Registro Digital Prisma

POLÍTICA DE CERTIFICACIÓN - CP -

Código:	AD-DO-01
Versión:	5
Fecha de la versión:	20-02-2019
Nivel de confidencialidad:	0

Política de Certificación de REGISTRO DIGITAL PRISMA

Impreso en la ciudad de Guatemala
Fecha de revisión: febrero 2019

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

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

Aviso de Propiedad Intelectual.

Políticas de Certificación de REGISTRO DIGITAL PRISMA SOCIEDAD ANÓNIMA

REGISTRO DIGITAL PRISMA se reserva todos los derechos de propiedad intelectual incluyendo el derecho de autor del presente documento.

REGISTRO DIGITAL PRISMA, SOCIEDAD ANÓNIMA se reserva el derecho de autor y los demás derechos de Propiedad Intelectual de las presentes políticas, incluyendo pero no limitando el texto, las marcas registradas o no así como nombres de dominio que figuran en el presente documento. La persona que accede a este documento tiene una autorización limitada de uso y reproducción de las mismas, ya que cualquier reproducción impresa deberá ser mediante la autorización expresa por parte de REGISTRO DIGITAL PRISMA S.A., así como deberá ser en forma íntegra y total e incluir a REGISTRO DIGITAL PRISMA como autor de las mismas. La reproducción, sin autorización expresa por parte de REGISTRO DIGITAL PRISMA ya sea total o parcial de este documento, su texto, sus elementos gráficos o marcas, nombres comerciales, nombres de dominio y demás signos distintivos, por cualquier persona o usuario constituye una violación al derecho de autor y los demás derechos de propiedad intelectual de REGISTRO DIGITAL PRISMA.

Las solicitudes para reproducir estas Políticas de Certificación de REGISTRO DIGITAL PRISMA, deben ser dirigidas a REGISTRO DIGITAL PRISMA SOCIEDAD ANÓNIMA, mediante el siguiente correo: suscriptor@prisma.gt.

Tabla de contenido

1. Introducción

La infraestructura de llave pública, conocida también por sus siglas en inglés PKI (Public Key Infraestructure) de REGISTRO DIGITAL PRISMA, en adelante PKI de REGISTRO DIGITAL PRISMA o PKI; 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 sus Promotores de Venta autorizados, 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 Promotores de Ventas autorizados por REGISTRO DIGITAL PRISMA, está publicada en el sitio web www.prisma.gt.

Este documento, establece las políticas que rigen la PKI de REGISTRO DIGITAL PRISMA. Las políticas de Certificación (CP) establecen los requerimientos de negocios, legales y técnicos para aprobar, emitir, administrar, utilizar, revocar y renovar los certificado dentro de la PKI de REGISTRO DIGITAL PRISMA y proporcionar servicios de confiabilidad asociados para todos sus participantes. 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. Cualquier cambio y/o modificación a este documento, será notificado al Registro de Prestadores de Servicios de Certificación (RPSC) del Ministerio de Economía, tal como se establece en la presente CP.

La CP no es 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, actuando como AC, calidad con que operará también en los términos de sus propias Declaraciones de Prácticas de Certificación (CPS *por su siglas en inglés*) mismas que cumplen con los requerimientos establecidos por estas CP.
- REGISTRO DIGITAL PRISMA, actuando como AR, en su función de validación de los datos y la información de los Suscriptores de certificados.
- Los Suscriptores de certificados de la PKI de REGISTRO DIGITAL PRISMA que deberán entender de qué manera están autenticados sus datos y documentos acreditativos y cuáles son sus

obligaciones al respecto y como se protegen conforme la PKI de REGISTRO DIGITAL PRISMA.

- PARTE QUE CONFÍA son las personas quienes deberán estar conscientes sobre qué tanta Confianza pueden tener en un Certificado emitido con base a la PKI DE REGISTRO DIGITAL PRISMA, o en una firma electrónica avanzada utilizando ese Certificado.

1.1. Ámbito de aplicación

Las presentes Políticas de Certificación son la base que establece los lineamientos bajos las cuales deben operar los participantes de la PKI de REGISTRO DIGITAL PRISMA.

Una Autoridad de Registro (AR), es una entidad que lleva a cabo el trámite de las solicitudes de certificados conforme a la PKI de REGISTRO DIGITAL PRISMA. Por su parte, REGISTRO DIGITAL PRISMA, actúa como AR para los certificados que expide.

Los certificados podrán ser utilizados por los suscriptores para asegurar documentos firmados electrónicamente, correos electrónicos, 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 el destinatario. A la persona que finalmente recibe un documento firmado o comunicación o accede un sitio web o de Internet seguro se le denomina como la PARTE QUE CONFÍA, por ejemplo, esa persona está confiando en el certificado y debe decidir si puede o no confiar en el mismo, en caso que decide aceptar la confianza en el certificado aceptará los términos y condiciones del contrato de "PARTE QUE CONFÍA".

Esta CP describe a detalle la identificación y autenticación llevada a cabo para cada Clase de Certificado.

1.2. Nombres del documento e identificación

Este documento es LA POLÍTICA DE CERTIFICACIÓN DE REGISTRO DIGITAL PRISMA, dentro de la PKI de REGISTRO DIGITAL PRISMA, y podrá denominársele simplemente como CP. REGISTRO DIGITAL PRISMA, es la autoridad de certificación que define la política. Los valores del identificador utilizados para las clases de certificados de suscriptor usuario final son los siguientes:

Política de Certificado: 2.16.438.101.10.316.2.1.1.1.1.1.2

1.3. Participantes de la PKI

1.3.1. Prestadores de Servicios de Certificación

El término Prestadores de Servicios de Certificación (PSC) es un término general que se refiere a todas las entidades que participan directa o indirectamente en la tramitación y emisión de Certificados dentro de la PKI de REGISTRO DIGITAL PRISMA, y se encuentran debidamente autorizados por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía de la República de Guatemala (RPSC).

REGISTRO DIGITAL PRISMA lleva a cabo el proceso de verificación, validación y aprobación de los certificados que se emiten por la propia REGISTRO DIGITAL PRISMA y a su vez, ejercerá todas las funciones que van dirigidas al público o a los usuarios de forma y de fondo.

1.3.2. Autoridad de Registro

Dentro de la Infraestructura de llave pública PKI de REGISTRO DIGITAL PRISMA, y desde el punto de vista técnico, REGISTRO DIGITAL PRISMA, tiene las funciones de AR, y ello implica estrictamente, que ejerce la función de validación y/o autenticación de datos de los certificados. Por lo anterior, REGISTRO DIGITAL PRISMA lleva a cabo las funciones formales dirigidas al público o a los usuarios en general consistentes entre otras: la confirmación de la identidad de los solicitantes –misma que puede hacerse por sí o por medio de Notario. La aprobación o rechazo de solicitudes de certificados y solicitudes de revocación de certificados, previo a la emisión de un certificado; actuando en calidad de AC.

Sin embargo, lo anterior no significa que REGISTRO DIGITAL PRISMA, adquiera la calidad de autoridad pública, ni por ello adquiere las funciones ni atribuciones que competen al RPSC de conformidad con la ley y demás legislación aplicable.

1.3.3. Suscriptores

Los suscriptores bajo la PKI de REGISTRO DIGITAL PRISMA, incluyen a todos los usuarios finales de certificados expedidos por REGISTRO DIGITAL PRISMA, como Prestador de Servicios de Certificación de la PKI. Un suscriptor es una persona individual o jurídica nombrada como suscriptor usuario final de un certificado.

1.3.4. Parte que confía

Una PARTE QUE CONFÍA es una persona individual o jurídica, que actúa con la confianza en un certificado de firma electrónica avanzada, expedida conforme a la PKI de REGISTRO DIGITAL PRISMA. Así mismo PARTE QUE CONFÍA es la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

1.4. Uso de Certificado

1.4.1. Usos apropiados del Certificado

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

Los certificados extendidos a personas individuales se utilizan normalmente por las personas naturales o individuales para firmar –utilizando firma electrónica avanzada-; y encriptar los correos electrónicos, así como 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 no esté prohibido por la Ley, por esta CP, por cualquier CPS conforme a la cual el certificado haya sido expedido y de conformidad con cualquier acuerdo con los suscriptores.

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, por ejemplo: la titularidad de un dominio de internet o correo electrónico. No es la intención de esta CP limitar los tipos de usos de los certificados de personas individuales o jurídicas. La PARTE QUE CONFÍA puede razonablemente confiar en que los certificados emitidos, siempre y cuando su uso no es prohibido según la Ley, por esta CP, las CPS bajo la cual el certificado haya sido expedido y conforme al contrato de suscriptor.

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 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.

1.5. Administración de política

1.5.1. Organización que administra el documento

REGISTRO DIGITAL PRISMA, SOCIEDAD ANÓNIMA Dirección: Avenida Reforma 3-48 zona 9, Edificio Anel, quinto nivel, Oficina 503; ciudad de Guatemala, Guatemala.

1.5.2. Persona de contacto

Atención: Desarrollo de Prácticas – CPS dirección: servicioalcliente@prisma.gt

1.5.3. Persona que determina la adecuación de la CP a la política

El Gerente General de REGISTRO DIGITAL PRISMA determina la adecuación y la aplicabilidad de esta CP.

1.5.4. Procedimiento de aprobación de CP

La aprobación de esta CP, 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 CP. Las modificaciones se harán, ya sea en el formato de un documento que contenga la versión modificada de la CP, o mediante un aviso de actualización. Las versiones modificadas o las actualizaciones serán asociadas a la sección de Actualizaciones de Prácticas y Avisos del Repositorio de REGISTRO DIGITAL PRISMA ubicado en www.prisma.gt. Las actualizaciones reemplazan cualquier disposición designada o en conflicto de la versión referenciada de la CP.

1.6. Acrónimos y glosario

Véase la sección 9 y 10 de la Declaración de Prácticas de Certificación CPS.

2. Publicación y responsabilidades de la base de datos / repositorio

2.1. Repositorios

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.

2.2. Publicación de información de Certificado

REGISTRO DIGITAL PRISMA mantiene una base de datos en línea o REPOSITORIO que permite a la PARTE QUE CONFÍA hacer solicitudes en línea con relación a revocaciones y a otra información del estatus de los certificados.

REGISTRO DIGITAL PRISMA proporciona a la PARTE QUE CONFÍA toda la información necesaria para encontrar revocaciones y otra información relacionada con los certificados. Además REGISTRO DIGITAL PRISMA ofrece el servicio de OCSP (siglas en inglés que corresponden al Protocolo en línea del estatus del Certificado) con el cual se puede validar en línea la vigencia de un certificado, en la dirección: www.prisma.gt

REGISTRO DIGITAL PRISMA publicará en su repositorio y en todo momento una versión actual de:

- Esta CP
- Las CPS
- Contrato del Suscriptor

2.3. Tiempo o frecuencia de publicación

La información de la AC se publica inmediatamente después de que se pone a disposición la información de la AR. REGISTRO DIGITAL PRISMA ofrece una lista de certificados revocados –CRL- por sus siglas en inglés **(CERTIFICATE REVOCATION LIST)**, que muestran la revocación de los certificados de REGISTRO DIGITAL PRISMA y ofrecen los servicios de revisión del estatus de los certificados, a través de los repositorios de REGISTRO DIGITAL PRISMA. Si un certificado que se encuentra en la lista en una CRL se encuentra vencido, podrá ser retirado de la CRL después de su vencimiento.

3. Identificación y autenticación

3.1. Nombres

A menos que se indique lo contrario en esta CP, las CPS, los contratos o cualquier otro documento relacionado con el contenido del certificado; los nombres que aparecen en los certificados expedidos de conformidad con la PKI de REGISTRO DIGITAL PRISMA, pasaron por un proceso de revisión y autenticación.

3.1.1. Tipo de nombres

Los certificados de Suscriptor, contienen un nombre distinguido en el campo del nombre del asunto.

El nombre distinguido del sujeto de los certificados del suscriptor de usuario final incluye un nombre común (NC=). El valor de nombre común incluido en los nombres distinguidos de sujeto de certificados de personas jurídicas, será un nombre de dominio, una dirección de correo electrónico de la persona jurídica, el nombre legal de la entidad o el nombre del representante de la entidad u organización autorizado para utilizar la clave privada de ésta. El componente (o =) será la razón social o denominación de entidad, el valor de nombre común incluido en el nombre distinguido del sujeto de los certificados individualizados representará el nombre personal generalmente aceptado. Los nombres comunes fueron autenticados en forma previa.

El valor de nombre común incluido en los nombres distinguidos de SUJETO DE CERTIFICADO de PERSONA INDIVIDUAL, será un nombre de dominio, una dirección de la persona individual quien estará autorizada para utilizar la clave privada. El componente (o=) será el nombre de la persona individual, el valor del nombre común incluido en el nombre distinguido.

3.1.2. Necesidad de nombres con significado

Los certificados del suscriptor, contendrán nombres con significados comúnmente conocidos que permitan identificación de la identidad de la persona individual o jurídica que sea el sujeto del certificado. En todo caso, para establecer y asignar dicho significado, deberá de estarse a lo consignado en la documentación fehaciente que se solicite al Suscriptor, respectivamente para cada tipo de certificado, como pueda ser el Documento Personal de Identificación, Patentes de Comercio o de Empresa extendidos por el Registro Mercantil o lo que sea pertinente y corresponda.

3.1.3. Exclusividad de nombre

Los nombres de los suscriptores dentro de la PKI DE REGISTRO DIGITAL PRISMA, serán únicos. Un suscriptor podrá tener uno o más certificados con el mismo nombre distinguido del asunto.

