



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

<b>Título del Documento</b>	Políticas de Certificado para Servicio de Certificados Digitales
<b>Versión</b>	8
<b>Grupo de Trabajo</b>	Comité de Gerencia
<b>Estado del documento</b>	Final
<b>Fecha de emisión</b>	15/02/2010
<b>Fecha de inicio de vigencia</b>	14/08/2020
<b>OID (Object Identifier)</b>	1.3.6.1.4.1.31136.1.4.8
<b>Ubicación de la Política</b>	<a href="https://gse.com.co/documentos/calidad/politicas/Políticas de Certificado para Certificados Digitales.pdf">https://gse.com.co/documentos/calidad/politicas/Políticas de Certificado para Certificados Digitales.pdf</a>
<b>Elaboró</b>	Director de Operaciones
<b>Revisó</b>	Sistema Integrado de Gestión
<b>Aprobó</b>	Comité de Gerencia



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

### Control de Modificaciones

Versión	Fecha	Cambio/Modificación
1	01-11-2016	Documento inicial conforme al desarrollo del plan de acción de la auditoría de ONAC.
2	05-10-2017	Actualización de información referente a la sede de ECD GSE.
3	03-04-2018	Actualización conforme a recomendaciones de la auditoría de ONAC.
4	27-11-2018	Se cambia de V3 a V4 26/11/2018 actualización cargos, tarifas, rutas de acceso a la página web, cambio de título, inclusión de los límites de responsabilidad de la entidad de certificación abierta, vigencia de los servicios, obligaciones de la ECD, de la RA, de la EE, del suscriptor, de los responsables, de los terceros de buena fe, de la entidad y obligaciones de otros participantes
5	12-04-2019	Se eliminó el numeral de las obligaciones de la EE, se unificaron las responsabilidades del suscriptor y responsable, se describe en el numeral de Sistemas Operativos soportados, las especificaciones para uso de MAC, se hizo la aclaración que, para uso de firma centralizada, es necesario la adquisición de una plataforma tecnológica con costos adicionales, y se actualizaron las obligaciones de los suscriptores de acuerdo con el tipo de servicio.
6	07-06-2019	5.10.3 Se aclararon las obligaciones y derechos del suscriptor
7	31/03/2020	Se ajusta la PC's a los cambios generados por las nuevas plataformas, Se agregan los numerales de Objetivo y Alcance y administración de las políticas, Se ajusta la lista de precios, se modifican los links para que apunten a las nuevas rutas y se actualiza la versión de los estándares de los ETSY y los ITU- 509.
8	14/08/2020	Se actualizó la persona de contacto en el numeral 4.1. Se agregó una nota al numeral 7.5, en caso de que el suscriptor cuente con un certificado vigente podrá radicar la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos solicitados inicialmente. Para el certificado tipo función pública, en caso de no contar con el certificado laboral, se puede adjuntar el acta de posesión, acta de nombramiento o contrato de prestación de servicios. Para el certificado tipo profesional titulado, el RUT se solicita (si aplica), se cambia la solicitud de matrícula profesional por el diploma y que el acta de grado debe ser autenticada.



# POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

## TABLA DE CONTENIDO

<b>1. OBJETIVO</b> .....	<b>5</b>
<b>2. ALCANCE</b> .....	<b>5</b>
<b>3. INTRODUCCIÓN</b> .....	<b>5</b>
3.1. Resumen .....	5
3.2. Definiciones y acrónimos .....	6
3.2.1 Definiciones .....	6
3.2.2 Acrónimos.....	7
<b>4. ADMINISTRACION DE POLITICAS</b> .....	<b>8</b>
4.1 Persona de contacto: .....	8
4.2 Procedimiento de aprobación de las Políticas .....	8
4.3 Responsabilidades de publicación.....	8
4.4 Peticiones, Quejas, Reclamos, Solicitudes y Apelaciones.....	8
<b>5. IDENTIFICACIÓN DE POLÍTICAS</b> .....	<b>9</b>
5.1. Criterio de Identificación de las Políticas (OID).....	9
5.2. El contenido de los certificados, distinguiendo:.....	9
5.3. OID de las Políticas .....	10
5.4. Políticas asignadas a este documento.....	10
<b>7. REQUERIMIENTOS DE LOS CERTIFICADOS DIGITALES DE LA ECD GSE</b> .....	<b>11</b>
7.2. Requerimientos específicos .....	12
7.3. Requerimiento específico: PKI participantes .....	12
7.4. Requerimiento específico: Uso de certificado.....	13
Límites de Responsabilidad de la Entidad de Certificación Abierta .....	14
7.5 Requerimiento específico tramitación del certificado .....	15
7.6 Actividades y referencias técnicas de los certificados.....	18
7.7 Características de los dispositivos criptográficos.....	20
7.7.1 Certificado Digital en Token .....	20
7.7.2 Certificado Digital en HSM – Hardware Security Module (FirmaCentralizada) .....	21
Algoritmo de Firma .....	21
Contenido del Certificado Digital .....	21
Ciclo de vida de los certificados .....	22
Generación de claves.....	22
Actividades de certificación artículo 161 del decreto ley 0019 de 2012 .....	22
7.8 Obligaciones .....	22



# POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

7.8.1	Obligaciones de la ECD GSE .....	22
7.8.2	Obligaciones de la RA .....	23
7.8.3	Obligaciones y derechos del suscriptor y/o responsable.....	23
7.8.4	Obligaciones de la Entidad (Cliente) .....	24
7.8.5	Obligaciones de otros participantes.....	25
<b>7.9</b>	<b>Tarifas del servicio de emisión de certificados digitales.....</b>	<b>26</b>
7.9.1	Tarifas de emisión o renovación de certificados.....	26
7.9.2	Modelos y minutas de los documentos de términos y condiciones .....	27
<b>7.10</b>	<b>Perfil de los certificados .....</b>	<b>27</b>

## 1. OBJETIVO

El objeto de la PC es definir aquellos requerimientos que son necesarios para la emisión de los distintos certificados ECD GSE.

