técnica de investigación alterna que permita validar la información de una persona que desea obtener un puesto de confianza.

Entre los factores revelados en una verificación de antecedentes que puedan considerarse fundamentos para rechazar a candidatos para que ocupen puestos de confianza o que tomen medidas en contra de una persona de confianza existente, generalmente se encuentran los siguientes:

- Declaraciones falsas hechas por el candidato o la persona de confianza,

- Referencias personales altamente desfavorables o desconfiables
- Condenas penales
- Indicaciones de falta de responsabilidad financiera.

El personal de recursos humanos y de seguridad evalúa los informes que contienen los datos mencionados con anterioridad y éste determinará el curso de acción apropiado a la luz del tipo, magnitud y frecuencia de la conducta revelada en la verificación de los antecedentes. Estas acciones pueden comprender medidas que incluyan la cancelación de ofertas de empleo que se les hayan hecho a los candidatos para ocupar puestos de confianza o el cese de la relación de REGISTRO DIGITAL PRISMA con las personas de confianza.

El uso de información revelada en la verificación de los antecedentes para llevar a cabo estas acciones, está sujeto al ordenamiento jurídico de Guatemala.

5.3.3.Requisitos de capacitación

REGISTRO DIGITAL PRISMA le proporciona a su personal capacitación al contratarlo, así como la capacitación en el empleo necesaria para que el personal pueda desempeñar el puesto que ocupa en forma competente y satisfactoria.

REGISTRO DIGITAL PRISMA revisa periódicamente sus programas de capacitación, como sea necesario. Los programas de capacitación de REGISTRO DIGITAL PRISMA se ajustan a las responsabilidades de la persona y los puntos importantes que comprenden, son:

- Conceptos básicos de las PKI,
- Responsabilidades del puesto
- Políticas y procesamientos de seguridad y operación de REGISTRO DIGITAL PRISMA
- Uso y operación del HARDWARE Y SOFTWARE desplegado
- Elaboración de informes y manejo de incidentes y compromisos y
- Procedimientos de recuperación de desastres y continuidad de los negocios.

5.3.4.Frecuencia y requisitos de nuevos cursos de capacitación

REGISTRO DIGITAL PRISMA proporciona cursos de capacitación y actualización a su personal, en la medida y frecuencia necesarias para garantizar que dicho personal mantenga el nivel necesario de pericia para llevar a cabo las responsabilidades de su puesto en forma competente y satisfactoria. Se da capacitación

en seguridad periódica y continua.

5.3.5.Sanciones para acciones no autorizadas

Se toman las medidas disciplinarias adecuadas cuando se llevan a cabo acciones no autorizadas o se violan las políticas y procedimientos de REGISTRO DIGITAL PRISMA. Las medidas disciplinarias pueden comprender hasta el cese de la relación entre el personal y REGISTRO DIGITAL PRISMA y se aplican de acuerdo con la frecuencia y severidad de las acciones no autorizadas.

5.3.6.Requisitos del personal que se contrata

En circunstancias limitadas, se pueden utilizar asesores, contratistas o consultores independientes para ocupar puestos de confianza. A dicho asesor, contratista o consultor se le aplican los mismos criterios funcionales y de seguridad que se les aplican a los empleados de REGISTRO DIGITAL PRISMA en un puesto equiparable.

Los contratistas y consultores independientes que no han cumplido con los procedimientos de verificación de los antecedentes, pueden acceder a las instalaciones seguras de REGISTRO DIGITAL PRISMA, sólo en la medida en que sean supervisados directamente por personas de confianza.

Todo el personal autorizado que esté laborando en REGISTRO DIGITAL PRISMA debe de tener un gafete visible con una foto. El asesor, contratista o consultor que esté dentro de las instalaciones debe de tener un gafete de visitante. Los controles de acceso de todos los empleados, contratistas, consultores y visitantes se determinarán según las políticas de empleados de confianza, detallado en el documento "Política de empleados de confianza". Los gafetes de visitante se emiten solamente con el recibo de una identificación oficial vigente y los gafetes permanentes de los empleados serán emitidos por el Encargado de Capital Humano solamente después de que el empleado haya cumplido con todos los requisitos de empleado de confianza.

5.3.7.Documentación que se proporciona al personal

El personal de REGISTRO DIGITAL PRISMA que participa en la operación de los servicios de PKI de REGISTRO DIGITAL PRISMA debe leer estas CPS, las CP y la política de seguridad de REGISTRO DIGITAL PRISMA. Esta última les proporciona a sus empleados la capacitación necesaria y los documentos requeridos para llevar a cabo las responsabilidades de su puesto en forma competente y satisfactoria.

6. Controles de seguridad técnicos

6.1. Generación e instalación de par de claves

6.1.1.Generación del par de claves

Estos registros se guardan para fines de auditoría y rastreo, durante el tiempo que la administración de REGISTRO DIGITAL PRISMA considere apropiado.

6.1.2.Entrega de la clave pública de la AC a los SUSCRIPTORES y PARTES QUE CONFÍAN

REGISTRO DIGITAL PRISMA, pone a disposición de los SUSCRIPTORES y de las PARTES QUE CONFÍAN, la Clave Pública de sus Certificados de AC, como Raíz, y la Clave Pública como Autoridad Intermedia, en su sitio web www.prisma.gt.

REGISTRO DIGITAL PRISMA proporciona la cadena de certificados completa al SUSCRIPTOR usuario final al emitir el Certificado.

6.1.3.Tamaños de clave

Los pares de claves de la AC de REGISTRO DIGITAL PRISMA son como mínimo RSA de 4096 bits. La llave pública que se encuentra dentro del certificado AC de REGISTRO DIGITAL PRISMA tiene un tamaño de 4,096 bits. Los pares de claves de los SUSCRIPTORES usuarios finales generan pares de clave RSA de 2,048 bits.

6.1.4.Generación de la clave del hardware/software

REGISTRO DIGITAL PRISMA genera el par de claves de la AC en los módulos criptográficos de hardware apropiados. Los pares de claves de la AR y el SUSCRIPTOR pueden generarse en hardware o software en un dispositivo seguro.

6.1.5.Propósitos de uso de clave (Según campo de uso de clave X.509 versión 3)

Con respecto a los Certificados X.509 versión 3, REGISTRO DIGITAL PRISMA por lo general llena la extensión KeyUsage (Uso de la Clave) de los Certificados, de acuerdo con la RFC 2459: “Certificado de Infraestructura de la Clave Pública Internet X.509 y Perfil de la CRL, de enero de 1999”. En el caso de REGISTRO DIGITAL PRISMA:

- La extensión KeyUsage no se usa con los certificados de servidor SSL y los Certificados de personas individuales.
- La criticidad de la extensión KeyUsage se puede fijar en “TRUE” segura y sólida con respecto a otros Certificados en el futuro.

6.2. Protección de la Clave Privada

REGISTRO DIGITAL PRISMA ha implementado una combinación de controles físicos, lógicos y de procedimientos para garantizar la seguridad de las claves privadas de la AC de REGISTRO DIGITAL PRISMA y los clientes de REGISTRO DIGITAL PRISMA. En el contrato de SUSCRIPTOR se exige que los SUSCRIPTORES se responsabilicen de la guardia y custodia de sus claves privadas y tomen las medidas necesarias para evitar la pérdida, divulgación, modificación o uso no autorizado de dichas claves privadas.