3.1.4. Reconocimiento, autenticación y papel de las marcas

Los solicitantes de certificado no usarán nombres en sus solicitudes de certificado que infrinjan los derechos de propiedad intelectual de otros. REGISTRO DIGITAL PRISMA no tendrá a su cargo la calificación, sobre si un solicitante de certificado tiene derechos o no de propiedad intelectual en el nombre que aparece en una solicitud de emisión de certificado. Así mismo, REGISTRO DIGITAL PRISMA no es y por ende no podrá fungir como juez, o árbitro o panel resolviendo conflictos en materia de nombres de dominio en Internet, conflictos de derecho de propiedad industrial, nombre comercial, marca o marca de servicio o cualquier signo distintivo. Por su parte, REGISTRO DIGITAL PRISMA se reserva el derecho de rechazar cualquier solicitud de certificado debido a asuntos de propiedad intelectual que le sean legalmente notificados y no será responsable por dicho rechazo.

3.2. Validación de identidad Inicial

3.2.1. Método para solicitar un certificado para firma electrónica avanzada

REGISTRO DIGITAL PRMA recibe las solicitudes de certificados para firma electrónica avanzada, por medio del sitio web www.prisma.gt, utilizando el estándar de envió de mensajes PKCS #11.

3.2.2. Autenticación de la identidad de Persona Jurídica

Previo a la emisión de un certificado de persona jurídica, REGISTRO DIGITAL PRISMA deberá verificar los datos proporcionados por la persona jurídica solicitante, mediante los procedimientos previamente dispuestos en las prácticas de registro para persona jurídica y como mínimo deberá:

- Determinar que la persona jurídica se encuentra legalmente constituida e inscrita en el Registro Mercantil General de la República de Guatemala, Registro de Personas Jurídicas del Ministerio de Gobernación y otra entidad gubernamental mediante la cual se pueda comprobar dicho extremo, en caso sea una entidad constituida al amparo de las leyes de la República de Guatemala.

- Determinar, en caso la solicitud para emisión de certificado provenga de una persona jurídica que se encuentra legalmente constituida al amparo de leyes que no sean de la República de Guatemala; que dicha entidad se encuentra inscrita en el Archivo General de Protocolos del Organismo Judicial, Registro Mercantil General de la República de Guatemala, Registro de Personas Jurídicas del Ministerio de Gobernación y/o cualquier otra entidad gubernamental, en la que deba de inscribirse o acreditarse de conformidad con la ley; así como que cuente con las correspondientes credenciales consulares o diplomáticas en caso aplicare; y en todo caso, determinando el cumplimiento de los pases de ley exigidos por las leyes de la República de Guatemala.

- Confirmar por teléfono, verificación o procedimiento similar que esté disponible, si la información de la entidad es correcta y que la persona que presenta la solicitud de Certificado en representación del solicitante de certificación está autorizada para hacerlo.

  Cuando un certificado incluya el nombre de una persona como un representante autorizado de la entidad, también se confirmará que esa persona desempeña el puesto en esa entidad y su calidad para actuar en representación de la misma.

- En el caso de que un nombre de dominio o una dirección de correo electrónico se incluyan en certificado, REGISTRO DIGITAL PRISMA podrá verificar el derecho de la persona jurídica para utilizar ese nombre de dominio ya sea como un nombre de dominio totalmente calificado o un dominio de correo electrónico.

3.2.3. Autenticación de Identidad Individual

Los procedimientos de autenticación para la identidad de persona individual varían conforme a la clase de certificado. El estándar mínimo de autenticación para el certificado de persona individual de la PKI de REGISTRO DIGITAL PRISMA es que se confirme la identidad del individuo mediante un documento legalmente expedido ya sea en Guatemala o en el extranjero.

La autenticación de certificados de personas individuales está basada, en la presencia personal (física) del solicitante del certificado, ante la propia REGISTRO DIGITAL PRISMA o ante notario. REGISTRO DIGITAL PRISMA revisará la identidad del solicitante de Certificado tomando como referencia la información contenida en las Prácticas de Registro para persona Individual.

REGISTRO DIGITAL PRISMA, podrá también tener la oportunidad de aprobar las solicitudes de Certificado para sus propios administradores. Los administradores son "Personas de Confianza". En este caso, la autenticación de sus solicitudes de certificado se basará en la confirmación de su identidad, con base a los requisitos para emisión de certificados de persona individual en relación de dependencia y los procedimientos de revisión de antecedentes.

3.2.4. Validación de Autoridad

En el caso de que el nombre de una persona esté asociado con el nombre de una entidad en un certificado de tal manera que indique la relación de la persona o la autorización para actuar en representación de la Persona Jurídica, REGISTRO DIGITAL PRISMA:

i. Determina que la persona jurídica mediante la confirmación de su existencia y si legamente se encuentra constituida de conformidad con las leyes de Guatemala, a través del Registro Mercantil General de la República y/u otra oficina gubernamental que pueda comprobar dicho extremo.
ii. Determina la inscripción y vigencia de la representación en los registros públicos que fueren pertinentes, en caso requiera de dichas inscripciones; o en su caso, confirma por medio del directorio de personal, por teléfono, o por cualquier medio, que la persona que presenta la solicitud de certificado trabaja en la entidad y que actúa en calidad de representante de la organización.

3.3. Identificación y autenticación de solicitud de Revocación

Los procedimientos de revocación aseguran que previo a la revocación de cualquier certificado, la misma fue solicitada por el suscriptor del certificado o la entidad que aprueba la solicitud de certificado.

Los procedimientos aceptables de autenticación para las solicitudes de revocación de un Suscriptor incluyen:

i. Que el suscriptor presente para el certificado, la clave de anulación y revoque el certificado automáticamente si coinciden los datos con los que se tiene en los registros.
ii. Recibir un mensaje del suscriptor a la cuenta de correo suscriptor@prisma.gt que solicite la revocación y que contenga una firma electrónica avanzada verificable con referencia al certificado que se revocará.

iii. Comunicación con el suscriptor que proporcione seguridad razonable en base a la clase de certificado que la persona individual o persona jurídica que ha solicitado la revocación es de hecho el suscriptor. Dicha comunicación dependiendo de las circunstancias podrá incluir uno o más de lo siguiente: teléfono, fax, correo electrónico, dirección de correos o servicios de mensajería.

4. Certificados de Requerimientos Operacionales de ciclo de vida del Certificado

4.1. Solicitud de Certificado

4.1.1. Validación de Autoridad

A continuación se encuentra una lista de las personas que podrán presentar solicitudes de certificado:

- Cualquier persona individual o natural que sea el sujeto de Certificado.
- Cualquier representante legal, debidamente autorizado de una Persona Jurídica.

4.1.2. Proceso de Registro y Responsabilidades

i. **SUSCRIPTORES DE CERTIFICADO DE USUARIO FINAL**

Todos los suscriptores de certificados de usuario final manifestarán su consentimiento mediante la aceptación del contrato de suscriptor relacionado que contiene los derechos y obligaciones y que pasarán un proceso de registro consistente en:

- Completar una solicitud de certificado y proporcionar información veraz y correcta.
- Presentar todos los documentos que le sean requeridos en las prácticas de registro correspondientes;
- Generar un par de claves.
- Entregar su clave pública, directamente o a través de un AR.
- Demostrar la posesión de la clave privada.

4.2. Proceso de solicitud del certificado

4.2.1. Llevando a cabo la identificación y las funciones de autenticación

REGISTRO DIGITAL PRISMA, actuando como AR, llevará a cabo la identificación y autenticación de toda la información requerida del suscriptor de conformidad con la sección 3.2.

4.2.2. Aprobación o rechazo de solicitudes de Certificado

REGISTRO DIGITAL PRISMA, como AR aprobará una solicitud de un certificado si se cumple con los siguientes requisitos:

- Identificación, verificación y autenticación exitosa de toda la información requerida del suscriptor.
- Mediante la presentación de un comprobante que acredite que el pago ha sido realizado.

REGISTRO DIGITAL PRISMA, como AR rechazará una solicitud de certificado si:

- No puede ser completada la identificación, verificación o comprobación y autenticación de toda la información requerida del Suscriptor es de conformidad con la sección 3.2.
- El suscriptor incumple en la presentación de la documentación de respaldo cuando se le solicite.
- El Suscriptor incumple a las notificaciones dentro de un tiempo específico.
- No se recibió el comprobante de pago correspondiente.

4.2.3. Tiempo para procesar las solicitudes del certificado

REGISTRO DIGITAL PRISMA comienza procesando las solicitudes de certificado dentro de un tiempo razonable a partir de la recepción. No hay una estipulación de tiempo para completar el trámite de una solicitud a menos que se indique lo contrario en el contrato del suscriptor relacionado. Una solicitud de certificado permanece activa hasta que la misma sea denegada o rechazada.

4.3. Expedición de certificado

4.3.1. Acciones de REGISTRO DIGITAL PRISMA, como AC, para la Expedición del certificado

REGISTRO DIGITAL PRISMA, actuando como Autoridad de certificación –AC-; crea y expide el certificado, luego de haber aprobado la solicitud para emisión del mismo.

4.3.2. Notificación de la Expedición del Certificado al Suscriptor por parte de REGISTRO DIGITAL PRISMA

REGISTRO DIGITAL PRISMA expide los certificados a los suscriptores directamente, notificando a los suscriptores que sus certificados están disponibles. Los certificados estarán a disposición de los suscriptores usuarios finales notificando por medio de un mensaje privado en el que le indica las instrucciones de obtención del certificado.

4.4. Aceptación de certificado

4.4.1. Acciones que constituyen la aceptación de un Certificado

Las siguientes acciones realizadas por un suscriptor, indican la ACEPTACIÓN de un CERTIFICADO.

- Aceptar el contrato de solicitante suscriptor y descargar el certificado de la página www.prisma.gt, constituye la aceptación del suscriptor del certificado.
- La utilización del certificado.
- Recibir el dispositivo criptográfico que contiene un certificado.

Los derechos y obligaciones derivados de la aceptación del certificado, están expresados en el contrato de solicitante suscriptor.

4.4.2. Publicación de un Certificado por parte de la AC

REGISTRO DIGITAL PRISMA publica los Certificados que expide en un repositorio públicamente accesible.

4.5. Par de claves y uso de Certificado

4.5.1. Clave privada del suscriptor y uso de Certificado

El uso de las claves tanto privada como pública en el certificado solamente será permitido una vez que el suscriptor haya firmado el contrato correspondiente y aceptado el certificado. El certificado será utilizado legalmente de conformidad con el contrato de suscriptor en los términos de esta CP y la CPS relacionada. El uso del certificado debe ser consistente con las extensiones de campo de uso de clave incluidas en el certificado.

Los suscriptores tienen a su cargo la guarda y custodia de sus propias claves privadas y las protegerán del uso no autorizado y descontinuarán el uso de la clave privada después del vencimiento o revocación del certificado.

4.5.2. Clave pública de la parte que confía y uso del Certificado

La PARTE QUE CONFÍA aceptará los términos y condiciones que se establezcan en el contrato de PARTE QUE CONFÍA aplicable, dicha aceptación es la condición para confiar en el certificado. La confianza en un certificado debe ser razonable de acuerdo con las circunstancias específicas. Si las circunstancias indican

una necesidad de aseguramientos adicionales, la PARTE QUE CONFÍA debe obtener dichos aseguramientos para que dicha confianza se considere razonable.

Antes de cualquier acto de confianza las PARTES QUE CONFÍAN independientemente evaluarán:

- Determinar que el certificado, de hecho, será utilizado para un propósito adecuado que no esté prohibido o contravenga éstas CP, las CPS, el contrato de suscriptor o la ley. Por su parte, REGISTRO DIGITAL PRISMA no es responsable por el uso adecuado o inadecuado que un suscriptor dé a un certificado.
- Que el certificado se esté utilizando de conformidad con las extensiones de campo del uso de clave incluido en el certificado.
- El estado del certificado y toda la cadena de certificados que se han expedido. Si cualquiera de los certificados en la cadena de certificados han sido revocados o comprometidos de alguna forma, LA PARTE QUE CONFÍA no deberá confiar en el certificado del suscriptor de usuario final u otro certificado que se encuentra revocado en la cadena de certificados.

Asumiendo que el uso del certificado es adecuado, la PARTE QUE CONFÍA utilizará el programa de cómputo adecuado para llevar a cabo la verificación de la firma electrónica avanzada u otras Operaciones criptográficas que deseen llevar a cabo como una condición de confianza en los certificados con relación a cada una de las operaciones. Dichas operaciones incluyen identificar una cadena de certificado y verificar las firmas electrónicas y/o firmas electrónicas avanzadas en todos los certificados y la cadena de certificación.

4.6. Renovación del Certificado

La renovación del certificado, consistirá en la expedición de un nuevo certificado para el suscriptor, después de pasar el certificado anterior, por el proceso de revocación.

4.6.1. Circunstancias de Renovación del Certificado

Antes del vencimiento de un certificado de suscriptor existente, es necesario que el suscriptor presente solicitud de renovación del certificado para mantener la continuidad de uso. La solicitud de renovación, también podrá ser presentada después del vencimiento.

4.6.2. Persona que puede solicitar una Renovación

Solamente el suscriptor de un certificado individual o un representante legal -para un certificado de persona jurídica-; podrán solicitar la renovación del certificado.

4.6.3. Solicitudes de proceso de una nueva expedición de Certificado para Suscriptor

Los procesos de renovación aseguran que la persona individual o persona jurídica que busca renovar un Certificado de Suscriptor, es de hecho el propio Suscriptor o el representante legal del Suscriptor del Certificado.

Un proceso aceptable es a través del uso de una carta de actualización de datos en la que el suscriptor registra la información de contacto en la que garantiza que ningún dato ha cambiado y por lo tanto no es necesario presentar nuevamente la documentación solicitada en original establecida en las Prácticas de Registro. Los suscriptores completan nuevamente el formulario de solicitud desde el sitio web www.prisma.gt y registran una clave de anulación, misma que servirá para revocar su certificado en un futuro. Después de la renovación de esta manera, REGISTRO DIGITAL PRISMA, actuando como AR y AC, reconfirma la identidad del Suscriptor de acuerdo con los requerimientos especificados en esta CP para la autenticación de una solicitud de Certificado original.