6.2.1.Normas para los módulos criptográficos

Para la generación de pares de claves de la AC Raíz emisora y el almacenamiento de claves privadas de la AC, REGISTRO DIGITAL PRISMA usa módulos criptográficos de hardware que están certificados en FIPS 140:2 Nivel 3 o substancialmente cubren los requisitos de éste. El HSM de la AC Raíz de REGISTRO DIGITAL PRISMA genera sus claves en cumplimiento con el estándar FIPS 140:2 NIVEL 3.

6.2.2.Clave privada (N de M) control de múltiples personas

REGISTRO DIGITAL PRISMA ha implementado mecanismos técnicos y de procedimiento que requieren de la participación de varias personas de confianza para que lleven a cabo las operaciones criptográficas sensibles de la AC. REGISTRO DIGITAL PRISMA utiliza la “Participación Secreta” para dividir los datos de activación necesarios para hacer uso de la clave privada en partes por separado: En dicha operación participan los administradores/operadores de la AC con acceso al HSM y personal de confianza designado dentro de las políticas internas de la institución.

6.2.3.Política de la clave privada

REGISTRO DIGITAL PRISMA no entrega en depósito claves privadas de la AC, AR y del SUSCRIPTOR usuario final a ningún tercero con el fin de que acceda al dispositivo de seguridad. REGISTRO DIGITAL PRISMA tampoco mantiene un depósito de las llaves privadas generadas por los SUSCRIPTORES de usuario final. Es responsabilidad del usuario final generar su propia clave privada, los términos y condiciones se detallan en el contrato de SUSCRIPTOR aplicable.

6.2.4.Respaldo de la clave Privada

REGISTRO DIGITAL PRISMA mantiene una copia de respaldo de las claves privadas necesarias para fines de recuperación de rutina y recuperación de desastres. Estas claves se almacenan en forma encriptada dentro de los módulos criptográficos.

REGISTRO DIGITAL PRISMA no almacena o crea copias de seguridad de las claves privadas de la Autoridad de Registro.

6.2.5.Archivo de la clave privada

Cuando los pares de claves de la AC llegan al fin de su período de validez, dichos pares de claves de la AC se archivarán durante un período de por lo menos 10 años. Los pares de claves de la AC archivados, se almacenarán en forma segura usando los módulos criptográficos de software que cubran los requisitos correspondientes. Los controles de los procedimientos evitan que los pares de claves de la AC archivados se devuelvan al uso de producción. Al final del período de archivo, las claves privadas de la AC archivadas se destruirán en forma segura. REGISTRO DIGITAL PRISMA no archiva copias de las claves privadas de la AR ni del SUSCRIPTOR.

6.2.6.Entrada de la clave privada al módulo criptográfico

REGISTRO DIGITAL PRISMA como AC es quien genera los pares de claves en los módulos criptográficos de hardware en los que las claves van a utilizarse. Asimismo, REGISTRO DIGITAL PRISMA saca copias de dichos pares de claves para fines de recuperación de rutina y de recuperación de desastres. Cuando los pares de claves de la AC se respaldan en otro módulo criptográfico de hardware, esos pares de claves se transportan entre los módulos en forma encriptada.

6.2.7.Método de activación de la clave privada

Todos los participantes en las PKI de REGISTRO DIGITAL PRISMA deben proteger los datos de activación de sus claves privadas, de manera que no se pierdan, no sean robados, no sean modificados, se divulguen o se usen en forma no autorizada.

i. Claves privadas del suscriptor usuario final

Esta sección se aplicará a los procedimiento de REGISTRO DIGITAL PRISMA para proteger los datos de activación de las claves privadas (cuando sea aplicable) de los SUSCRIPTORES usuarios finales para las PKI de REGISTRO DIGITAL PRISMA. Asimismo, los SUSCRIPTORES tienen la opción de usar mecanismos de protección de la clave privada disponibles en la actualidad, incluyendo el uso de tarjetas inteligentes, dispositivos de acceso biométricos y otros códigos de hardware para almacenar claves privadas. Se sugiere el uso de dos mecanismos de autenticación como por ejemplo, contraseña y frase de ingreso combinado al sistema, sistemas biométricos y contraseña o biométrica y frase de ingreso combinados.

6.2.8.Método de desactivación de la clave privada

Las claves privadas de la AC de REGISTRO DIGITAL PRISMA se desactivan al quitarse del lector de contraseña. Las claves privadas de la AR de REGISTRO DIGITAL PRISMA (que se usa para la autenticación de la solicitud de la AR), se desactivan cuando desconectan el sistema. Es necesario que las AR de REGISTRO DIGITAL PRISMA desconecten sus estaciones de trabajo cuando salen de su área de trabajo.

Las claves privadas de los usuarios finales se pueden desactivar mediante su exportación a otro dispositivo criptográfico. En todos los casos, los SUSCRIPTORES usuarios finales tienen la obligación de proteger adecuadamente su(s) clave(s) privada(s).

6.2.9.Método de destrucción de la clave privada

A la conclusión de la vida de operación de la AC de REGISTRO DIGITAL PRISMA, se archivan una o más copias de la clave privada de la AC. Las copias restantes de la clave privada de la AC se destruyen en forma segura. Asimismo, las claves privadas de la AC archivadas se destruyen en forma segura cuando concluyen sus períodos de archivo. Las actividades de destrucción de la clave de la AC requieren de la participación de varias personas de confianza. Cuando se requiere, REGISTRO DIGITAL PRISMA destruye las claves

privadas de la AC, de manera que garantice en forma razonable que no quedan restos de la clave que pudieran dar como resultado la reconstrucción de ésta. REGISTRO DIGITAL PRISMA utiliza la función de desmagnetización y borrado de sus módulos criptográficos de hardware y otros medios apropiados para garantizar la destrucción completa de las claves privadas de la AC. Cuando se llevan a cabo, se registran las actividades de destrucción de la clave de la AC. En todo caso, se dará aviso al Registro de Prestadores de Servicios de Certificación del Ministerio de Economía (RPSC).

6.3. Otros aspectos de la administración del par de claves

6.3.1.Archivo de la clave pública

Los certificados de la AC, AR y SUSCRIPTOR usuario final de REGISTRO DIGITAL PRISMA, están respaldados y archivados como parte de los procedimientos de respaldo de rutina de REGISTRO DIGITAL PRISMA.

6.3.2.Períodos de uso para las claves públicas y privadas

El período de operaciones de un certificado termina a su vencimiento o revocación. El período de operación de los pares de claves es igual al período de operación de los certificados asociados, salvo que las claves privadas pueden continuar usándose en el archivo no encriptado y las claves públicas pueden continuar usándose en la verificación de firmas. Los períodos de operación máximos para los certificados de REGISTRO DIGITAL PRISMA emitidos en la fecha efectiva de estas CPS o después, se establecen en el siguiente cuadro.

Certificado Emitido por:	Período de validez
REGISTRO DIGITAL PRISMA, como AC y AR, auto-firmado (4096 bits)*	Hasta 10 años
REGISTRO DIGITAL PRISMA a Suscriptor usuario final (individual o persona jurídica).	hasta 3 años después de la emisión o renovación

*Auto Firmado: Emitido por REGISTRO DIGITAL PRISMA, a sí mismo, para ambas funciones: AC y AR.
Cuadro – Períodos de Operación del Certificado.

6.4. Datos de activación

6.4.1.Generación e instalación de datos de activación

Los datos de activación (frase de inicio e ingreso de claves secretas o privadas) que se usan para proteger contraseñas que contienen las claves privadas de REGISTRO DIGITAL PRISMA, se generan de acuerdo con los requisitos que establecen las CPS.