REGISTRO DIGITAL PRISMA, podrá utilizar otro proceso distinto a éste para determinar los requerimientos para la autenticación de una solicitud de certificado o de renovación de un certificado del suscriptor de usuario final. REGISTRO DIGITAL PRISMA pondrá en conocimiento del Registro de Prestadores de Servicios de Certificación, de todo cambio y/o modificación en estos procesos.

4.6.4. Notificación de expedición de Certificados para el Suscriptor

La notificación de expedición de una renovación de certificado al suscriptor es de conformidad con la sección 4.3.2. Si la información de contacto ha cambiado, el Suscriptor utilizará el procedimiento de cambio de contacto formal aprobado.

4.6.5. Conducta que constituye la aceptación de un Certificado de Renovación

La conducta que constituye la aceptación de un certificado renovado es de conformidad con la sección 4.4.1.

4.6.6. Publicación del Certificado de Renovación por parte de REGISTRO DIGITAL PRISMA

El Certificado renovado se publica en el repositorio públicamente accesible en la página web de REGISTRO DIGITAL PRISMA www.prisma.gt.

4.7. Modificación del Certificado

4.7.1. Circunstancia de modificación del Certificado

La modificación de certificado, se entenderá y gestionará conforme a la solicitud para la expedición de un nuevo certificado, debido a cambios en la información en un certificado existente (otros que no sea la clave pública del suscriptor). La modificación del certificado se considera una solicitud de certificado en términos de la sección 4.1.

4.7.2. ¿Quién puede solicitar una modificación de Certificado?

VÉASE LA SECCIÓN 4.1.1

4.7.3. Solicitudes de Proceso de Modificación de Certificado

REGISTRO DIGITAL PRISMA llevará a cabo la identificación y autenticación de toda la información del Suscriptor requerida en términos de la sección 3.2

4.7.4. Notificación de una Expedición de un Nuevo Certificado a Suscriptor

Véase la sección 4.3.2.

4.7.5. Acciones que constituyen la Aceptación del Certificado Modificado

Véase la sección 4.4.1

4.7.6. Publicación del Certificado Modificado por parte de la AC

Véase la sección 4.4.2

4.8. Revocación de Certificado

4.8.1. Circunstancias de Revocación

Solamente en las circunstancias listadas a continuación un Certificado del Suscriptor de usuario final será revocado y publicado en una CRL. También se acogerá la solicitud de un Suscriptor titular del certificado que no pueda utilizar más (o que no desee utilizar más) el mismo, por una razón que no sea la mencionada a continuación.

Un Certificado del Suscriptor de usuario final se revoca si se llegara a comprobar cualquiera de las siguientes causas:

- REGISTRO DIGITAL PRISMA, como Autoridad de Registro o un suscriptor tienen una sospecha justificada que ha habido una manipulación o un compromiso de la clave privada del suscriptor.
- REGISTRO DIGITAL PRISMA, como Autoridad de Registro tienen razones para creer que el suscriptor ha faltado a una obligación, manifestación o garantía de conformidad con el contrato de suscriptor.
- El contrato de suscriptor ha terminado, ya sea mediante la terminación anticipada del plazo o mediante la finalización del plazo.
- La relación entre una Autoridad de Registro con un Suscriptor ha terminado.
- La relación entre una persona jurídica que es un suscriptor de un certificado de persona jurídica y el representante de dicha persona jurídica que controla la clave privada del suscriptor se da por terminada.
- REGISTRO DIGITAL PRISMA tiene razones justificadas para creer que el Certificado fue expedido sin la autorización de la persona nombrada en el sujeto de dicho Certificado.
- REGISTRO PRISMA tiene razón justificada para creer que el certificado fue expedido de una manera que no haya sido acorde con los procedimientos requeridos por la CPS vigente y aplicable.
- REGISTRO DIGITAL PRISMA tiene motivos o razones suficientes para creer que el CERTIFICADO fue expedido con información presumiblemente falsa.
- REGISTRO DIGITAL PRISMA, como Autoridad de Registro determina que no se cumplió con un requisito importante de una expedición de Certificado.
- REGISTRO DIGITAL PRISMA, llega a determinar que en el caso de los certificados de personas jurídicas, el nombre de la entidad del suscriptor cambió.

- La información dentro del certificado, que no sea la información del suscriptor no fue verificada, es incorrecta o ha cambiado;
- El uso del certificado puede dañar la confianza en la PKI de Registro Digital Prisma.

EL uso del certificado puede dañar a la CONFIANZA en la PKI de REGISTRO DIGITAL PRISMA por los siguientes motivos:

- La naturaleza y número de las quejas recibidas
- La identidad de las quejas
- La legislación relacionada vigente
- Respuestas al supuesto uso dañino del Suscriptor.

El contrato de suscriptor de REGISTRO DIGITAL PRISMA contendrá una cláusula en la que se establece la obligación del suscriptor, para que notifique a REGISTRO DIGITAL PRISMA cualquier sospecha o manipulación conocida de su clave privada.

REGISTRO DIGITAL PRISMA también podrá revocar un certificado si llegara a conocer que las facultades del representante legal de la entidad para actuar como como tal han sido suspendidas o terminadas en forma definitiva.

Se tendrán incluidas como causales de revocación de Certificados, las establecidas en el artículo 47 del decreto 47-2008 del Congreso de la República de Guatemala.

4.8.2. Personas autorizadas para solicitar la revocación de un Certificado

Para los certificados emitidos a Personas Individuales, serán los propios suscriptores individuales quienes podrán solicitar la revocación. En el caso de los certificados de personas jurídicas, un representante debidamente autorizado tendrá la capacidad de solicitar la revocación de los certificados expedidos a la entidad. La entidad que aprobó una solicitud de certificado de suscriptor también podrá solicitar la revocación del certificado de suscriptor. REGISTRO DIGITAL PRISMA, como AR, debe solicitar la revocación de sus propios certificados y solicitar la cancelación de su inscripción en el RPSC con una antelación no inferior a 20 días hábiles al cese de su actividad, todos los certificados quedarán guardados en el respectivo almacén criptográfico con el que se cuenta.

4.8.3. Proceso para Solicitud de Revocación

Antes de la revocación de un Certificado, REGISTRO DIGITAL PRISMA, como AC, verifica que la revocación haya sido solicitada por el suscriptor del certificado o la entidad que aprobó la solicitud de certificado. Los procesos aceptables para autenticar las solicitudes de revocación del suscriptor incluyen:

- Que el suscriptor presente la clave de anulación y cancele el certificado automáticamente si coincide con la información que se tiene en los registros.
- Recibir un mensaje al correo electrónico suscriptor@prisma.gt que se supone es del suscriptor que solicita la revocación y que contenga una firma electrónica avanzada verificable con referencia al certificado que se revocará.
- Comunicación con el suscriptor que proporcione aseguramiento razonable, basándose en la clase de certificado, que la persona u organización que solicita la revocación es, de hecho el suscriptor, dependiendo de las circunstancias, dicha comunicación podrá incluir uno o más de lo siguiente: teléfono, fax, correo electrónico, o servicios de mensajería.

4.8.4. Período de la Solicitud de Revocación

Las solicitudes de revocación serán presentadas tan pronto como sea posible dentro de un tiempo razonable.

4.8.5. Tiempo dentro del cual REGISTRO DIGITAL PRISMA debe procesar la Solicitud de Revocación

Se toman los pasos razonables para procesar sin retraso las solicitudes de revocación.

4.8.6. Requerimientos de Revisión de Revocación para el suscriptor:

Las Partes que Confían revisarán el estado de los Certificados en los cuales desean confiar. Un método por el cual la PARTE QUE CONFÍA puede revisar el estado del certificado es consultando la CRL más reciente de REGISTRO DIGITAL PRISMA. Alternativamente, la PARTE QUE CONFÍA podrá validar el estado de un certificado utilizando OCSP.

4.8.7. Frecuencia de Expedición de las CRLS

La CRL para certificados de suscriptor, se expide por lo menos una vez al día. Si un certificado listado en una CRL vence, puede retirarse de la CRL expedida subsecuentemente después del vencimiento del certificado.

4.8.8. Duración Máxima para CRL

La CRL se indica en el repositorio dentro de un tiempo razonable después de su generación de manera automática.

4.8.9. Revocación En-Línea/Disponibilidad de Revisión de Estado

La revocación en-línea y otra información del estado del certificado están disponibles en las bases de datos de REGISTRO DIGITAL PRISMA por medio de la CRL y el servicio OCSP. La PKI de REGISTRO DIGITAL PRISMA permitirá a las PARTES QUE CONFÍAN hacer solicitudes en-línea con relación a la revocación y la información del estado de los certificados.

4.8.10. Requerimientos para Revisar la Revocación En-Línea

Una PARTE QUE CONFÍA debe revisar el estado de un certificado en el que desee confiar y deberá consultar la CRL más reciente y revisar el estado del certificado consultando el repositorio aplicable o solicitando el estado del certificado utilizando el contestador OCSP.

4.8.11. Requerimientos Especiales con Relación a la Manipulación de Claves

REGISTRO DIGITAL PRISMA utilizará todos los esfuerzos razonables para notificar a los Participantes de la PKI de REGISTRO DIGITAL PRISMA una posible manipulación real o que se sospeche de la clave privada de la AC.

4.9. Servicios de Estado de Certificado

4.9.1. Características Operacionales

El Estado de los certificados públicos está disponible vía CRL a través de un Sitio (en una URL especificada en las CPS), el directorio LDAP y vía un contestador OCSP.

4.9.2. Disponibilidad de Servicio

Los Servicios de Estado de Certificados estarán disponibles 24 x 7 sin interrupción programada.

4.9.3. Características de OCSP

El OCSP es un servicio que se prestará en base al estándar X.509 versión 3 RFC 2560 IETF, mismo que debe encontrarse disponible las veinticuatro horas, siete días a la semana, todos los días del año calendario.

4.9.4. Final de la Suscripción

Un suscriptor puede terminar una suscripción de un certificado de PKI de REGISTRO DIGITAL PRISMA:

- Dejando que su certificado venza sin renovar ese certificado o sin hacer otra clave del mismo.
- Revocando su certificado antes del vencimiento del certificado, sin reemplazarlo.

4.9.5. Depósito de la Clave y Recuperación

REGISTRO DIGITAL PRISMA no podrá dar en depósito las llaves de suscriptor usuario final. REGISTRO DIGITAL PRISMA no almacena copias de claves privadas de suscriptores.

5. Instalaciones, Administración y Controles de Operación

5.1. Controles Físicos

REGISTRO DIGITAL PRISMA cuenta en sus oficinas con controles físicos de seguridad para sus sistemas de AC y AR.

5.2. Puestos de Confianza

Los empleados, asesores, contratistas y consultores que estén designados para manejar información relativa a la PKI de REGISTRO DIGITAL PRISMA que se describe en el presente punto, serán considerados como “Personas de Confianza” que sirven en un “Puesto de Confianza”. Las personas que intentan llegar a ser Personas de Confianza obteniendo un Puesto de Confianza cumplirán con los requerimientos de monitoreo de esta CP.

Las Personas de Confianza incluyen a los empleados, asesores, contratistas y consultores que tienen acceso o autenticación de control u operaciones criptográficas que pueden afectar de manera importante:

- La validación de información en Solicitudes de Certificado;
- La aceptación, rechazo u otro procesamiento de Solicitudes de Certificado, solicitudes de revocación o solicitudes de renovación o información de inscripción;

- La expedición o revocación de Certificados, incluyendo personal que tenga acceso a partes restringidas de su repositorio o el manejo de la información o solicitudes del Suscriptor.

Las Personas de Confianza incluyen mas no están limitadas a:

- Junta Directiva y Gerencia General
- Operador PKI y Operador AC
- Personal de asesoría legal
- Oficial de Seguridad de la Información
- Personal de servicio a clientes

5.2.1. Número de Personas Requeridas por Tarea:

REGISTRO DIGITAL PRISMA, actuando como AC y AR; establecerá, mantendrá y ejercerá procesos de control estricto para asegurar la segregación de obligaciones basadas en la responsabilidad de trabajo y para asegurar que se les requiera a las múltiples Personas de Confianza, cumplir con las tareas delicadas. Los procesos de políticas y control son para asegurar la segregación de obligaciones basadas en las responsabilidades de trabajo. Las tareas más delicadas, tales como el acceso y la administración del equipo de cómputo criptográfico de la AC (unidad de firma criptográfica o CSU) y el material asociado de la clave y su administración, se encuentran ubicados en la ciudad de México, Distrito Federal (Estados Unidos Mexicanos), en un Data Center 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.

5.2.2. Identificación y Autentificación de Cada Puesto

REGISTRO DIGITAL PRISMA, confirmará la identidad y autorización de todo el personal que desea ser Personal de Confianza y antes deberán de llevar a cabo lo siguiente:

- Se les entregarán sus dispositivos de acceso y se les otorgará acceso a las instalaciones requeridas;
- Se les darán identificaciones electrónicas para acceder y llevar a cabo funciones específicas sobre los Sistemas de Información y los sistemas de REGISTRO DIGITAL PRISMA.

La autenticación de identidad incluirá la presencia (física) individual de dicho personal ante las personas de confianza que llevan a cabo funciones de recursos humanos o de seguridad dentro de una entidad y una revisión de formatos de identificación bien reconocidos, tales como documento personal de identificación (DPI), pasaportes y licencias de conducir. La idoneidad será confirmada además a través de antecedentes penales y policíacos y los procesos de revisión especificados en esta CP.

5.2.3. Puestos que Requieren Separación de Deberes

Los puestos que requieren Separación de deberes incluyen (mas no están limitados a):

- La validación de información en las Solicitudes de Certificado;
- La aceptación rechazo u otro proceso de Solicitudes de Certificado, solicitudes de revocación o solicitudes de renovación o información de registro;

La expedición o revocación de certificados, incluyendo el personal que tiene acceso a:

- Partes restringidas del repositorio;
- El manejo de la información del suscriptor o solicitudes;
- Acceso a los sistemas de producción de REGISTRO DIGITAL PRISMA.

5.2.4. Controles de Personal

La PKI de REGISTRO DIGITAL PRISMA cuenta con los estándares generales del personal que se describen a continuación:

5.2.5. Requerimientos de Habilidades, Experiencia y Autorización

REGISTRO DIGITAL PRISMA, requiere que el personal que desea llegar a ser personas de confianza presenten evidencia de los antecedentes requeridos, de las habilidades y la experiencia que se necesita para cumplir con sus eventuales responsabilidades de trabajo de manera competente y satisfactoria, así como la prueba de cualquier autorización gubernamental si fuere necesario para llevar a cabo servicios de certificación de conforme a la ley.

5.2.6. Procesos de Revisión de Antecedentes

REGISTRO DIGITAL PRISMA, llevará a cabo revisiones de antecedentes de personal que desea llegar a ser personas de confianza. Las revisiones de los antecedentes serán repetidas por el personal que tiene puestos de confianza por lo menos cada año. Estos procesos estarán sujetos a revisiones de conformidad con la ley y reglamentos aplicables. En la medida que uno de los requerimientos impuestos por esta sección no puedan cumplirse debido a una prohibición o limitación de ley local, la entidad investigadora utilizará una técnica de investigación substituta permitida por la ley que proporcione información

substancialmente similar, incluyendo mas no limitada a obtener una revisión de antecedentes llevada a cabo por una oficina de gobierno aplicable. Los factores revelados en una revisión de antecedentes que puedan ser considerados razones para rechazar a los candidatos de puestos de confianza o para tomar acción contra una persona de confianza ya existente se encuentran dentro de los procedimientos de operación del área de Recursos Humanos de REGISTRO DIGITAL PRISMA y generalmente incluyen (mas no están limitados) a lo siguiente:

- Manifestaciones fraudulentas hechas por el candidato o por la Persona de Confianza.
- Referencias profesionales altamente desfavorables o no confiables.
- Antecedentes penales, criminales o policíacos e
- Indicaciones de falta de responsabilidad financiera.

Para mayor referencia se pueden ver los procedimientos relacionados a selección y contratación dentro del área de Recursos Humanos.

Los reportes que contienen dicha información se evaluarán por personal de recursos humanos y de seguridad, y dicho personal tomará las acciones que sean razonables con base en el tipo, magnitud y frecuencia del comportamiento descubierto por la revisión de antecedentes. Dichas acciones podrán incluir medidas tales como la revocación de ofertas de empleo hechas a los candidatos de puestos de confianza o la terminación anticipada del contrato laboral con las personas de confianza existentes. El uso de la información revelada en una revisión de antecedentes para tomar dichas acciones estará sujeto a la ley aplicable. La investigación de los antecedentes de los individuos que desean ser una persona de confianza incluye:

- La confirmación de información relacionada con los empleos anteriores,
- Una revisión de referencias profesionales,
- Una confirmación del grado de escolaridad más alto o más importante obtenido,
- Una búsqueda de antecedentes penales (locales, municipales, departamentales nacionales),
- Una verificación de registros crediticios y financieros.

5.2.7. Requerimientos de Capacitación

REGISTRO DIGITAL PRISMA, para lo que sea pertinente a sus roles como AC y como AR, proporcionará a su personal la capacitación necesaria para cumplir con sus responsabilidades laborales con relación a las

operaciones como Autoridad de Registro y las de Autoridad de Certificación, de manera competente y satisfactoria. También revisará periódicamente sus programas de capacitación y ésta tratará los elementos relacionados con las funciones llevadas a cabo por su personal.

Los programas de capacitación deben tratar los elementos relacionados con el ambiente específico de la persona que se capacita, incluyendo:

- Principios de seguridad y mecanismos de la PKI de REGISTRO DIGITAL PRISMA
- Equipo de cómputo y versiones de programas de cómputo en vigor,
- Todos los deberes que se espera que la persona lleve a cabo,
- Reporte y manejo de incidentes y manipulaciones, y
- Procedimientos de recuperación o de desastre y continuidad del negocio.

5.2.8. Frecuencia y Requerimientos de Nueva Capacitación

REGISTRO DIGITAL PRISMA proporcionará capacitación nueva y actualizaciones a su personal en la medida y frecuencia requerida para asegurar que dicho personal mantiene el nivel requerido de eficiencia para cumplir con las responsabilidades de su trabajo de manera competente y satisfactoria.

5.2.9. Sanciones para Acciones No Autorizadas

REGISTRO DIGITAL PRISMA mantendrá y ejercerá las políticas de empleo para la disciplina del personal que siga acciones no autorizadas. Las acciones disciplinarias podrán incluir medidas tales como la terminación anticipada del contrato laboral y serán proporcionales a la frecuencia y gravedad de los actos no autorizados.

5.2.10. Requerimientos de Contratistas Independientes

REGISTRO DIGITAL PRISMA, podrá permitir a los contratistas independientes o consultores como Personas de Confianza solamente en la medida necesaria para ajustarse a relaciones independientes claramente definidas y solamente conforme a las siguientes condiciones:

- Que la entidad que utilice los contratistas independientes o consultores como Personas de Confianza no tengan empleados adecuados disponibles para llenar los puestos de Personas de Confianza, y

- Que la entidad confíe en contratistas o consultores en la misma medida como si fueran empleados.

De lo contrario, los contratistas independientes y consultores tendrán acceso a las instalaciones de seguridad de REGISTRO DIGITAL PRISMA solamente en la medida en que estén acompañados y directamente supervisados por las Personas de Confianza.

5.2.11. Documentación proporcionada al Personal

REGISTRO DIGITAL PRISMA proporcionará a su personal (incluyendo las Personas de Confianza) la capacitación necesaria y el acceso a otra documentación que se necesite para cumplir con sus responsabilidades de trabajo de manera competente y satisfactoria.

5.3. Procedimientos de Bitácoras de Auditoría del ciclo de vida de los certificados

5.3.1. Tipos de Eventos Registrados

Los tipos de eventos auditables que deben ser registrados por REGISTRO DIGITAL PRISMA se establecen a continuación. Todas las bitácoras electrónicas, contendrán la fecha y hora del evento, y la identidad de la persona o entidad que causó el evento. REGISTRO DIGITAL PRISMA, establecerá en su CPS, los registros de eventos relacionados con el ciclo de vida del certificado (punto 4.5 de la CPS).

El acceso a las bitácoras de auditoría se protege mediante el uso de un certificado al acceder al sistema de bitácoras de auditoría del ciclo de vida de los certificados.

5.3.2. Evaluaciones de Vulnerabilidad

Se llevan a cabo evaluaciones de seguridad lógicas de vulnerabilidad, se revisan y se verifican después de un examen de estos eventos monitoreados. Las evaluaciones se basan en datos automatizados cargados en tiempo real y de forma periódica de acuerdo a las políticas de REGISTRO DIGITAL PRISMA. Una evaluación anual podrá efectuarse en el mismo momento que sea requerida en una Auditoría de Cumplimiento anual de la entidad.

5.4. Registros de Archivos

5.4.1. Tipos de Registros Archivados

REGISTRO DIGITAL PRISMA, como AC y como AR, archiva:

- Todos los datos de auditoría reunidos conforme a la Sección 5.4.
- Información de solicitud de Certificado.
- Documentación soportando la información de solicitud de certificado.
- Información del ciclo de vida del certificado, por ejemplo, revocación e información de solicitud de renovación.

5.4.2. Período de Guarda de Archivos

Los registros serán guardados por lo menos por un término de diez años, en caso que la ley aplicable no establezca otro específico para determinado acto en particular.

5.4.3. Protección de Archivos

Una entidad que mantiene un archivo de registros, protegerá el mismo de manera que solamente las Personas de Confianza de la entidad puedan tener acceso al archivo. El archivo se protege contra acceso, modificación, supresión no autorizada u otra alteración mediante almacenamiento con un sistema confiable. Los medios que guardan los datos de archivos y las aplicaciones requeridas para procesar los datos de archivo se mantendrán para asegurar que los datos del archivo pueden ser accedidos por el tiempo establecido en esta CP.

5.4.4. Procesos de Respaldo de Archivos

Las entidades que compilan información electrónica respaldarán de manera incrementada los archivos de sistemas de dicha información diariamente y llevarán a cabo respaldos totales. Las copias de registros en papel se mantendrán en una instalación segura fuera del sitio. REGISTRO DIGITAL PRISMA, garantizará en todo caso la integridad, confidencialidad de los registros, así como mantener la privacidad de los registros del suscriptor.

REGISTRO DIGITAL PRISMA, actúa de conformidad con la Política de Respaldos de la Norma ISO27001:2013, por lo que la designación descriptiva de actividades que lleva a cabo REGISTRO DIGITAL PRISMA, para tales fines, incluye el backup de base de datos, de sistemas operativos; aplicación web y de gestión de clientes, configuración de switch y firewall y de grabación de cámaras de seguridad, actividades que se realizan con la periodicidad establecida en la mencionada política.

5.4.5. Requerimientos para Sello de Hora de Recepción de los Registros

Los Certificados, la CRL y otros registros de revocación contendrán la información de hora y fecha. Dicha información de tiempo no necesita estar criptográficamente basada.

5.4.6. Sistema de Recolección de Archivos (Interno o Externo)

REGISTRO DIGITAL PRISMA recolectará archivos de forma externa, a través del formulario disponible en el sitio web www.prisma.gt. La documentación de soporte de las solicitudes de emisión de certificados, se hará por medios electrónicos o magnéticos que estén al alcance del solicitante, los cuales serán almacenados en un repositorio seguro.

El mecanismo de respaldo de la información recolectada, es mediante copia de seguridad incremental de dichos archivos, resguardados en medios magnéticos, resguardados en el área segura de REGISTRO DIGITAL PRISMA.

5.4.7. Procesos para Obtener y Verificar Información de Archivos

Solamente el Personal de Confianza autorizado puede obtener acceso al archivo. La integridad de la información se verifica cuando se restaura.

5.5. Manipulación y Recuperación en Caso de Desastre

5.5.1. Procesos de Manejo de Incidentes y Manipulaciones

REGISTRO DIGITAL PRISMA, actuando como AC y como AR, cuenta con un procedimiento para la gestión de incidentes, apegado a la norma ISO27001:2013. Dicha norma la clasificación de incidentes, debilidades y defectos, estableciendo el procedimiento para el tratamiento de las debilidades o eventos de seguridad, así como el tratamiento de incidentes menores y graves, con el objetivo de garantizar la detección temprana de las debilidades y eventos de seguridad, así como la rápida reacción y respuesta hacia el incidente. Cada empleado, proveedor y/o tercero, que esté en contacto con información y/o sistemas de REGISTRO DIGITAL PRISMA, debe de reportar lo antes posible y por el medio que esté a su alcance toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente. Es el Oficial de Seguridad Informática, el responsable de gestionar y dar respuesta a dichas alertas, conforme lo establecido en el procedimiento para gestión de incidentes que forma parte del SGSI.

REGISTRO DIGITAL PRISMA, mantiene en almacenamiento fuera del sitio y se pondrán a disposición en el caso de una Manipulación o desastre, los respaldos de la siguiente información: los datos de la Solicitud del Certificado, datos de auditoría y registros de base de datos para todos los Certificados expedidos, así como los archivos de soporte para la emisión de los Certificados.

5.5.2. La Corrupción de los Recursos de Cómputo, Programas de Cómputo y/o Datos

Después de que haya una corrupción de recursos de cómputo, programas de cómputo, y/o datos, REGISTRO DIGITAL PRISMA, como AC y como AR, preparará inmediatamente un reporte del incidente y una respuesta al evento de conformidad con LOS PROCESOS DE REPORTE Y MANEJO DE INCIDENTES Y MANIPULACIONES DE REGISTRO DIGITAL PRISMA DOCUMENTADOS en la CPS aplicable y las políticas documentadas confidenciales de seguridad de la PKI de REGISTRO DIGITAL PRISMA.

5.5.3. Capacidad de Continuidad de Negocios después de un Desastre

REGISTRO DIGITAL PRISMA cuenta con el apoyo de la infraestructura desarrollada dentro de su PKI con un plan de recuperación en caso de desastres diseñado para mitigar los efectos de cualquier clase de desastre natural o provocado por el hombre. Los planes de recuperación en caso de desastre tratan la restauración de los servicios de sistemas de información y las funciones de negocio clave. Los sitios de recuperación en caso de desastre tienen las protecciones de seguridad física especificadas por la CPS de la PKI de REGISTRO DIGITAL PRISMA.

5.6. Terminación de la AC o AR:

La terminación de REGISTRO DIGITAL PRISMA como AC o como AR estará sujeta a lo establecido por el artículo 13 del Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas, en sus literales d), h), i) y j), y/o la normativa legal vigente. REGISTRO DIGITAL PRISMA, así como los suscriptores y los demás participantes en la PKI de REGISTRO DIGITAL PRISMA; de buena fe, utilizarán los esfuerzos que sean razonables para convenir un plan de terminación que minimice la interrupción a los Clientes, Suscriptores y partes que confían. El plan de terminación puede cubrir aspectos tales como: Proporcionar notificación a las partes afectadas por la terminación, tales como:

- Suscriptores y PARTE QUE CONFÍA.
- Manejo del costo de dicha notificación,
- La revocación del Certificado expedido por REGISTRO DIGITAL PRISMA,

- La preservación de los archivos y registros de la AC durante los períodos de tiempo requeridos por esta CP.
- La continuación de los servicios de soporte del Suscriptor y del cliente.
- La continuación de los servicios de revocación, tales como la expedición de CRL o el mantenimiento de servicios de revisión de estado en línea.
- La revocación de Certificados no vencidos de Suscriptores usuario final y AC's subordinadas, si es necesario.
- El reembolso (si es necesario) a Suscriptores cuyos Certificados no han sido vencidos y no se han revocado para que sean revocados conforme al plan o disposición de terminación para la expedición de un sucesor de la AC de los Certificados sustituto.
- La disposición de la clave privada de la AC y el token que contienen dicha clave privada.
- Disposiciones que se necesitan para la transición de los servicios de la AC a un sucesor de la CA. La transición de los servicios, puede o no puede trasladarse a otro prestador de servicio de certificación autorizado, siempre y cuando no exista oposición.