Los Suscriptores y AR de REGISTRO DIGITAL PRISMA, tienen que seleccionar contraseñas seguras o robustas para proteger sus claves privadas. Las directrices para la selección de las contraseñas de REGISTRO DIGITAL PRISMA exigen que las contraseñas:

- Sean generadas por el usuario,
- Tengan por lo menos ocho caracteres,
- Tengan por lo menos un carácter alfabético y un carácter numérico (alfanumérico),
- Tengan por lo menos una letra minúscula,
- No contengan muchas repeticiones del mismo carácter,
- No sean iguales al nombre de perfil del operador y,
- No contengan una sub-cadena larga del nombre de perfil del usuario

REGISTRO DIGITAL PRISMA sugiere el uso del mecanismo de autenticación de dos factores para obtener mayor seguridad en el acceso a sus claves, por ejemplo, las siguientes combinaciones: acceso biométrico y contraseña, contraseña y frase, etc.

6.4.2.Protección de datos de activación

Los iniciadores del sistema de PKI de REGISTRO DIGITAL prisma deben salvaguardar sus claves y contraseñas secretas y firman un contrato reconociendo sus responsabilidades como iniciador.

REGISTRO DIGITAL PRISMA recomienda firmemente que los Administradores, y los SUSCRIPTORES usuarios finales, almacenen sus claves privadas en forma encriptada y protejan sus claves privadas a través del uso de una contraseña de hardware y/o una frase de ingreso que contenga un nivel alto de seguridad. Se promueve el uso de dos mecanismos de autenticación de factor (por ejemplo, contraseña y frase de ingreso, biométrica y contraseña y todas combinadas).

6.5. Controles de Seguridad de Computadoras

REGISTRO DIGITAL PRISMA lleva a cabo todas las funciones de AC y AR usando sistemas confiables que cubran los requisitos mínimos de seguridad dentro de las computadoras de los colaboradores y administradores.

6.5.1.Requisitos Técnicos de los sistemas de la AC:

REGISTRO DIGITAL PRISMA garantiza que los sistemas que alberguen el software y archivos de datos de

la AC sean sistemas confiables protegidos contra acceso no autorizado. Además, REGISTRO DIGITAL PRISMA limita el acceso a los servidores de producción a las personas que no tienen un motivo válido para dicho ingreso. Los usuarios de aplicación general no tienen cuentas en los servidores de producción.

La red de producción de REGISTRO DIGITAL PRISMA está separada lógicamente de otros componentes. Esta separación evita el acceso a la red, salvo a través de procesos de aplicación definidos. REGISTRO DIGITAL PRISMA utiliza sistemas de seguridad incluyendo firewalls que con un conjunto de dispositivos configurados para permitir, limitar, cifrar descifrar el tráfico ante diferentes ámbitos sobre la base de normas y otros criterios y que tiene como fin, en este caso concreto, proteger la red de producción del acceso no autorizado y limitar la naturaleza y la fuente de actividades de la red a la que puedan acceder los sistemas de producción.

REGISTRO DIGITAL PRISMA exige el uso de contraseñas que tienen una longitud de caracteres mínima y una combinación de caracteres alfanuméricos y especiales. REGISTRO DIGITAL PRISMA exige que se cambien las contraseñas en forma periódica.

El acceso directo a las bases de datos de REGISTRO DIGITAL PRISMA que soportan el repositorio de REGISTRO DIGITAL PRISMA, está limitado a las personas de confianza del grupo de operaciones de REGISTRO DIGITAL PRISMA que tienen un motivo válido para dicho acceso.

6.6. Controles técnicos de ciclo de vida

6.6.1.Controles de Desarrollo de Sistema

REGISTRO DIGITAL PRISMA implementa las solicitudes de acuerdo con las normas de administración del desarrollo y cambio de sistemas.

El software de REGISTRO DIGITAL PRISMA como AC, cuando se carga por primera vez, ofrece un método para verificar que el software del sistema proveniente de REGISTRO DIGITAL PRISMA cuando actúa como AC, no ha sido modificado antes de la instalación, y es la versión planeada para usarse.

6.6.2.Controles de Administración de la Seguridad

REGISTRO DIGITAL PRISMA tiene mecanismos y/o políticas en funcionamiento para controlar y supervisar la configuración de sus sistemas de AC. REGISTRO DIGITAL PRISMA crea una comprobación aleatoria de todos los paquetes de software y de las actualizaciones del software de REGISTRO DIGITAL

PRISMA. Esta comprobación aleatoria se usa para verificar la integridad de dicho software en forma manual. Desde la instalación y en forma periódica, REGISTRO DIGITAL PRISMA valida la integridad de sus sistemas de AC.

6.7. Controles de Seguridad de la Red

REGISTRO DIGITAL PRISMA lleva a cabo todas sus funciones de AC y AR usando redes protegidas para evitar el acceso no autorizado y otro tipo de actividad maliciosa. REGISTRO DIGITAL PRISMA protege sus comunicaciones de información sensible a través del uso de la encriptación y las firmas electrónicas y/o firmas electrónicas avanzadas.

7. Certificado, y Perfil de la CRL

7.1. Perfil del Certificado

Las CPS definen el Perfil del Certificado de REGISTRO DIGITAL PRISMA y los requisitos de contenido de las PKI DE REGISTRO DIGITAL PRISMA emitidos conforme a estas CPS. Los Certificados de REGISTRO DIGITAL PRISMA se conforman con (a) ITU Recomendación; X.509 versión 3 (1997): Tecnología de la Información – Interconexión de los Sistemas Abiertos – El Directorio marco de Autenticación, junio de 1997 y (b) RFC 2459: Internet X.509 versión 3 Certificado de Infraestructura de la Clave Privada y Perfil de la CRL, enero de 1999 (“RFC 2459”).

7.1.1.Número(s) de Versión

Los Certificados de la AC de REGISTRO DIGITAL PRISMA y del SUSCRIPTOR usuario final son Certificados X.509 versión 3.

7.1.2.Extensiones del Certificado

Cuando se usan Certificados X.509 versión 3, REGISTRO DIGITAL PRISMA llena los Certificados con las extensiones que exigen las CPS. Las extensiones privadas son permisibles mientras su uso sea congruente con las CP de las PKI de REGISTRO DIGITAL PRISMA y estas CPS.

i. **Uso de las Claves**

Cuando se usan Certificados X.509 versión 3, REGISTRO DIGITAL PRISMA llena la extensión KeyUsage, de acuerdo con el apartado 6.1.6 de la CPS. El campo de criticidad de esta extensión se pone en “FALSE”.

ii. **Extensión de las políticas de los Certificados**

Los certificados del SUSCRIPTOR usuario final X.509 versión 3 de REGISTRO DIGITAL PRISMA usa la extensión de Certificate Policies (Políticas de los Certificados). La extensión de Certificate Policies se llena con el identificador de objeto aplicable para las CP, de acuerdo con las CPS y con los calificadores de política que se establecen en las CPS. El campo de criticidad de esta extensión se pone en FALSE.

iii. **Restricciones básicas**

REGISTRO DIGITAL PRISMA llena los Certificados de la AC X.509 versión 3 con extensión de BasicConstraints (Restricciones Básicas) y el Tipo de Asunto se pone en AC. Los Certificados del SUSCRIPTOR usuario final también se llenarán con una extensión de BasicConstraints y el Tipo de Sujeto es igual a la Entidad Final. La criticidad de la extensión de BasicConstraints generalmente se pone en FALSE. La criticidad de esta extensión se puede poner en TRUE con respecto a otros Certificados en el futuro.

Los Certificados de la AC X.509 versión 3 de REGISTRO DIGITAL PRISMA emitidos para que tengan un campo de "pathLenConstraint" de la extensión de BasicConstraints puesto en el número máximo de certificados de la AC que pueden seguir a este Certificado en una trayectoria de certificación.