Dicha notificación, deberá de darse con antelación de por lo menos quince días hábiles, de conformidad con el Reglamento de la ley para el reconocimiento de las comunicaciones y firmas electrónicas. Asimismo, se deberá de notificar al Registro de Prestadores de Servicios de Certificación de tal circunstancia.

6. Controles Técnicos de Seguridad

6.1. Generación e Instalación de Par de Claves

6.1.1. Generación de Par Claves

La generación del par de claves se llevará a cabo utilizando los Sistemas de Confianza y los procesos que proporcionan la fuerza criptográfica requerida de las claves generadas y que previenen la pérdida, divulgación, o uso no autorizado de las claves privadas. Los suscriptores deben generar su par de claves confidencialmente. Este requerimiento aplica a los Suscriptores usuario final de certificados de persona jurídica o individual.

Las Claves de AC se generan en una Ceremonia de Generación de Claves. Todas las Ceremonias de Generación de Claves se apegan a los requerimientos documentados en las políticas confidenciales de seguridad de la PKI de REGISTRO DIGITAL PRISMA.

6.1.2. Entrega de Clave Privada al Suscriptor

Las claves privadas del Suscriptor usuario final son generadas por los mismos Suscriptores usuario final, y por lo tanto, la entrega de la clave privada a un Suscriptor, se realiza directamente en el dispositivo criptográfico autorizado, que incluirá el par de claves. Al almacenar el certificado en un dispositivo criptográfico, el solicitante suscriptor debe por seguridad cambiar la clave de acceso al mismo.

6.1.3. Entrega de Clave Pública a parte que Confía

Las claves públicas de REGISTRO DIGITAL PRISMA se incluyen en los Certificados raíz y que no estén insertadas dentro de alguna aplicación de las muchas aplicaciones de programas de cómputo, haciendo que los mecanismos especiales de distribución de las raíces sean innecesarios. También, en muchas instancias, la PARTE QUE CONFÍA que utiliza el protocolo S/MIME automáticamente recibirá, además del Certificado del Suscriptor, los Certificados (y por lo tanto las claves públicas) de REGISTRO DIGITAL PRISMA.

6.1.4. Tamaños de Clave

El par de claves serán de suficiente tamaño para evitar que personas no autorizadas puedan fácilmente revelar o averiguar la clave privada utilizando criptoanálisis durante el período de uso de dicho par de claves. El Estándar Actual de la PKI de REGISTRO DIGITAL PRISMA para tamaños de clave mínimos es de 2048 bits en RSA para los certificados de suscriptor y de 4096 bits para los certificados AC y AR.

6.1.5. Generación de Parámetros de Clave Pública y Revisión de Calidad

REGISTRO DIGITAL PRISMA utiliza un conjunto de algoritmos en la generación de firma electrónica avanzada basados en el estándar FIPS 140-2 nivel 3 para el almacenamiento seguro de la firma electrónica avanzada, a través del cual REGISTRO DIGITAL PRISMA garantiza la calidad de los Parámetros Clave generados, almacenamiento seguro y el no repudio a la información.

6.1.6. Propósitos de Uso de Clave (Según Campo de Uso de Clave X.509 V3)

Refiérase a la sección 7.1.2.

6.1.7. Estándares y Controles de Módulo Criptográfico

Las claves privadas dentro de REGISTRO DIGITAL PRISMA se protegerán utilizando un Sistema confiable y los propietarios de las claves privadas tomarán las precauciones necesarias para prevenir la pérdida, divulgación, o uso no autorizado de dichas Claves Privadas de conformidad con esta CP, las obligaciones contractuales y los requerimientos documentados en las políticas confidenciales de seguridad de la PKI de REGISTRO DIGITAL PRISMA. Los Suscriptores Usuarios Finales tienen la opción de proteger sus claves privadas en tarjetas inteligentes u otro token criptográfico. REGISTRO DIGITAL PRISMA llevará a cabo todas las operaciones criptográficas AC en módulos criptográficos clasificados en un mínimo de FIPS 140-2 nivel 3.

6.1.8. Control de Clave Privada (M fuera de N) de multi-persona

El control de multi-persona se ejerce para proteger los datos de activación necesitados para activar las claves privadas AC que tiene REGISTRO DIGITAL PRISMA, conforme a los estándares documentados en las políticas confidenciales de seguridad de la PKI de REGISTRO DIGITAL PRISMA. Se utilizarán "Secretos Compartidos" para dividir la clave privada o los datos de activación necesitados para operar la clave privada en partes separadas llamadas "Partes Secretas" que tienen los individuos denominados los "Propietarios de las Partes". El mismo número de Partes Secretas (m) del total de Partes Secretas (n) se requerirá para operar la clave privada. REGISTRO DIGITAL PRISMA utiliza Secretos compartidos para proteger los datos de activación requeridos para activar sus propias claves privadas, conforme a los estándares documentados en las políticas confidenciales de seguridad de la PKI de REGISTRO DIGITAL PRISMA. REGISTRO DIGITAL PRISMA también utiliza secretos compartidos para proteger los datos de activación necesarios para activar las claves privadas, localizadas en sus respectivos sitios de recuperación en caso de desastre. El mismo número de partes necesitado para firmar un certificado AC es de 3. Debe tomarse en cuenta que el número de partes distribuido para tokens en caso de desastre puede ser menor que el número distribuido para tokens operacionales, mientras que el número mismo de acciones requeridas sigue siendo el igual.

6.1.9. Clave Privada en Depósito

Las claves privadas no se depositan.

6.2. Respaldo de Clave Privada

REGISTRO DIGITAL PRISMA, como AC, respaldará sus propias claves privadas de manera que puedan recuperarse de desastres y malfuncionamiento del equipo de conformidad con los estándares documentados en las políticas confidenciales de seguridad de la PKI de REGISTRO DIGITAL PRISMA. Los respaldos serán hechos de acuerdo con estas políticas documentadas. Los respaldos serán hechos copiando dichas claves privadas y registrándolas en los módulos criptográficos de respaldo conforme a la Sección 6.2.6 y 6.2.7.

6.2.1. Archivo de Clave Privada

Cuando el par de claves de la AC lleguen al final de su período de validez, dicho par de claves AC se archivarán durante un período de por lo menos 10 años. El par de claves de la AC archivadas serán almacenadas de manera segura utilizando módulos de equipo criptográfico que cumpla con los requerimientos de esta CP. Los controles de procedimientos evitan que el par de claves de la AC archivadas se devuelvan a producción para uso. Al momento del final del período archivado, las claves privadas AC archivadas serán destruidas de manera segura conforme a esta CP.

6.2.2. Transferencia de Clave Privada hacia o desde un Módulo Criptográfico

El registro de una clave privada en un módulo criptográfico utilizará los mecanismos para prevenir la pérdida, el robo, la modificación, la divulgación no autorizada o el uso no autorizado de dicha clave privada. Cuando REGISTRO DIGITAL PRISMA genera las claves privadas AC o AR en un módulo de equipo criptográfico y que las transfieren hacia otro de manera segura, dichas claves privadas hacia el segundo módulo criptográfico en la medida necesaria para prevenir pérdida, robo, modificación, divulgación no autorizada, o uso no autorizado de dichas claves privadas. Las transferencias estarán limitadas a hacer copias de respaldo de las claves privadas en tokens de conformidad con los estándares documentados en las políticas confidenciales de seguridad de la PKI de REGISTRO DIGITAL PRISMA. Las claves privadas serán encriptadas durante la transferencia.

6.2.3. Almacenamiento de la Clave Privada en Módulo Criptográfico

Las claves privadas AC o AR que se tienen en módulos de equipo criptográfico se almacenan en formatos encriptados.

6.2.4. Método de Protección de La Clave Privada

REGISTRO DIGITAL PRISMA no conserva ninguna copia de las claves privadas, por lo que recomienda que el suscriptor proteja sus claves privadas contra la pérdida, robo, modificación, divulgación no autorizada o uso no autorizado.

i. **CERTIFICADOS**

El Estándar de la PKI de REGISTRO DIGITAL PRISMA para protección de clave privada (que no sea la de Administradores) es para que los suscriptores:

- Utilicen un dispositivo criptográfico, o seguridad de fuerza equivalente, para autenticar al suscriptor antes de la activación de la clave privada; y
- Tomen las medidas razonables para la protección física del dispositivo criptográfico utilizado y evitar el uso de su clave privada asociada sin la autorización del suscriptor.

Aun cuando la guarda y custodia de la clave privada es responsabilidad del suscriptor, se recomienda el uso de una contraseña, quedando a discreción del suscriptor, colocar dicha contraseña en los casos en los que el certificado sea instalado en un servidor para emisión masiva de firma electrónica avanzada.

ii. **CLAVES PRIVADAS EN PODER DE REGISTRO DIGITAL PRISMA**

Se activará una clave privada AC en-línea por un mismo número de Propietarios de Partes, como se define en la Sección 6.2.2, que proporcionen sus datos de activación (almacenados en medios seguros). Una vez que la clave privada se active, la clave privada podrá estar activa por un período de tiempo indefinido hasta que se desactive cuando el AC salga de la línea. Asimismo, se les requerirá a un mismo número de propietarios de las partes sus datos de activación con el objeto de activar una clave privada AC fuera de línea. Una vez que la clave privada se active, estará activa solamente por una vez.

6.2.5. Método de Desactivación de Clave Privada

Los Suscriptores usuarios finales tienen la obligación de proteger sus claves privadas. Dichas obligaciones se extienden a la protección de clave privada después de que se le haya generado y entregado su clave privada. La clave privada puede ser desactivada, mediante su exportación a otro dispositivo criptográfico, o simplemente desactivando y resguardando el dispositivo criptográfico donde se encuentre resguardado.

6.2.6. Método de Destrucción de Clave Privada

Al terminar las operaciones de REGISTRO DIGITAL PRISMA como AC, o cuando se dé el caso de la pérdida, robo, modificación, divulgación no autorizada, o uso no autorizado de una clave privada de A.C., el personal desactivará la clave privada de REGISTRO DIGITAL PRISMA como AC, eliminándola utilizando la funcionalidad del token que contiene dicha clave privada de AC para prevenir su recuperación después de la eliminación. Este proceso será vigilado de conformidad con los estándares documentados en las políticas de seguridad confidencial en la PKI de REGISTRO DIGITAL PRISMA y en todo caso, se dará aviso al Registro de Prestadores de Servicios de Certificación del Ministerio de Economía.

6.3. Otros Aspectos de la Administración del Par de Claves

6.3.1. Archivo de Clave Pública

REGISTRO DIGITAL PRISMA archivarán sus propias claves públicas, de conformidad con la Sección 5.4.

6.3.2. Períodos Operacionales de Certificados y Períodos de Uso de Par de Claves:

El Período Operacional para los Certificados, se establecerá conforme a los límites de tiempo establecidos en la Tabla a continuación. El período de uso para el par de claves de Suscriptor usuario final es el mismo que el Período Operacional para sus Certificados, excepto que las claves privadas pueden continuar utilizándose después del Periodo Operacional para desencriptación y verificación de firma electrónica avanzada. El Período Operacional de un Certificado termina al momento de su vencimiento, o de su revocación. REGISTRO DIGITAL PRISMA no expedirá certificados si sus períodos operacionales se extienden más allá del período de uso del par de claves de la AC. Por lo tanto, el período de uso del certificado del suscriptor, es necesariamente más corto que el período operacional del Certificado AC. Específicamente, el período de uso es el Período Operacional del Certificado AC menos el Período Operacional de los Certificados de los suscriptores. Al vencimiento o a la fecha de la revocación de un certificado de Suscriptor, o del par de claves de REGISTRO DIGITAL PRISMA, como AC, el Suscriptor o el propio REGISTRO DIGITAL PRISMA, en su caso, cesarán posteriormente todo el uso del par de claves, excepto en la medida que REGISTRO DIGITAL PRISMA, como AC necesite firmar información de revocación hasta el final del Período Operacional del último Certificado que haya expedido.

Certificado expedido 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.

Tabla – Períodos Operacionales de Certificado

6.4. Datos de Activación

6.4.1. Generación e Instalación de Datos de Activación

REGISTRO DIGITAL PRISMA, al generar e instalar datos de activación de sus claves privadas utilizarán los métodos que protegen los datos de activación en la medida necesarias para prevenir la pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de las claves privadas. En la medida que se utilizan las contraseñas como datos de activación, los suscriptores generarán contraseñas que no fácilmente pueden ser adivinadas o penetradas por ataques de archivos y directorios electrónicos.

REGISTRO DIGITAL PRISMA genera datos de activación para sus propias claves privadas de AC, de conformidad con los estándares documentados en las políticas confidenciales de seguridad de la INFRAESTRUCTURA DE CLAVE PÚBLICA de REGISTRO DIGITAL PRISMA.

6.4.2. Protección de Datos de Activación

REGISTRO DIGITAL PRISMA protegerá los datos de activación para sus claves privadas utilizando los métodos que protegen contra pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de dichas claves privadas. Los Suscriptores usuario final protegerán los datos de activación para sus claves privadas en la medida necesaria para prevenir pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de dichas claves privadas. REGISTRO DIGITAL PRISMA proporciona los procesos y medios para dar la capacidad a los usuarios y propietarios de información confidencial, y estos deberán de tomar las precauciones necesarias para prevenir pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de toda información confidencial que está en su poder. Los usuarios o propietarios de información confidencial, no llevarán a cabo los siguientes actos:

- Copiarán, divulgarán o pondrán a disposición de un tercero la información confidencial que tienen a su cargo ni harán ningún uso no autorizado de ella; ni
- Divulgarán a ningún tercero su carácter o el carácter de otra persona como un usuario o propietario de información confidencial.

Cualquier información divulgada a REGISTRO DIGITAL PRISMA, por parte del Propietario de la misma, con relación a sus obligaciones como usuario o propietario de dicha información, constituyen Información Confidencial. REGISTRO DIGITAL PRISMA mantiene un registro de auditoría de información confidencial.