Los Certificados del SUSCRIPTOR usuario final tienen un campo "pathLenConstraint" puesto en un valor de "0", el cual indica que sólo el Certificado del SUSCRIPTOR usuario final puede seguir la trayectoria de certificación.

iv. **Uso de la Clave Extendida**

REGISTRO DIGITAL PRISMA hace uso de la extensión ExtendedKeyUsage (Uso de la Clave Extendida) en los tipos específicos de Certificados X.509 versión 3 de REGISTRO DIGITAL PRISMA que se describen en el cuadro siguiente.

Tipo de Certificado	
Autoridad Certificadora	AC del Servidor Internacional
Respondedor OCSP	Reapondedor OCSP Primarios Públicos Respondedor OCSP del Servidor Seguro
Certificados del Servidor de Web	Identificadores del Servidor Seguro Identificadores del Servidor Global

Cuadro – Certificados que usan la extensión ExtendedKeyUsage

v. **Puntos de Distribución de la CRL**

Los Certificados del Servidor Seguro X.509 versión 3 y del SUSCRIPTOR usuario final Individual de REGISTRO DIGITAL PRISMA utilizan la extensión CRLDistributionPoints (Puntos de Distribución de la CRL) que contiene la URL del lugar en el que una PARTE QUE CONFÍA puede obtener una CRL para verificar el estado del Certificado de la AC. El campo de criticidad de esta extensión se ajusta en FALSE. El uso de los Puntos de Distribución CRL se soportará para otras AC de REGISTRO DIGITAL PRISMA en el futuro.

vi. **Identificador de la Clave de Autoridad**

REGISTRO DIGITAL PRISMA llena la extensión Authority Key Identifier (Identificador de la Clave de la Autoridad) de los Certificados del SUSCRIPTOR usuario final X.509 versión 3 que emite la AC de REGISTRO DIGITAL PRISMA. El Identificador de la Clave de Autoridad está compuesto de la comprobación aleatoria SHA256 con RSA de la clave pública de la AC que emite el Certificado. El campo de criticidad de esta extensión se pone en FALSE.

vii. **Identificador de la Clave del Sujeto**

Cuando REGISTRO DIGITAL PRISMA llena los Certificados X.509 versión 3 con una extensión subjectKeyIdentifier, se genera el Identificador de Clave basado en la clave pública del Certificado del Sujeto. Cuando se usa esta extensión, el campo de criticidad de esta extensión se pone en FALSE.

viii. **Algoritmo de Firma del Certificado**

El algoritmo de firma del certificado es SHA256 con RSA.

7.1.3.Identificadores de objetos (OID) de la política de Certificados y Declaración de Prácticas de Certificación

El identificador de objeto de la Política de Certificados de la Autoridad de Certificación del PSC REGISTRO DIGITAL PRISMA es: 2.16.484.101.10.316.2.1.1.1.1.2.2.1.

Formas del Nombre

REGISTRO DIGITAL PRISMA llena los Certificados con un Nombre Distinguido del Emisor y del Sujeto, de acuerdo con el apartado 3.1.1 del CPS. Asimismo, REGISTRO DIGITAL PRISMA comprende dentro de los Certificados del SUSCRIPTOR usuario final un campo de Unidad Organizacional, que contiene un aviso que manifiesta que se establecen los términos de uso del Certificado en una URL que es indicador del Contrato

de la PARTE QUE CONFÍA. Sólo se permiten excepciones al requisito anterior cuando existan limitaciones de espacio, formato o interoperabilidad dentro de los Certificados, hacen que dicha Unidad Organizacional no pueda usarse junto con la aplicación para la que están destinados los certificados.

7.1.4.Identificador del objeto de la política del Certificado

Cuando se usa la extensión de políticas del Certificado, los Certificados contienen el identificador del objeto de la política del Certificado que le corresponde a la Clase de Certificado apropiada, como se manifiesta en la CPS.

7.1.5.Sintaxis y Semántica de los Calificadores de política

REGISTRO DIGITAL PRISMA llena los Certificados X.509 versión 3 con un calificador de política dentro de la extensión de CertificatePolicies (políticas de Certificado). Por lo general, estos Certificados contienen un calificador indicador de las CPS que remite al Contrato de la PARTE QUE CONFÍA o la CPS.
Asimismo, algunos Certificados contienen un Calificador del Aviso del Usuario que remite al Contrato de la PARTE QUE CONFÍA aplicable.

7.2. Perfil de la CRL

REGISTRO DIGITAL PRISMA emite CRL que se conforman con RFC 2459. Como mínimo, las CRL de REGISTRO DIGITAL PRISMA contienen los campos básicos y contenidos que se indican en el siguiente Cuadro:

CAMPO	VALOR O RESTRICCIÓN DEL VALOR
ALGORITMO DE LA FIRMA	ALGORITMO USADO PARA FIRMAR LA CRL. LAS CRL SE FIRMAN USANDO SHA-256 EN RSA.
EMISOR	LA ENTIDAD QUE FIRMÓ LA CRL. EL NOMBRE DEL EMISOR DE LA CRL ES CONFORME LOS REQUISITOS DEL NOMBRE DISTINGUIDO DEL EMISOR QUE SE INDICAN EN LA CPS.
FECHA EFECTIVA	FECHA DE EMISIÓN DE LA CRL. LAS CRL DE REGISTRO DIGITAL PRISMA SON EFECTIVAS AL EMITIRLAS
SIGUIENTE ACTUALIZACIÓN	FECHA EN QUE SE EMITIRÁ LA SIGUIENTE CRL. LA SIGUIENTE FECHA DE ACTUALIZACIÓN DE LAS CRL DE REGISTRO DIGITAL PRISMA SE ESTABLECE DE LA SIGUIENTE MANERA: 3 MESES A PARTIR DE LA FECHA EFECTIVA PARA REGISTRO DIGITAL PRISMA.
CERTIFICADOS REVOCADOS	LA LISTA DE LOS CERTIFICADOS REVOCADOS, INCLUYENDO EL NÚMERO DE SERIE DEL CERTIFICADO REVOCADO Y LA FECHA DE REVOCACIÓN.

Cuadro – Campos básicos del Perfil de la CRL.

7.2.1.Número(s) de Versión

REGISTRO DIGITAL PRISMA emite actualmente CRL X.509 versión 3.

8. Administración de Especificaciones

8.1. Procedimientos de Cambio de Especificación

8.1.1.Modificaciones sin Previo Aviso

REGISTRO DIGITAL PRISMA se reserva el derecho de modificar las CPS sin dar aviso de las modificaciones que no son sustanciales, incluyendo de manera enunciativa y no limitativa de errores tipográficos, cambios a las URL, y cambios para contactar información. La decisión de REGISTRO DIGITAL PRISMA de designar las modificaciones como sustanciales y no sustanciales, será a discreción exclusiva de REGISTRO DIGITAL PRISMA. Las modificaciones sustanciales de fondo deberán ser avisadas de conformidad con la ley al Registro de Prestadores de Servicios de Certificación (RPSC).

i. Tipos de Modificaciones

Modificaciones substanciales son los cambios que REGISTRO DIGITAL PRISMA considera que varían el fondo, el concepto o el sentido de una disposición incluida al tenor las CPS. Modificaciones no sustanciales, serán las no incluidas en el concepto anteriormente mencionado, y las que impliquen cambios solo de forma, sin alterar el fondo de lo dispuesto.

ii. Modificaciones Mediante Aviso Previo

REGISTRO DIGITAL PRISMA como AC periódicamente hará modificaciones sustanciales a la CPS, las cuales deberán ser autorizadas por el Registro de Prestadores de Servicios de Certificación (RPSC). Los cambios planeados serán publicados en www.prisma.gt/repositorio Las modificaciones de la versión anterior a la versión vigente de las CPS se registrarán en la sección 1.1 del CPS.