6.4.3. Otros Aspectos de Datos de Activación

i. **TRANSMISIÓN DE DATOS DE ACTIVACIÓN**

En la medida en que se transmitan los datos de activación para sus claves privadas, REGISTRO DIGITAL PRISMA protegerá la transmisión de dichas claves, utilizando protocolos seguros de comunicación, entre el usuario y REGISTRO DIGITAL PRISMA, garantizando que dicha comunicación está encriptada y protegida contra robo, modificación y/o divulgación o uso no autorizados de dichas claves privadas.

ii. **DESTRUCCIÓN DE DATOS DE ACTIVACIÓN**

Los datos de activación para claves privadas AC serán desactivados utilizando métodos que protegen contra la pérdida, robo, modificación, divulgación no autorizada o uso no autorizado de dichas claves privadas protegidas por dichos datos de activación. Después de que venzan los períodos de retención de registros especificados en la Sección 5.4.2, REGISTRO DIGITAL PRISMA desactivará los datos de activación mediante sobre-escritura y/o destrucción física.

6.5. Controles de Seguridad de Computadoras

Las funciones AC y AR ocurren en los Sistemas confiables de conformidad con los estándares documentados en las políticas confidenciales de seguridad de la PKI de REGISTRO DIGITAL PRISMA.

6.5.1. Requerimientos técnicos específicos de seguridad de computadoras

REGISTRO DIGITAL PRISMA asegurará que los sistemas que guardan los programas de cómputo y archivos de datos de la AC, son Sistemas confiables seguros contra acceso no autorizado, que puede demostrarse

mediante el cumplimiento con el criterio de auditoría aplicable conforme a la Sección 4.5.1. Además, REGISTRO DIGITAL PRISMA da acceso limitado y únicamente permitirá acceso a los equipos que realizan las funciones de AR y de AC –ubicados en el perímetro físico identificado como área segura-; a través de accesos biométricos exclusivamente otorgados al operador PKI y al operador AC. Los demás funcionarios, empleados, y en general, los usuarios de aplicación general que no sean los ya mencionados, no tendrán cuentas en dichos equipos, ni acceso biométrico al área segura designada. REGISTRO DIGITAL PRISMA tendrá las redes de producción lógicamente separadas de otros componentes. Esta separación previene el acceso a la red excepto a través de procesos de aplicación definidos. Se utilizarán sistemas de seguridad externos (firewalls) para proteger la red de producción de intrusiones internas y externas y limitar la naturaleza y fuente de las actividades de la red que puedan tener acceso a los sistemas de producción. Se requerirá del uso de contraseñas con un mínimo de tamaño de caracteres y una combinación de caracteres alfanuméricos y especiales, y requerirán que las contraseñas se cambien periódicamente y cuando sea necesario. El acceso directo a una base de datos de REGISTRO DIGITAL PRISMA que guarda el repositorio de REGISTRO DIGITAL PRISMA estará limitado a las Personas de Confianza, identificadas como Operador PKI y operador AC.

REGISTRO DIGITAL PRISMA, separará de manera lógica, el acceso a estos sistemas y a esta información de otros componentes. Esta separación previene el acceso excepto a través de procesos definidos. REGISTRO DIGITAL PRISMA, utilizará sistemas de seguridad externos para proteger la red de intrusiones internas y externas y limitarán la naturaleza y fuente de actividades que puedan tener acceso a dichos sistemas e información. REGISTRO DIGITAL PRISMA, requerirá el uso de contraseñas con un mínimo de tamaño de caracteres y requerirán que las contraseñas se cambien periódicamente y según sea necesario. El acceso directo a la base de datos de la AR que guarda información del Suscriptor estará limitado a las Personas de Confianza identificadas como Operador PKI y operador AC.

6.5.2. Seguridad de dispositivos

Los dispositivos de cómputo que se utilicen por REGISTRO DIGITAL PRISMA, en sus roles de AC y de AR, deberán cumplir con estándares de seguridad altos tanto de acceso a las redes como de seguridad local del dispositivo entre ellos, claves de arranque, claves de disco duro, utilización de dispositivos criptográficos, biométricos conforme sea requerido para salvaguardar tanto el hardware como el software.

6.6. Controles Técnicos de Ciclo de Vida

6.6.1. Controles de Desarrollo de Sistema

REGISTRO DIGITAL PRISMA proporciona programas de cómputo para funciones AC y AR. Dicho programa de cómputo, en la medida utilizada para manejar Certificados ha sido desarrollado dentro de un ambiente de desarrollo de sistemas que cumplan con los requerimientos de REGISTRO DIGITAL PRISMA.

REGISTRO DIGITAL PRISMA utilizará un proceso de diseño y desarrollo que ejerza aseguramiento de calidad y corrección de procesos.

6.6.2. Controles de Administración de Seguridad

El programa de cómputo para funciones de AC y AR, diseñado para administrar certificados estará sujeto a revisiones para verificar su integridad. REGISTRO DIGITAL PRISMA proporciona una mezcla de todos sus paquetes de programas de cómputo o actualizaciones de programas de cómputo. Esta mezcla puede utilizarse para verificar la integridad de dichos programas de cómputo de manera manual. También se tendrán mecanismos y/o políticas para controlar y monitorear la configuración de sus sistemas AC. En el momento de la instalación y por lo menos una vez al día, REGISTRO DIGITAL PRISMA validará la integridad del sistema AC.

6.7. Controles de Seguridad de Red

Las funciones que tiene REGISTRO DIGITAL PRISMA como AC y AR se llevan a cabo utilizando redes aseguradas de conformidad con los estándares documentados en las Políticas de Confidencialidad de REGISTRO DIGITAL PRISMA para evitar el uso no autorizado, la falsificación y ataques de negación del servicio. Las comunicaciones de información delicada estarán protegidas utilizando sistemas de encripción punto-a- punto para electrónicas avanzadas para no-rechazo y autenticación.

6.8. Sellos de Hora de Recepción

Los certificados, las CRLs y OCSP, contendrán información de la hora y la fecha. Dicha información de la hora no necesita ser criptográfica.

7. Certificado, CRL y Perfiles OCSP

7.1. Perfil de Certificado

Los Certificados de la PKI de REGISTRO DIGITAL PRISMA se apegan al estándar (a) ITU-T Recomendación X.509 (1997): Tecnología de la Información – Interconexión de Sistemas Abiertos – El Directorio: Estructura de Autenticación, Junio 1997 y (b) RFC 3280: Internet X.509 Certificado de PKI y al Perfil CRL, Abril 2002 ("RFC 3280"). Por lo menos, los Certificados X.509 REGISTRO DIGITAL PRISMA contendrá los campos básicos y los valores indicados prescritos o las obligaciones de valor especificados en la Tabla a continuación:

Campo	**Valor u Obligación de Valor**
Número de serie:	Valor único por Emisor DN
Algoritmo Firma	SHA-2 con RSA
Emisor	Valor único por Emisor DN
Válido desde	Base Universal de Tiempo Coordinado. Codificado de acuerdo con la RFC 5280.
Válido hasta	Base Universal de Tiempo Coordinado. Codificado de acuerdo con la RFC 5280.
Suscriptor	Valor único por Emisor DN
Clave Pública	Codificado de acuerdo con la RFC 5280 Certificado de Suscriptor: 2048 bits Certificado de AC/AR: 4096 bits
Firma	Generado y codificado de conformidad con la RFC 5280.

Tabla – Campos Básicos de Perfil de Certificado.

7.1.1. Número(s) de Versión

Los Certificados REGISTRO DIGITAL PRISMA serán Certificados X.509 Versión 3. Los Certificados AC serán Certificados AC X.509 Versión 3. Los Certificados de Suscriptor usuario final serán X.509 Versión 3.

7.1.2. Extensiones de Certificado

REGISTRO DIGITAL PRISMA distribuirá Certificados X.509 Versión 3 con las extensiones requeridas por la Sección 7.1.

i. **USO DE LA CLAVE**

Generalmente se distribuyen Certificados X.509 Versión 3 de conformidad con la RFC5280: Internet X.509 Versión 3, Certificado de Infraestructura Clave Pública X.509 Versión 3 y Perfil CRL, Abril2002. La extensión de Uso de Clave en los Certificados X.509 Versión 3 generalmente se configura para establecer y autorizar datos y el campo crítico de conformidad con la Tabla a continuación.

El campo crítico en la extensión del Uso de la Clave generalmente se establece como falso.

		ACs	**Suscriptores Usuario Final Clase 2**
Criticalidad		FALSO	FALSO
0	digitalSignature	Autorizado	Establecido
1	nonRepudation	Autorizado	Autorizado
2	keyEncipherment	Autorizado	Establecido
3	dataEnchipherment	Autorizado	Autorizado
4	keyAgreement	Autorizado	Autorizado
5	keyCertSign	Establecido	Autorizado
6	CRLSign	Establecido	Autorizado
7	enchipherOnly	Autorizado	Autorizado
8	dicipherOnly	Autorizado	Autorizado

APLICACIONES PARA EXTENSIÓN DEL USO DE CLAVE

Nota: Aunque el bit nonRepudation no está establecido en la extensión de Uso de Clave, REGISTRO DIGITAL PRISMA sin embargo, soporta los servicios de nonRepudation para los Certificados que emite. No se requiere que el bit nonRepudation sea establecido en estos Certificados, porque la industria de la PKI no ha alcanzado un consenso de lo que significa el bit nonRepudation. Hasta que surja tal consenso, el bit

nonRepudation no será significativo para PARTE QUE CONFÍA. Además, las aplicaciones más comúnmente utilizadas no reconocen el bit nonRepudation. Por lo tanto, establecer el bit no ayudará a la PARTE QUE CONFÍA a tomar una decisión confiable. Consecuentemente, esta CP requiere que el bit nonRepudiation sea autorizado.

ii. **EXTENSIÓN DE POLÍTICAS DE CERTIFICADO**

La extensión de las Políticas de Certificado de Certificados X.509 Versión 3 se distribuye con el objeto identificador de esta CP de conformidad con la Sección 7.1.6 y con los calificadores de política establecidos en la Sección 7.1.8. El campo crítico de esta extensión se establecerá en FALSO.

iii. **NOMBRES ALTERNATIVOS DE SUJETO**

La extensión subjectAltName de los Certificados X.509 Versión 3, se distribuyen de acuerdo con la RFC 3280. El campo crítico de esta extensión se establecerá en FALSO.

iv. **OBLIGACIONES BÁSICAS**

La extensión de Obligaciones Básicas de Certificados AC X.509 Versión 3 tendrá el campo AC establecido en VERDADERO. La extensión de Obligación Básica de Certificados de Suscriptor Usuario Final se distribuirá con un valor de una secuencia vacía. El campo crítico de esta extensión se establecerá en VERDADERO para los Certificados AC de lo contrario se establecerá en FALSO.

Los Certificados AC X.509 Versión 3 tendrán un campo “pathLenConstraint” de la extensión de Obligaciones Básicas establecido en el número máximo de certificados AC que pueden seguir a este Certificado en un patrón de certificación. Los Certificados AC expedidos a un Cliente en-línea que expide Certificados de Suscriptor usuario final tendrán un campo “pathLenConstraint” establecido en un valor “0” indicando que solamente un Certificado de Suscriptor usuario final podrá seguir en el patrón de certificación.

v. **PUNTOS DE DISTRIBUCIÓN DE CRL**

Los certificados de la PKI DE REGISTRO DIGITAL PRISMA X.509 Versión 3 se distribuyen con una extensión CrlDistribution que contiene el URL de la ubicación donde una PARTE QUE CONFÍA puede obtener una CRL para verificar el estado del Certificado. El campo de criticalidad de esta extensión se establecerá en FALSO.

vi. **IDENTIFICADOR DE CLAVE DE AUTORIDAD**

Los certificados emitidos en la PKI DE REGISTRO DIGITAL PRISMA X.509 Versión 3 generalmente se distribuyen con una extensión authorityKeyIdentifier. El método para generar el keyIdentifier basado en la clave pública de la AC que expide el Certificado se calculará de acuerdo a uno de los métodos descritos en la RFC 5280. El campo crítico de esta extensión se establecerá en FALSO.

vii. **IDENTIFICADOR DE CLAVE DE SUJETO**

En los certificados emitidos en la PKI DE REGISTRO DIGITAL PRISMA X.509 Versión 3, el campo crítico de esta extensión se establecerá en FALSO y el método para generar el keyIdentifier basado en la clave pública del Sujeto del Certificado se calculará de acuerdo con uno de los métodos descritos en la RFC 5280.

viii. **IDENTIFICADORES OBJETO ALGORITMO**

Los certificados PKI DE REGISTRO DIGITAL PRISMA se firman utilizando los siguientes algoritmos:

- Sha-1WithRSAEncription OBJECT IDENTIFIER::={iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Las firmas de Certificados producidas utilizando estos algoritmos cumplirán con la RFC 3279. El uso de sha-1WithRSAEncryption será el método de firma de REGISTRO DIGITAL PRISMA.

7.1.3. Formas de Nombres

Los Certificados REGISTRO DIGITAL PRISMA se distribuyen con el nombre requerido conforme a la Sección 3.1.1. Además, los Certificados de Suscriptor usuario final generalmente incluyen un campo adicional de Unidad Persona Jurídica, campo que contiene una notificación que establece que los términos de uso del Certificado se establecen en una URL, y dicha URL será indicadora para EL CONTRATO DE LA PARTE QUE CONFÍA aplicable. Las excepciones al requerimiento anterior se permitirán cuando el espacio, el formato o las limitaciones de inter-operabilidad dentro de los Certificados hagan que esa Unidad organizacional sea imposible de usar junto con la aplicación de los Certificados.

7.1.4. Sintaxis y Semántica de Clasificadores de Política

Todos los Certificados REGISTRO DIGITAL PRISMA X.509 Versión 3 incluyen un clasificador de política dentro de sus extensiones CertificatePolicies. Específicamente dichos Certificados contendrán un clasificador indicador CPS distribuido con una URL indicando el Contrato de Partes confiables aplicable.