8.1.2.Mecanismo de Notificación

El grupo de Desarrollo de Prácticas de REGISTRO DIGITAL PRISMA publicará los cambios propuestos a las CPS en la sección de Actualizaciones y Avisos de Prácticas del Repositorio de REGISTRO DIGITAL PRISMA, el cual se ubica en: www.prisma.gt/repositorio. REGISTRO DIGITAL PRISMA solicita las modificaciones propuestas a las CPS de otros Participantes del Subdominio de REGISTRO DIGITAL PRISMA. Si este último considera que esta modificación es conveniente y propone aplicar la modificación, REGISTRO DIGITAL

PRISMA dará aviso de esa modificación, de acuerdo con esta sección.

No obstante, alguna disposición en contrario, si REGISTRO DIGITAL PRISMA cree que es necesario hacerle modificaciones sustanciales inmediatas a estas CPS para detener o prevenir una transgresión a la seguridad de las PKI de REGISTRO DIGITAL PRISMA tendrá derecho de hacer estas modificaciones mediante la publicación en su Repositorio. Estas modificaciones entrarán en vigor de inmediato a su publicación.

8.2. Políticas de Publicación y Notificación

8.2.1.Artículos que no se Publicaron en la CPS

Los documentos de seguridad que REGISTRO DIGITAL PRISMA se consideran de carácter confidencial y no se divulgan al público.

8.2.2.Distribución de la CPS

Estas CPS se publican en formato electrónico dentro del Repositorio de REGISTRO DIGITAL PRISMA en www.prisma.gt/biblioteca. La CPS está disponible en formato de Adobe Acrobat (.pdf).

8.3. Procedimientos de Aprobación de la CPS

La aprobación de estas CPS y sus anexos subsecuentes serán hechos por la Autoridad de administración de políticas (APP) de REGISTRO DIGITAL PRISMA. La aprobación de estas CPS y los anexos subsecuentes serán registrados por medio de un documento de notificación de actualización o por medio de un formulario adjuntado al CPS. Las versiones actualizadas y los anexos serán publicados en: www.prisma.gt/biblioteca. Las versiones actualizadas del CPS serán considerados como las versiones vigentes del mismo. La Autoridad de administración de políticas (APP) determinará si se debe cambiar los identificadores de objetos de la política de certificados que corresponden a cada clase de certificado. Todo cambio o modificación posterior, serán aprobados por el Registro de Prestadores de Servicios de Certificación (RPSC), previo a su publicación.

8.4. Vigencia y Finalización

8.4.1.Vigencia

Esta CPS entra en vigencia a partir de su publicación en el Repositorio de REGISTRO DIGITAL PRISMA. Las enmiendas para estas normas para el proceso de certificación entrarán en vigor a partir de su publicación en el Repositorio de REGISTRO DIGITAL PRISMA.

8.4.2.Finalización

Estas normas para el proceso de certificación, tal como sus modificaciones mantendrán su vigencia hasta que sean reemplazadas por una nueva versión.

8.4.3.Efectos de la Finalización y Supervivencia

Sin perjuicio, la finalización de la vigencia de las presentes normas para el Proceso de Certificación, todos los participantes de las PKI de REGISTRO DIGITAL PRISMA, estarán obligados por sus términos con relación a todos los certificados emitidos por el plazo de vigencia restante de dichos certificados.

9. Tabla de Acrónimos

Acrónimo	Término
AC	Autoridad de Certificación
ANSI	Instituto Americano de Estándares (American National Standards Institute).
AR	Autoridad de Registro (Registration Authority o RA).
CDP	CRL Distribution Points
CP	Política de Certificación (Certificate Policy)
CPS	Normas para el Proceso de Certificación (Certification Practice Statement).
CRL	Lista de Certificados Revocados (Certificate Revocation List).
FCA	Firma de Contenido Autenticado (Authenticated Content Signing o ACS)
FIPS	United States Federal Information Processing Standards.
ICC	Cámara Internacional de Comercio (International Chamber of Commerce).
KRB	Conjunto de Recupero de Clave (Key Recovery Block)
LSVA	Análisis lógico de vulnerabilidades de seguridad (Logical security vulnerability assessment).
OCSP	Protocolo de Estado del Certificado en Línea (Online Certificate Status Protocol).
PIN	Número de Identificación Personal (Personal identification number)
PKCS	Estándar Criptográfico de Clave Pública (Public-Key Cryptography Standard).
PKI	PKI (Public Key Infrastructure).
PMA	Autoridad de administración de la política (Policy Management Authority)
PSC	Prestador de Servicios de Certificación
RFC	Request for comment.
S/MIME	Secure multipurpose Internet mail extension.
SAR	Requerimientos de Seguridad y Auditoría (Security and Audit Requierements)
SSL	Secure Sockets Layer.

10.Glosario

Para efectos de interpretar las Políticas de Certificación (CP), la CPS (CPS), las Prácticas de Registro y los contratos relacionados con la PKI de REGISTRO DIGITAL PRISMA, se entiende por:

- **ACCESO:**
  Tipo específico de interacción entre la remisión y las comunicaciones o recursos informáticos que determinan un flujo de información, el ejercicio de un control o la actividad de un proceso.

- **ACEPTAR (UN CERTIFICADO)**
  Es el acto mediante el cual un solicitante aprueba un certificado al tomar conocimiento de la información contenida en el mismo, de acuerdo con la declaración para el Proceso de Certificación (CPS).

- **ACREDITACIÓN:**
  Declaración formal realizada por una autoridad de aprobación designada por REGISTRO DIGITAL PRISMA manifestando que un sistema informático determinado, un profesional o empleado o contratista, o una empresa en particular, está acreditada para realizar ciertas tareas y para operar en un modo de seguridad específico, usando componentes de seguridad preestablecidos.

- **ADMINISTRACIÓN DE CERTIFICADOS:**
  La administración de certificados incluye, pero no está limitada a almacenar, diseminar, publicar y revocar certificados.

- **ADMINISTRADOR DE UNA AUTORIDAD DE REGISTRO:**
  Un empleado o persona autorizada mediante acta de nombramiento o documento lo acredita como persona autorizada de una AUTORIDAD DE REGISTRO (AR) que es responsable de llevar a cabo las funciones de una AUTORIDAD DE REGISTRO (AR) en un ámbito determinado. Las autoridades de registro deberán tener por lo menos un ADMINISTRADOR DE AUTORIDAD DE REGISTRO.

- **AFIRMAR O AFIRMACIÓN:**
  Establecer que un dato es correcto o una información es verdadera.

- **ALGORITMO CRIPTOGRÁFICO:** Función matemática usada en procesos de encriptación y des encriptación, cuyo objetivo es brindar seguridad a los datos, resguardando la confidencialidad e integridad de estos; los cuales sin el uso de una llave no es posible verlos o desencriptarlos.

- **AMENAZA:**
  Circunstancia o evento que potencialmente pueda llegar a causar daños a un sistema, incluyendo la destrucción, conocimiento no autorizado o modificación de datos y / o desconocimiento del servicio.

- **ARCHIVAR:**
  Guardar registros y libros asociados, durante un determinado período de tiempo, por cuestiones de seguridad, backup o auditoría.

- **ASEGURAR:**
  Declaración o conducta que indica una intención general, de buena fe, de realizar los máximos esfuerzos para proveer y mantener un servicio específico por parte de la Autoridad de Certificación (REGISTRO DIGITAL PRISMA). Asegurar no implica necesariamente una garantía de que los servicios se realizarán plena y satisfactoriamente. Es distinto de confiabilidad, promesa, garantía, excepto que se exprese lo contrario.

- **AUDITORÍA:**
  Procedimiento utilizado para verificar que los controles se llevan a cabo y son adecuados para el cumplimiento de sus propósitos. Incluye el registro y análisis de las actividades para detectar intrusos o violaciones del sistema informático. Las irregularidades encontradas mediante una auditoría son reportadas al personal gerencial apropiado.

- **AUTENTICACIÓN:**
  Proceso utilizado para confirmar la identidad de una persona o para probar la integridad de determinada información. La autenticación de un mensaje implica determinar su origen y verificar que no haya sido modificado al transmitirse. (Confrontar con verificar (una firma electrónica avanzada)).

- **AUTORIDAD DE REGISTRO:**
  Persona individual o jurídica (pública o privada) aprobada por la Autoridad de Certificación REGISTRO DIGITAL PRISMA, y cumpliendo con lo establecido en la Ley para el Reconocimiento de las comunicaciones y firmas electrónicas Decreto 47-2008 del Congreso de la República de Guatemala para asistir a las personas en el proceso de solicitar certificados o revocar sus certificados, o ambas y también aprobar dichas solicitudes. La Autoridad de Registro no puede delegar la autoridad para aprobar solicitudes, salvo a sus ADMINISTRADORES del AMBITO DE LA AUTORIDAD DE REGISTRO.

- **AUTORIZACIÓN:**
  El otorgamiento de derechos, incluyendo la posibilidad de acceder a información o recursos específicos.

- **BASE DE DATOS:**
  Conjunto de información relacionada, creada, almacenada o manipulada por un sistema computarizado.

- **CADENA DE CERTIFICACIÓN:**
  Serie ordenada de certificados que contiene el certificado del suscriptor final y los certificados de la Autoridad de Certificación.

- **CANAL SEGURO:**
  Comunicación mejorada criptográficamente que protege mensajes frente a posibles amenazas a la seguridad.

- **CERTIFICAR:**
  El proceso de emisión de un certificado por parte de una Autoridad e misión.

- **CERTIFICADO:**
  Todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma usualmente emitido por un tercero diferente del originador y del destinatario.

- **CERTIFICADO VÁLIDO:**
  Certificado emitido por una autoridad de certificación y aceptado por el suscriptor que aparece en él.

- **CERTIFICADO VIGENTE:**
  Certificado que se encuentra dentro de su período de vigencia en este instante o en otro momento específico, dependiendo del contexto.

- **CDP:**
  Es una interfaz que representa un punto de distribución, cuya lista constituye una extensión de puntos de distribución de CRL. Estos fragmentan el conjunto completo de certificados emitidos por la autoridad en subconjuntos, de modo que cada fragmento pueda tener su propia CRL más pequeña.

- **CLAVE PRIVADA:**
  Clave matemática (mantenida en secreto por su propietario) usada para crear firmas digitales y, dependiendo del algoritmo, desencriptar mensajes o archivos encriptados (por confidencialidad) con la clave pública correspondiente.

- **CLAVE PÚBLICA:**
  Clave matemática que puede estar disponible al público y que es utilizada para verificar firmas creadas con su correspondiente clave privada. Dependiendo del algoritmo, las claves públicas se usan también para encriptar mensajes o archivos que pueden luego ser desencriptados con la correspondiente clave privada.

- **COMPROMISO:**

  Violación (o presunta violación) de un procedimiento de seguridad, por la cual pudo haber ocurrido un conocimiento o lectura no autorizada o pérdida de control sobre información importante.

- **CONFIANZA:**

  Generalmente, la suposición de que una persona o entidad va a comportarse sustancialmente como es esperado. La confianza debe aplicar solamente para una función específica.

- **CONFIANZA EN UNA FIRMA ELECTRÓNICA AVANZADA O EN UN CERTIFICADO:**

  Aceptar una firma electrónica avanzada y actuar de manera tal que sería perjudicial para quien la acepta, si la firma fuera inválida.

- **CONFIDENCIALIDAD:**

  Condición bajo la cual información relevante o identificada como "confidencial" es mantenida en secreto y solo se pone a disposición de terceros autorizados.

- **CONTRATO DEL SUSCRIPTOR:**

  El acuerdo formalizado entre el suscriptor y una Autoridad de Certificación y sus Autoridades de Registro para la provisión de determinados servicios de certificación se rige de acuerdo con estas normas para el Proceso de Certificación.

- **CONTRASEÑA (NÚMERO DE IDENTIFICACIÓN PERSONAL)**

  Información confidencial de autenticación, generalmente compuesta por una sucesión de caracteres, utilizada para proveer acceso a un recurso computacional.

- **CONTROLES:**

  Medias tomadas para asegurar la integridad y calidad de un proceso.

- **CRIPTOGRAFÍA:**

  Ciencia matemática utilizada para asegurar la confidencialidad y autenticación de información, reemplazándola por una versión transformada que puede ser recuperada para revelar su forma original, solamente por alguien que posea el algoritmo matemático y la clave apropiados.
  Disciplina que nuclea los principios, la capacidad y los métodos necesarios para transformar datos con el propósito de ocultar la información contenida en ellos, prevenir modificaciones no detectables y / o impedir utilizaciones no autorizadas de los mismos.

- **CRIPTOGRAFÍA DE CLAVE PÚBLICA O CRIPTOGRAFÍA ASIMÉTRICA:**

  Tipo de criptografía que utiliza un par de claves criptográficas matemáticamente relacionadas. La clave pública puede estar a disposición de todo el que quiera usarla y puede encriptar información o verificar una firma electrónica avanzada; la clave privada es mantenida en secreto por su propietario y puede desencriptar información o generar una firma electrónica avanzada.

- **DATOS:**

  Programas, archivos y cualquier otra información almacenada, comunicada o procesada por una computadora.

- **DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA AVANZADA:**

  Los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica avanzada.

- **DATOS DE VERIFICACIÓN DE FIRMA:**

  Los datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica avanzada.

- **DESTINATARIO:**

  Por destinatario de un mensaje de datos se entenderá la persona designada por el iniciador (originador) para recibir el mensaje, antes de ser archivado, si este es el caso, pero que no haya actuado a título de intermediario con respecto a él.

- **DISPOSITIVO DE CREACIÓN DE FIRMA:**

  Un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma.

- **DISPOSITIVO DE VERIFICACIÓN DE FIRMA:**

  Un programa informático configurado o un aparato informático configurado, que sirve para aplicar los datos de verificación de firma.

- **EMISIÓN DE CERTIFICADOS:**

  Los pasos desarrollados por una ENTIDAD DE CERTIFICACIÓN *(entidad de emisión)* (REGISTRO DIGITAL PRISMA E.R) al crear un certificado y notificar de su contenido al solicitante del certificado (posible futuro suscriptor) cuyo nombre aparece en el certificado.

- **FIRMA ELECTRÓNICA AVANZADA:**

  La firma electrónica avanzada que cumple los requisitos siguientes:

a) Estar vinculada al firmante de manera única.

b) Permitir la identificación del firmante.

c) Haber sido creado utilizando los medios que el firmante puede mantener bajo su exclusivo control.

d) Estar vinculada a los datos a que se refiere, de modo que cualquier cambio ulterior de los mismos sea detectable.