7.2. Perfil CRL

Los CRLs se apegan a la RFC 3280 y contienen los campos básicos y contenidos especificados en la Tabla 8 a continuación:

Campo	**Valor o Obligación de Valor**
Versión	Véase la Sección 7.2.1.
Algoritmo de Firma	Algoritmo utilizado para firmar la CRL. Las CRLs de REGISTRO DIGITAL PRISMA se firman utilizando sha1WithRSAEncryption
Emisor	REGISTRO DIGITAL PRISMA , SOCIEDAD ANÓNIMA
Fecha Efectiva.	La fecha de emisión de la CRL. Las CRLs son efectivas al momento de expedición.
Próxima Actualización:	La fecha mediante la cual se expedirá la próxima CRL. La frecuencia de expedición de la CRL es de conformidad con los requerimientos de la Sección 4.4.7.
Certificados Revocados	El listado de los certificados revocados, incluyendo el Número de Serie del Certificado revocado y la Fecha de Revocación.

Tabla – Campos Básicos de Perfil de CRL

7.2.1. Número(s) de Versión

La REGISTRO DIGITAL PRISMA soporta tanto CRLs X.509 Versión 3.

7.3. Perfil OCSP

OSCP (Protocolo de Estado de Certificado En-Línea) es una forma de obtener información oportuna acerca del estado de revocación de un certificado en especial. El OCSP puede utilizarse para validar: o Certificados de Persona Jurídica e individual. Los contestadores OCSP se apegan a la RFC2560.

7.3.1. Número(s) de Versión

Se soporta la Versión 1 de la especificación del OCSP como se define por la RFC2560.

7.3.2. Extensiones OCSP

REGISTRO DIGITAL PRISMA brinda el servicio para validar el estado de revocación de un certificado, mediante el método de OCSP cuando son consumidos desde un ERP, utilizando el protocolo especificado en el RFC2560, utilizando estructuras de sintaxis ASN.1.

8. Auditoría de Cumplimiento y otras evaluaciones

REGISTRO DIGITAL PRISMA pasa por auditorías periódicas de cumplimiento, formalizadas por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, para asegurar la observancia de los Estándares de la PKI de Registro Digital Prisma, después de que comiencen las operaciones. Dichas auditorías, se realizan como mínimo una vez al año.

Además de estas auditorías de cumplimiento, REGISTRO DIGITAL PRISMA tendrá la capacidad de llevar a cabo otras revisiones e investigaciones para asegurarse de la confiabilidad de la PKI de REGISTRO DIGITAL PRISMA, que incluye más no está limitada a:

- Una “Revisión de Seguridad y Prácticas”. Una Revisión de Seguridad y Prácticas consiste de un examen de la instalación segura, documentos de seguridad, CPS, Prácticas de Registro, contratos relacionados con la PKI de REGISTRO DIGITAL PRISMA, políticas de privacidad y planes de validación para asegurar que cumple con los Estándares PKI de REGISTRO DIGITAL PRISMA.
- REGISTRO DIGITAL PRISMA tendrá la capacidad de llevar a cabo “Revisiones Complementarias de Administración de Riesgos” por sí misma o por medio de un tercero después de encontrar Auditorías de Cumplimiento incompletas o descubrimientos excepcionales o como parte del proceso general de administración de riesgos en el curso ordinario de operaciones.

REGISTRO DIGITAL PRISMA tendrá la capacidad de delegar la realización de estas auditorías, revisiones e investigaciones a un tercero. Las personas que estén sujetas a una auditoría, revisión o investigación; proporcionarán cooperación razonable a REGISTRO DIGITAL PRISMA y al personal que lleve a cabo la auditoría, revisión o investigación.

8.1. Frecuencia y Circunstancias de Evaluación

Las Auditorías de Cumplimiento del Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, se llevan a cabo por lo menos anualmente por cuenta y gasto de la entidad auditada.

8.2. Identidad / Habilidades del Evaluador

El Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, designará al auditor o persona idónea que llevará a cabo las Auditorías de Cumplimiento de REGISTRO DIGITAL PRISMA dentro de un período de doce (12) meses.

Las revisiones y las auditorías complementarias, llevadas a cabo por una entidad de auditoría serán realizadas por instituciones con experiencia demostrada en seguridad informática o mediante profesionales en seguridad informática empleados por un consultor competente de seguridad. Dicha entidad también habrá demostrado su experiencia en la realización de auditorías de seguridad IT y de cumplimiento de la PKI.

8.3. Relación del Evaluador con la Entidad Evaluada

Las auditorías y revisiones complementarias llevadas a cabo por entidades de auditoría serán realizadas por entidades independientes de la entidad auditada. Dichas entidades no tendrán un conflicto de intereses que entorpezca su capacidad de llevar a cabo servicios de auditoría.

8.4. Temas Cubiertos por la Evaluación

Los temas de auditoría para cada categoría de la entidad se establecen a continuación. La entidad auditada podrá hacer una Auditoria de Cumplimiento, un módulo que sea parte de una auditoría general anual de los sistemas de información de la entidad.

8.5. Auditoría de Registro Digital Prisma

REGISTRO DIGITAL PRISMA será auditada de conformidad con los requisitos del REGISTRO DE PRESTADORES DE SERVICIOS DE CERTIFICACIÓN del Ministerio de Economía de Guatemala (RPSC), así mismo se programarán auditorías por entes certificadores con lo cual se mantendrán certificaciones como la ISO 9001:2015 e ISO 27001:2013 así como cualquier otra Auditoría externa requerida.

8.6. Acciones tomadas como Resultado de Deficiencia

En el caso de las Auditorías de cumplimiento formalizadas por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía dirigidas a REGISTRO DIGITAL PRISMA, se regirán bajo los requisitos definidos por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía de Guatemala.

REGISTRO DIGITAL PRISMA como AC y/o AR, podrá programar y contratar a terceros para que hagan auditorías de funcionamiento general a sus operaciones. Después de recibir un informe de Auditoría de Cumplimiento, la entidad de auditoría contactará a la parte auditada para discutir cualquier irregularidad, falta de cumplimiento o deficiencia demostrada en el Informe correspondiente de la auditoría de cumplimiento. REGISTRO DIGITAL PRISMA también tendrá la capacidad de discutir dichas irregularidades, falta de cumplimiento o deficiencia con la parte auditada. La entidad auditada, de buena fe, utilizará sus mejores esfuerzos para convenir en un plan de acción correctiva para enmendar los problemas que surjan, las irregularidades o la falta de cumplimiento o deficiencias y los pasos para implementar el plan de acción. En el caso de omisión de la entidad auditada en desarrollar un plan de acciones correctivas o implementarlo, o si el reporte revela irregularidades, faltas de cumplimiento o deficiencias que REGISTRO DIGITAL PRISMA considere que representa una amenaza inmediata a la seguridad o integridad de la PKI de REGISTRO DIGITAL PRISMA, entonces:

(a) Verificará si el reporte de revocación y manipulación es necesario;

(b) Tendrán la capacidad de suspender los servicios a la entidad auditada;

(c) Podrán dar por terminados los servicios sujetos a esta CP y a los términos del contrato de la entidad auditada con su Entidad Superior.

8.7. Comunicaciones de Resultados

Después de cualquier Auditoria de Cumplimiento, la entidad auditada proporcionará a REGISTRO DIGITAL PRISMA el reporte y los informes basados en su auditoría o auto-auditoría dentro de los catorce (14) días después de terminar la auditoría y a más tardar cuarenta y cinco (45) días después de la fecha de aniversario del comienzo de operaciones.

Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, podrá solicitar la información proveniente de las auditorías, y REGISTRO DIGITAL PRISMA, responderá dentro del plazo establecido en el artículo 26 del Reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

9. Otros Negocios y Asuntos Jurídicos

9.1. Tarifas

9.1.1. Expedición de Certificado o Tarifas de Renovación

REGISTRO DIGITAL PRISMA está plenamente facultadas para establecer sus propias tarifas y cobrar por los servicios relacionados con seguridad informática, incluyendo pero no limitando a la expedición, administración y renovación de certificado. Dicho cobro, se formalizará a través de la intervención de un Promotor de Ventas Autorizado, quien establecerá libremente la tarifa a fijar al solicitante suscriptor.

9.1.2. Tarifas de Acceso a Certificado

REGISTRO DIGITAL PRISMA, como AC y AR, no establecerá tarifas ni cobrará los servicios por poner a disposición el repositorio de los certificados. No obstante lo anterior REGISTRO DIGITAL PRISMA se reserva el derecho de cambiar su política y establecer una tarifa así como la suscripción de un contrato para obtener los certificados.

9.1.3. Tarifas de Acceso a Revocación o a la Información de Status

REGISTRO DIGITAL PRISMA no establecerá ni cobrará una tarifa como condición para poner a disposición en el repositorio las CRLs o los servicios OCSP requeridas por esta CP. REGISTRO DIGITAL PRISMA no permitirá el acceso a la información de revocación, información de estatus de Certificado digital o el tiempo de recepción en sus repositorios, a terceros que proporcionen productos o servicios que utilicen

dicha información de estatus de Certificado sin el previo consentimiento por escrito de REGISTRO DIGITAL PRISMA.

9.1.4. Tarifas para Otros Servicios

REGISTRO DIGITAL PRISMA no cobrará una tarifa por acceso a esta CP o a sus respectivos CPS. Cualquier uso hecho con propósitos distintos a los de simplemente ver el documento, tal como la reproducción, redistribución, modificación o creación de trabajos derivados, estarán sujetos a un contrato de licencia con la entidad que tiene los derechos de autor del documento.

9.2. Responsabilidad Civil

9.2.1. Seguro de Responsabilidad Civil

REGISTRO DIGITAL PRISMA cumplirá con lo establecido en la Ley de la República de Guatemala y mantendrá un Seguro de Responsabilidad Civil emitido por una Aseguradora de pleno reconocimiento y respaldo, por la cantidad de doscientos mil dólares de los Estados Unidos de América, exactos (US$200,000.00).

9.2.2. Otros Activos

REGISTRO DIGITAL PRISMA, deberá tener suficientes recursos financieros para mantener sus operaciones y cumplir con sus obligaciones, y ellos razonablemente deberán poder soportar el riesgo de responsabilidad ante los Suscriptores y las partes que confían.

9.3. Confidencialidad de la Información de Negocio

9.3.1. Alcance de la Información Confidencial

Los datos de los suscriptores de conformidad con las disposiciones de la Sección 9.3.2, sí serán conservados como confidenciales y privados (“Información Confidencial/Privada”) en los siguientes casos:

- Registros de solicitud de AC, ya sea aprobados o rechazados, Registros de Solicitud de Certificado,
- Registros de operaciones (tanto registros totales como el registro de auditoría de las operaciones),
- Registros de auditoría a la PKI de REGISTRO DIGITAL PRISMA creados o retenidos por REGISTRO DIGITAL PRISMA o un Cliente,

- Reportes de auditoría de la PKI de REGISTRO DIGITAL PRISMA creados por REGISTRO DIGITAL PRISMA o un Cliente (en la medida que dichos reportes se mantengan), o por sus auditores respectivos (ya sea internos o públicos),
- Planeación de contingencia y planes de recuperación en caso de desastre, y Medidas de seguridad que controlan las operaciones de REGISTRO DIGITAL PRISMA o el equipo y programas de cómputo de las entidades Afiliadas y la administración de servicios de Certificado y servicios designados de registro.

9.3.2. Información no Considerada como "Confidencial"

REGISTRO DIGITAL PRISMA reconoce que los Certificados, la revocación de Certificado y otra información de estatus, el repositorio de REGISTRO DIGITAL PRISMA y la información contenida dentro ellos no es considerada Información Confidencial. La información no expresamente considerada Información Confidencial conforme a la Sección 9.3.1 no será considerada ni confidencial ni privada. Esta sección está sujeta a la Ley aplicable en la República de Guatemala y en lo establecido en el Decreto 57-2008 Ley de acceso a la información pública.

9.4. Privacidad de la Información Personal

9.4.1. Plan de Privacidad

REGISTRO DIGITAL PRISMA establecerá una política de privacidad conforme a la Guía de Requerimientos Legales. Dichas políticas de privacidad se apegarán a las leyes aplicables en la República de Guatemala. Por su parte, REGISTRO DIGITAL PRISMA no divulgará, comercializará, ni venderá los datos personales de los Solicitantes de Certificados u otra información de identificación acerca de ellos, de conformidad con las disposiciones de la Sección 9.3.2.

9.4.2. Información Tratada como Privada

Cualquier información acerca de los Suscriptores que no esté disponible públicamente a través del contenido del certificado expedido, el directorio del certificado y las CRLs en- línea es tratada como privada.

9.4.3. Información no Considerada como Privada

De acuerdo a la ley aplicable toda la información que se hace pública mediante un certificado no es considerada como privada.

9.4.4. Responsabilidad de Proteger la Información Privada

Los Participantes de la PKI DE REGISTRO DIGITAL PRISMA que reciben información privada tomarán las medidas necesarias para asegurarla contra manipulaciones y divulgación a terceros y cumplirán con todas las leyes aplicables a la privacidad de los datos.

9.4.5. Aviso y Consentimiento para Utilizar Información Privada

A menos que se establezca lo contrario en esta CP, en la Política de Privacidad aplicable o mediante acuerdo, la información privada no se utilizará sin el consentimiento de la parte a quien dicha información aplique. Esta sección estará sujeta a la ley aplicable en la República de Guatemala.

9.4.6. Divulgación de Conformidad con los Procesos Judiciales o Administrativos

REGISTRO DIGITAL PRISMA reconoce que tendrá la capacidad de divulgar Información Confidencial/Privada si, de buena fe, REGISTRO DIGITAL PRISMA considera que:

- La divulgación es necesaria en respuesta a una notificación judicial o administrativa legalmente realizada y a las garantías de búsqueda;
- La divulgación es necesaria en respuesta a procesos judiciales, administrativos o legales durante el proceso de averiguación en una acción civil, penal o administrativa, tales como citaciones, interrogatorios, solicitudes de admisión y solicitudes de producción de documentos.

Esta sección está sujeta a la ley aplicable en la República de Guatemala.

9.4.7. Otras Circunstancias de Divulgación de Información

Las políticas de privacidad contendrán las disposiciones relacionadas con la divulgación que una persona realice de información confidencial o privada de REGISTRO DIGITAL PRISMA y esta sección está sujeta a la ley aplicable en la República de Guatemala.

9.5. Derechos de Propiedad Intelectual

9.5.1. Derechos de Propiedad en Información de Certificados y Revocación

REGISTRO DIGITAL PRISMA, retiene todos los Derechos de Propiedad Intelectual que le corresponda, para la emisión y revocación de los certificados que expide. REGISTRO DIGITAL PRISMA, como AC y AR, otorgará permisos para el uso y distribución de los Certificados que emita, en el entendido de los mismos puedan ser reproducidos completamente y que el uso de los Certificados esté sujeto al Contrato de PARTE QUE CONFÍA al que se hace referencia en el Certificado. REGISTRO DIGITAL PRISMA y los suscriptores, otorgarán permiso o licencia para utilizar la información de revocación con el objeto de llevar a cabo las funciones de la PARTE QUE CONFÍA conforme al contrato de uso de CRL aplicable o a cualquier otro contrato.

Los suscritores, así como los solicitantes a suscriptores, serán propietarios de la información y la propiedad intelectual, así como los datos sensibles que les correspondan.

REGISTRO DIGITAL PRISMA, como AC y AR, no mantendrá copia de los datos de creación de firma electrónica, una vez éstos hayan sido entregados a su titular, momento desde el cual éste comenzará a ser responsable de mantenerlos bajo su exclusivo control.

9.5.2. Derechos de Propiedad en la CP

Los Participantes de la PKI de REGISTRO DIGITAL PRISMA reconocen que REGISTRO DIGITAL PRISMA retiene todos los Derechos de Propiedad Intelectual de esta CP.

9.5.3. Derechos de Propiedad en Nombres

Un Solicitante de Certificado retiene todos los derechos que tiene (si hubiere) en cualquier marca, marca de servicio o nombre comercial contenidos en cualquier Solicitud de Certificado y nombre distinguido dentro de cualquier Certificado expedido para dicho Solicitante de Certificado.

9.5.4. Derechos de Propiedad en Claves y Material Clave

El par de claves que corresponden a los Certificados de REGISTRO DIGITAL PRISMA y a los Suscriptores usuario final son propiedad de estos, respectivamente, independientemente del medio físico dentro del cual se almacenan y protegen, y dichas personas retienen todos los Derechos de Propiedad Intelectual en

ese par de claves. Sin detrimento de lo anterior, las claves públicas raíz de REGISTRO DIGITAL PRISMA y los Certificados raíz que las contienen, incluyendo todas las claves públicas y los Certificados auto-firmados, son propiedad de REGISTRO DIGITAL PRISMA.

9.6. Manifestaciones y Garantías

9.6.1. Manifestaciones y Garantías de la AC

REGISTRO DIGITAL PRISMA, como AC manifiesta y garantiza que:

- No hay ninguna alteración de hechos importante en el Certificado conocida por las entidades o que se origine de las entidades que aprueban la Solicitud de Certificado o que expiden el Certificado,
- No existen errores en la información en el Certificado, que hayan sido introducidos por las Autoridades que aprueban la Solicitud de Certificado o que expiden el Certificado como resultado de una omisión en ejercer el cuidado razonable en el manejo de la Solicitud de Certificado o en la creación del Certificado,
- Sus Certificados cumplen con todos los requerimientos de esta CP y la CPS aplicable, y
- Los servicios de revocación y el uso de un repositorio, se apegan a todos los requerimientos de esta CP y la CPS aplicable en todos sus aspectos.

9.6.2. Manifestaciones y Garantías de la AR

REGISTRO DIGITAL PRISMA, como AR, manifiesta y garantiza que:

- No hay ninguna alteración de hechos importantes en el Certificado, o que se origine de la aprobación de la Solicitud de Certificado, o que expiden el Certificado,
- No existen errores en la información en el Certificado que hayan sido introducidos por las entidades que aprueban la Solicitud de Certificado o que expiden el Certificado como resultado de una omisión en ejercer el cuidado razonable en el manejo de la Solicitud de Certificado.
- Sus Certificados cumplen con todos los requerimientos de esta CP y la CPS aplicable,
- Los servicios de revocación (cuando apliquen) y el uso de un depósito se apegan a todos los requerimientos de esta CP y la CPS aplicable en todos sus aspectos.
- Los Contratos de Suscriptor podrán incluir derechos y obligaciones adicionales a los anteriormente establecidos.

9.6.3. Manifestaciones y Garantías del Suscriptor

El Suscriptor garantiza que:

- Cada firma electrónica avanzada creada que utiliza la clave privada que corresponde a la clave pública listada en el Certificado es la firma electrónica avanzada del Suscriptor y que el Certificado ha sido aceptado y que está en operación (no vencido o revocado) en el momento en que se crea la firma electrónica avanzada.
- Su clave privada está protegida y que ninguna persona no autorizada ha tenido nunca acceso a la clave privada del Suscriptor.
- Todas las manifestaciones hechas por el Suscriptor en la Solicitud de Certificado y presentadas por el Suscriptor son verdaderas.
- Toda la información proporcionada por el Suscriptor y contenida en el Certificado es verdadera.
- El Certificado está siendo utilizado exclusivamente para propósitos autorizados y legales, consistentes con todos los requerimientos importantes de esta CP y la CPS aplicable, y
- El Suscriptor es un Suscriptor usuario final y no una AC, y no está utilizando la clave privada que corresponde a ninguna clave pública listada en el Certificado para propósitos de firmar digitalmente ningún Certificado (o cualquier otro formato de clave pública certificada) o CRL, como una AC o en contrario.

Los Contratos de Suscriptor podrán incluir manifestaciones y garantías adicionales.

9.6.4. Manifestaciones y Garantías de la Parte que Confía

Los Contratos de PARTE QUE CONFÍA requieren a la PARTE QUE CONFÍA reconocer que tienen suficiente información para tomar una decisión informada y consciente con respecto a la medida en la cual ellos escogen Confiar en la información de un Certificado, que son los únicos responsables por decidir si Confían o no en dicha información y que ellos soportarán todas las consecuencias legales por su omisión en cumplir con las obligaciones de PARTE QUE CONFÍA en los términos de esta CP, CPS y del contrato correspondiente. Los Contratos de la PARTE QUE CONFÍA podrán incluir derechos y obligaciones adicionales.

9.7. Renuncia de Garantías

En la medida permitida por la ley aplicable, los Contratos de Suscriptor renunciarán a las posibles garantías de REGISTRO DIGITAL PRISMA y a las de las entidades Afiliadas, incluyendo cualquier garantía de comerciabilidad o adecuación a un propósito especial.

9.8. Limitaciones de Responsabilidad

En la medida que la ley lo permita, los derechos y obligaciones comprendidos en los Contratos de Suscriptor limitarán la responsabilidad de REGISTRO DIGITAL PRISMA. Las limitaciones de responsabilidad incluirán una exclusión de daños indirectos, especiales, incidentales y consecuenciales. También incluirán los siguientes topes de responsabilidad que limitan los daños de REGISTRO DIGITAL PRISMA con relación a un Certificado específico:

Clase	**Topes de Responsabilidad**
	Doscientos mil dólares de los Estados Unidos de América (US$200,000.00), conforme al seguro de responsabilidad civil.

Tabla 9 – Topes de Responsabilidad

La responsabilidad civil asegurada, comprenderá la originada en hechos acontecidos durante la vigencia de la póliza de seguro de responsabilidad civil, no obstante sea reclamada con posterioridad a ella. Quedará cubierta la responsabilidad civil por los dependientes, representantes, apoderados y por cualquier persona que participe en la prestación de los servicios de REGISTRO DIGITAL PRISMA. Asimismo, queda cubierta la responsabilidad de toda otra persona por la cual el asegurado sea civilmente responsable en el ejercicio de su actividad como prestador de servicios de certificación.

9.9. Vigencia y Terminación

9.9.1. Vigencia

Las CP entran en vigor al momento de su publicación en el repositorio de REGISTRO DIGITAL PRISMA. Las modificaciones a estas CP son ejercibles al momento de su publicación en el repositorio de REGISTRO DIGITAL PRISMA. Previo a su publicación, la CP debe de ser aprobada por el Registro de Prestadores de Servicios de Certificación del Ministerio de Economía.

9.9.2. Terminación por Modificación

Estas CP según se modifique periódicamente permanecerá vigente hasta que sea reemplazada por una nueva versión.

9.9.3. Efecto de Terminación por Modificación y Sobrevivencia

REGISTRO DIGITAL PRISMA podrá dar por terminadas las presentes CP. Sin embargo, los certificados expedidos durante las CP conservarán su validez y de conformidad con las presentes CP no obstante que las mismas hayan terminado.

9.9.4. Notificaciones Individuales y Comunicaciones con Participantes

A menos que se especifique en contrario mediante acuerdo entre las partes, los participantes de la PKI de REGISTRO DIGITAL PRISMA utilizarán los métodos razonables para comunicarse entre sí, tomando en consideración la importancia y materia objeto de la comunicación.

9.9.5. Procedimiento de Modificación

REGISTRO DIGITAL PRISMA se reserva el derecho de modificar las presentes CP. Las modificaciones a esta CP podrán realizarse mediante el órgano de administración que tenga a su cargo la Política de Certificación de REGISTRO DIGITAL PRISMA. Las modificaciones serán por medio de un documento que contenga un formato modificado de las CP o una actualización. Las versiones modificadas o actualizaciones estarán asociadas con la sección de Actualizaciones de Prácticas y Notificaciones del Repositorio de REGISTRO DIGITAL PRISMA ubicado en: www.prisma.gt/biblioteca. Las actualizaciones reemplazan cualquier disposición designada o en conflicto de la versión referenciada en las CP.

El órgano de Administración de Prácticas y Políticas de REGISTRO DIGITAL PRISMA, determinará si las modificaciones a las CP requieren algún cambio y lo notificarán al órgano correspondiente a la Junta Directiva de REGISTRO DIGITAL PRISMA. En todo caso, la modificación de las CP, así como su publicación, estarán a la previa autorización por parte del Registro de Prestadores de Servicios de Certificación del Ministerio de Economía.

9.9.6. Mecanismo y Período de Notificación

REGISTRO DIGITAL PRISMA se reserva el derecho de modificar las CP sin notificación previo de las correcciones a errores de forma que no son importantes, incluyendo mas no limitadas a correcciones de errores tipográficos, cambios a las URLs, y cambios a la información de contacto. La decisión de REGISTRO DIGITAL PRISMA de designar correcciones como importantes o no importantes será a la sola discreción de REGISTRO DIGITAL PRISMA. Independientemente de cualquier disposición en contrario en estas CP, si REGISTRO DIGITAL PRISMA considera que las modificaciones importantes a la CP son necesarias inmediatamente para detener o evitar una violación a la seguridad de la PKI de REGISTRO DIGITAL PRISMA o de cualquier parte de ella, REGISTRO DIGITAL PRISMA tendrá la capacidad de hacer dichas modificaciones mediante su publicación en su repositorio. Dichas modificaciones serán efectivas inmediatamente en el momento de su publicación.

9.10. Disposiciones de Resolución de Disputas

En la medida que lo permita la Ley aplicable en la República de Guatemala, los Contratos de Suscriptor y los Contratos de PARTE QUE CONFÍA, contendrán una cláusula de solución de controversias.

9.11. Ley Aplicable

Las leyes de Guatemala, establecerán la ejecutabilidad, interpretación y validez de esta CP, independientemente del contrato o de otras disposiciones legales y sin el requerimiento de establecer un nexo comercial en la República de Guatemala.

La disposición de aplicabilidad de la ley de Guatemala se toma para asegurar procesos e interpretación uniforme para todos los Participantes de la PKI de REGISTRO DIGITAL PRISMA, independientemente de donde se localizan. Esta disposición de ley gobernante aplica solamente a éstas CP.

Los contratos que incorporan la CP mediante referencia podrán tener sus propias disposiciones de ley gobernante, en el entendido de que la ejecutabilidad, interpretación y validez de los términos de la CP separados y aparte de las disposiciones remanentes de cualquier otro contrato, sujetas a cualquier limitación que establezca en la ley aplicable, demás regulaciones, ordenanzas, decretos y órdenes incluyendo mas no limitando a restricciones de exportación o importación de programas de cómputo, equipo de cómputo o información técnica.

9.11.1. Separabilidad

En el caso de que un tribunal competente considere que una cláusula o disposición de esta CP no es válida, las cláusulas o disposiciones remanentes de la CP permanecerán válidas.

9.11.2. Causas de Fuerza Mayor

En la medida permitida por la ley aplicable, los Contratos de Suscriptor incluirán una cláusula de previsión para casos de fuerza mayor que puedan afectar de cualquier forma la continuidad de los servicios de certificación prestados por REGISTRO DIGITAL PRISMA.

9.11.3. Los Servidores Gateway incluirán la siguiente Funcionalidad:

Control de acceso a los servicios AC, identificación y autenticación de lanzamiento de servicios AC, re-uso de objeto para la memoria aleatoria de acceso de la AC, uso de criptografía para comunicación de sesión y seguridad de base de datos, archivos de historial de AC y de Suscriptor usuario final y de datos de auditoría, auditoria de seguridad relacionada con eventos, auto-prueba de seguridad relacionada con los servicios AC, y patrón confiable para identificación de puestos de la PKI e identidades asociadas. Las Claves de AC se generan en una Ceremonia de Generación de Clave. Todas las Ceremonias de Generación de Claves se apegan a los requerimientos documentados en las Políticas de Confidencialidad de seguridad de la PKI DE REGISTRO DIGITAL PRISMA.