- **FIRMANTE:**
  La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

- **FRASE DE COMPROBACIÓN:**
  Conjunto de números y/o letras (caracteres alfanuméricos) que son elegidos por el solicitante de un certificado, comunicado a la Autoridad de Certificación (Emisión) junto con la solicitud y utilizado por la Autoridad de Certificación para autenticar al suscriptor para diversos propósitos exigidos por las normas para el Proceso de Certificación (CPS).

- **GENERACIÓN DE CLAVES (LLAVES)**
  Proceso confiable de creación del par de claves: clave privada y clave pública. La clave pública es entregada a una Autoridad de Certificación (emisión REGISTRO DIGITAL PRISMA) durante el proceso de solicitud del certificado.

- **GENERADOR:**
  Persona de la cual (o en cuyo nombre) se supone que un mensaje ha sido generado, almacenado o transmitido. No incluye a una persona que actúa como intermediario.

- **HASH (función hash)**
  Un algoritmo que transforma un conjunto de bits en otro conjunto (generalmente más pequeño) de manera que:
  a) Un mensaje produce igual resultado cada vez que el algoritmo es aplicado al mismo mensaje original.
  b) Es computacionalmente no factible reconstruir el mensaje original a partir del resultado producido por el algoritmo.
  c) Es computacionalmente no factible encontrar dos mensajes distintos que produzcan, utilizando el algoritmo, idéntico resultado hash.

- **HSM**

  Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas; aporta funcionalidad criptográfica de PKI de alto rendimiento que se efectúa dentro del propio hardware.

- **INCORPORACIÓN POR REFERENCIA:**

  Convertir un mensaje en parte de otro mensaje, identificando al mensaje a ser incorporado con información que le permite al destinatario acceder y obtener el mensaje incorporado en forma completa, haciéndose expresa mención que éste es parte integrante del mensaje original. Tal mensaje incorporado tiene el mismo efecto que si hubiese formado parte del mensaje original, con el sentido que la ley le otorga.

- **INFORMACIÓN DEL FIRMANTE:**

  Información provista a la autoridad certificante como parte de la solicitud de un certificado.

- **INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)**

  Arquitectura, organización, técnicas, políticas y procedimientos en los que se basa la implementación y operación del sistema criptográfico de certificados de clave pública. La PKI consiste en sistemas que permiten proveer e implementar los Servicios de Certificación y otros servicios relacionados.

- **LISTA DE CERTIFICADOS REVOCADOS (CRL):**

  Lista emitida periódicamente, firmada digitalmente por una Autoridad de Certificación (AC) en la que figuran los certificados que han sido revocados con anterioridad a su fecha de vencimiento. La lista generalmente incluye el nombre del emisor de la Lista de Certificados Revocados (CRL), la fecha de emisión, la fecha de emisión programada de la próxima Lista de Certificados Revocados (CRL), los números de serie de los certificados revocados y la fecha exacta y los motivos de la revocación.

- **LOCALIZADOR UNIFORME DE RECURSOS (URL):**

  Dispositivo estandarizado para identificar y localizar ciertos registros y otros recursos existentes en la World Wide Web.

- **MENSAJE O MENSAJE DE DATOS:**

  Se entiende por mensaje de datos toda la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudiera ser entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama el télex o el telefax.

- **MODULO CRIPTOGRÁFICO**
  Implementación confiable de un sistema criptográfico que realiza la encripción y desencripción de datos de manera segura.

- **NOMBRE**
  Conjunto de atributos que identifican a una entidad (persona individual o jurídica).

- **NOMBRE DEL TITULAR**
  Valor unívoco en el campo de nombre del titular del certificado que está ligado a su clave pública.

- **NOMBRE DISTINGUIDO**
  Conjunto de datos que identifican a una entidad real, como por ejemplo una persona, en un contexto computacional.

- **NOMBRE DISTINGUIDO RELATIVO (RDN)**
  Conjunto de atributos que comprende el nombre distintivo de la entidad, que distingue a esa entidad de otras del mismo tipo.

- **NOMINACIÓN EXTENDIDA**
  Uso de campos de extensión opcionales en un certificado X.509 versión 3.

- **NORMAS PARA EL PROCESO DE CERTIFICACIÓN (CPS)**
  Este documento, tal como es actualizado periódicamente.

- **NOTARIO**
  Profesional del Derecho, graduado en Licenciado en Ciencias Jurídicas y Sociales, inscrito y activo por el Colegio de Abogados y Notarios de Guatemala, quien tiene fe pública para hacer constar y autorizar actos y contratos en que intervengan por disposición de la ley o a requerimiento de parte.

- **NOTIFICACIÓN**
  El resultado de una notificación de acuerdo con estas normas para el Proceso de Certificación (CPS).

- **NOTIFICAR**
  Comunicar información específica a otra persona de acuerdo con estas normas para el proceso de Certificación (CPS) y las leyes pertinentes.

- **NÚMERO DE SERIE DE LOS CERTIFICADOS**
  Cifra que identifica unívocamente a cada certificado generado por una Autoridad de Certificación (emisión) REGISTRO DIGITAL PRISMA.

- **ON-LINE**
  Comunicación que provee una conexión en tiempo real con los Servicios de Certificación de REGISTRO DIGITAL PRISMA.

- **ORGANIZACIÓN**
  Entidad a la cual un usuario está vinculado. Una organización también puede ser un usuario.

- **ORIGINADOR O INICIADOR:**
  Se entiende por iniciador de un mensaje de datos aquella persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario respecto a él;

- **PAR DE CLAVES**
  Una clave privada y su correspondiente clave pública. La clave pública puede verificar una firma electrónica avanzada que fue creada utilizando la clave privada correspondiente. Además, dependiendo del tipo de algoritmo implementado, los componentes del par de claves también pueden encriptar y desencriptar información para que sea confidencial, en cuyo caso la clave privada puede revelar unívocamente la información encriptada, mediante el uso de la clave pública correspondiente.

- **PARTE QUE CONFÍA**
  Persona que trabaja en una posición de confianza y está calificada para ello de acuerdo con estas normas para el Proceso de Certificación (CPS). (*Confrontar con* **confianza).**

- **PARTES**
  Personas y/o Entidades cuyos derechos y obligaciones son establecidos por estas normas para el Proceso de Certificación (CPS). Estas entidades pueden ser solicitantes de certificado, Autoridad de Certificación REGISTRO DIGITAL PRISMA, suscriptores y receptores confiados.

- **PC card** (*Ver* **smart card**)
  Instrumento de hardware que cumple con los estándares promulgados por la Personal Computer Memory Card International Association (PCMCIA), que provee capacidad de expansión a las computadoras, incluyendo la posibilidad de contener información de seguridad.

- **PERÍODO DE VIGENCIA**
  Período que comienza en la fecha y hora de emisión del certificado (o en una fecha y hora futura si así estuviera estipulado en el certificado) y finaliza con la fecha y hora en la que el certificado vence o es revocado previamente a su vencimiento.

- **PERSONA**
  Persona individual o Jurídica, capaz de firmar o verificar un mensaje, ya sea legalmente o de hecho.

- **PRESENCIA**
  Acto de aparecer o comparecer (físicamente, no virtual ni figurativamente) frente a una Autoridad de Registro (E.R) o ante una persona designada (Administrador) por ella y probar la propia identidad, como pre-requisito para la emisión de un certificado bajo ciertas circunstancias.

- **PSC**
  Término general que se refiere a todas las entidades que emiten certificados y pueden prestar otros servicios relacionados con las firmas electrónicas avanzadas comprendidos en la ley guatemalteca

- **PUBLICAR / PUBLICACIÓN**
  Registrar o archivar información en el repositorio de REGISTRO DIGITAL PRISMA y opcionalmente en uno o más repositorios distintos para dar a conocer y hacer pública dicha información en forma consistente con estas normas para el Proceso de Certificación (CPS) y la ley pertinente.

- **RAÍZ**
  La Autoridad de Certificación Emisión (IA) que emite el primer certificado en una cadena de certificados. La clave pública de la raíz debe ser conocida previamente por el usuario del certificado para poder validar la cadena de certificación. La clave pública de la raíz se hace confiable mediante un mecanismo distinto al de un certificado, como por ejemplo una distribución física segura.

- **RAÍZ CONFIABLE**
  Una raíz confiable es una clave pública que ha sido confirmada como vinculada a una Autoridad de Certificación (IA) por un usuario o administrador de sistema. El software y los sistemas que implementan la autenticación basada en criptografía asimétrica y los certificados asumen que esta clave se obtuvo correctamente. Se confirma accediendo siempre a ella a través del repositorio de un sistema confiable, el cual sólo puede tener autorizaciones de modificación de parte de administradores identificados y confiables.

- **REGISTRO**
  Información que se encuentra en un medio tangible (documento) o almacenado en forma electrónica o cualquier otro medio en el cual la información se puede recuperar. El término "registro" incluye los términos "documento" y "mensaje". (*Confrontar con* **documento; mensaje**)

- **RENOVACIÓN**
  Proceso de obtención de un nuevo certificado de la misma clase y tipo para el mismo sujeto, luego de la expiración de un certificado preexistente.

- **REPOSITORIO**
  Base de datos de certificados y otra información relevante accesible on-line.

- **REVOCAR UN CERTIFICADO**
  Proceso de finalización del período de vigencia de un certificado a partir de una fecha determinada.

- **RSA**
  Sistema criptográfico de clave pública inventado por Rivest, Shamir y Adleman.

- **SEGURIDAD**
  Calidad o estado de protección de los accesos no autorizados o pérdidas o efectos no controlados. La seguridad absoluta es imposible de alcanzar en la práctica y la calidad de un determinado sistema de seguridad es relativa. Dentro de un modelo de seguridad establecido, seguridad es un estado específico que debe ser preservado bajo varias operaciones.

- **SERVICIOS DE INTEGRIDAD DEL CONTENIDO**
  Los servicios de integridad del contenido proveen certificados a editores de software que desean firmar digitalmente sus publicaciones de software para facilitar a sus clientes (usuarios finales) la posibilidad de validar el software.

- **SERVICIOS DE SEGURIDAD**
  Servicios desarrollados dentro de un marco de seguridad, realizados mediante ciertos mecanismos de seguridad. Dichos servicios incluyen, pero no se limitan a control de acceso, confidencialidad e integridad de datos.

- **SERVIDOR**
  Sistema computacional que responde a los requerimientos de los sistemas de los clientes.

- **SISTEMA CONFIABLE**
  Hardware, software y procedimientos que son razonablemente seguros en contra de su violación de intrusos o mal uso, que proveen un nivel razonable de disponibilidad, confiabilidad y operación correcta. Están razonablemente diseñados para realizar las funciones pretendidas y para imponer

la política de seguridad pertinente. Un sistema confiable no es necesariamente un "sistema en el cual se confía totalmente" tal como está definido en la nomenclatura clasificada del gobierno de los Estados Unidos de Norteamérica.

- **SUCESIÓN DE CARACTERES REGISTRADA**
  Clase de objeto sujeto a procedimientos de registro y grabado que demuestran que el valor es unívoco dentro de los registros de la Autoridad de Registro. El tipo de valor registrado es una sucesión de caracteres.

- **SUSCRIPCIÓN**
  Proceso que realiza un solicitante, para pedir un certificado.

- **SUSCRIPTOR**
  Persona a la que se le ha emitido un certificado del cual es titular y es capaz y está autorizada a utilizar la clave privada que corresponde a la clave pública que figura en su certificado.

- **TIPO (DE CERTIFICADO)**
  Propiedades definidas de un certificado que limitan su propósito a una clase de aplicaciones asociadas exclusivamente a ese tipo.

- **TITULAR (DE UN CERTIFICADO)**
  Propietario de la clave privada que corresponde a una clave pública. El término titular puede referirse tanto al equipo o dispositivo que tiene la clave privada como al individuo, si existe, que controla tal equipo o dispositivo. A cada titular se le asigna un nombre distintivo que está ligado a la clave pública contenida en el certificado del titular.

- **TOKEN**
  Pieza de hardware de seguridad que contiene la(s) clave(s) privada(s) de un titular de certificado de clave pública, incluyendo todos los certificados en la cadena de certificación del usuario.

- **USUARIO**
  Entidad autorizada a utilizar un certificado como solicitante, suscriptor, destinatario o parte confiada. Excluye a la Autoridad de Certificación (IA) que emitió dicho certificado. (*Confrontar con* **solicitante del certificado; entidad; persona; suscriptor**)

- **VALIDAR UN CERTIFICADO (***ej.,* de un **certificado de suscriptor final)**
  Proceso realizado por un destinatario o receptor confiado para confirmar que el certificado de un suscriptor final es válido y estaba vigente en el momento en que la firma electrónica avanzada fue creada.

- **VENCIMIENTO DEL CERTIFICADO**
  Fecha y hora especificada en el certificado en la cual expira el período de vigencia del mismo, sin perjuicio de cualquier revocación previa.

- **VERIFICACIÓN** (DE UNA SOLICITUD DE CERTIFICADO)
  Proceso realizado por la Autoridad de Registro o en su caso por la Autoridad de Certificación REGISTRO DIGITAL PRISMA luego de la entrega de una solicitud de certificado, como pre-requisito para la aprobación de dicha solicitud y la emisión de un certificado

- **VERIFICAR** (UNA FIRMA ELECTRÓNICA AVANZADA)
  Con respecto a una firma electrónica avanzada dada, mensaje y clave pública, determinar positivamente que (i) la firma electrónica avanzada fue creada durante el período de vigencia de un certificado válido utilizando la clave privada que corresponde a la clave pública contenida en el certificado y (ii) el mensaje asociado a dicha firma no ha sido alterado desde que la firma electrónica avanzada fue creada.

- **VERIFICAR UNA CADENA DE CERTIFICACIÓN**
  Es el proceso realizado por un destinatario o receptor confiado para autenticar la clave pública de cada certificado de una cadena de certificados, confirmando que cada uno de ellos es válido, fue emitido durante el período de vigencia del certificado de la Autoridad de Certificación (CA) correspondiente y todas las partes (Autoridades de Certificación (CA), suscriptores finales, destinatarios y partes confiadas) han actuado de acuerdo a estas normas para el Proceso de Certificación (CPS) con respecto a todos los certificados de la cadena.

- **VINCULANTE**
  Afirmación de una Autoridad de Certificación (CA) (o su Autoridad de Registro Local (LRA)), de la relación existente entre un ente nominado y su clave pública.

- **World Wide Web (WWW)**
  Sistema distribuido de información basado en hipertexto, mediante el cual los usuarios pueden crear, editar o navegar por documentos de hipertexto. Medio de publicación y recuperación de documentos gráficos. Una colección de documentos relacionados que residen en la Red.

- **X.509 versión 3**
  El formato estándar de la ITU-T (International Telecommunications Union-T) para certificados. X.509 versión 3, referida a los certificados que contienen o pueden contener extensiones.