En la medida en que en la DPC de la ECD GSE se establece todos los requerimientos genéricos acerca de sistema de seguridad, soporte, administración y emisión de los Certificados ECD GSE, las políticas harán referencia únicamente los requerimientos específicos de cada tipo de certificado remitiéndose en el resto de los términos a lo establecido en la DPC.

En caso de discrepancia entre los términos de las PC y de la DPC, se considerará que lo establecido en esta PC tiene prelación con respecto a cualquier otra condición contradictoria establecida en la DPC.

## 2. ALCANCE

Este documento aplica para emitir certificados en relación con las firmas electrónicas o digitales de personas Naturales o jurídicas, emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999

## 3. INTRODUCCIÓN

El presente documento especifica las Políticas de Certificado para Certificados Digitales (en adelante PC) para los diferentes certificados emitidos por la ECD GSE.

De esta forma, los distintos certificados de la ECD GSE, deberán ajustarse a los requerimientos genéricos y niveles de seguridad que se detallan en la DPC y a los requerimientos específicos para cada uno definidos en este documento.

ECD GSE deberá informar a los Suscriptores y/o Responsables de la existencia de este documento donde se da respuesta a las PC de los distintos certificados emitidos por ECD GSE.

### 3.1. Resumen

**Política para Certificado de Certificados Digitales**, en adelante **Política** es un documento elaborado por **Gestión de Seguridad Electrónica S.A. (en adelante GSE)** que, actuando como una Entidad de Certificación Digital, contiene las normas, procedimientos que la **Entidad de Certificación Digital (en adelante GSE)** como **Prestador de Servicios de Certificación digital (PSC)** aplica como lineamiento para prestar el Servicio de acuerdo a lo establecido en la Ley 527 de 1999, el Decreto Ley 0019 de 2012, el Decreto 333 de 2014, el Decreto 1471 de 2014 y los reglamentos que los modifiquen o complementen, en el territorio de Colombia.

## 3.2. Definiciones y acrónimos

### 3.2.1 Definiciones

Los siguientes términos son de uso común y requerido para el entendimiento de la presente Política.

**Entidad de Certificación Digital:** Es aquella persona jurídica, acreditada conforme a la ley 527 de 1999 y el Decreto 333 de 2014, facultada por el gobierno Colombiano (Organismo Nacional de Acreditación en Colombia) para emitir certificados en relación con las firmas digitales de los clientes que las adquieran, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

**Entidad de Certificación Abierta:** Es aquella que ofrece servicios propios de las entidades de certificación, tales que:

- a) Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o
- b) Recibe remuneración por éstos.

**Prestador de Servicios de Certificación (PSC):** En inglés “Certification Service Provider” (CSP), persona natural o jurídica que expide certificados digitales y presta otros servicios en relación con las firmas digitales.

**Autoridad de Certificación (CA):** En inglés “Certification Authority” (CA), Autoridad de Certificación, entidad raíz y entidad prestadora de servicios de certificación de infraestructura de llave pública.

**Autoridad de Registro (RA):** En inglés “Registration Authority” (RA), es la entidad encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

**Declaración de Prácticas de Certificación (DPC):** En inglés “Certification Practice Statement” (CPS), manifestación de la entidad de certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.

**Política de Certificación (PC).** Es un conjunto de reglas que definen las características de los distintos tipos de certificados y su uso.

**Certificado digital:** Mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la llave pública de éste último.

**Estampado cronológico:** Mensaje de datos que vincula a otro mensaje de datos con un momento o periodo de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento o periodo de tiempo y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado.

**Autoridad de sellado de tiempo (TSA):** Sigla en inglés de “Time Stamp Authority”, entidad de confianza que emite sellos de tiempo.

**Solicitante:** Toda persona natural o jurídica que solicita un servicio de certificación o la expedición o renovación de un certificado digital.

**Suscriptor y/o responsable:** Persona natural o jurídica a la cual se emiten o activan los servicios de certificación digital y por tanto actúa como suscriptor o responsable del mismo.

**Tercero de buena fe:** Persona o entidad diferente del titular que decide aceptar y confiar en un servicio prestado por GSE.

**Clave Personal de Acceso (PIN):** Sigla en inglés de “Personal Identification Number”, secuencia de caracteres que permiten el acceso al certificado digital.

**Repositorio:** Sistema de información utilizado para almacenar y recuperar certificados y otra información relacionada con los mismos.

**Módulo Criptográfico Hardware de Seguridad:** Sigla en inglés de “Hardware Security Module”, módulo hardware utilizado para realizar funciones criptográficas y almacenar llaves en modo seguro.

**Servicio del estado del certificado en línea:** Sigla en inglés “Online Certificate Status Protocol” (OCSP), actividad de consulta en tiempo real al sistema de la ECD, sobre el estado de un certificado digital a través del protocolo OCSP.

**CA de GSE:** Es la Autoridad de Certificación de GSE, entidad prestadora de servicios de certificación digital.

**RA de GSE:** Es la Autoridad de Registro de GSE, entidad prestadora del servicio de registro de la Autoridad de Certificación CA GSE en el proceso de solicitud e identificación de los solicitantes de un certificado digital.

### 3.2.2 Acrónimos

**CA:** Certification Authority

**CPS:** Certification Practice Statement

**CRL:** Certificate Revocation List

**CSP:** Certification Service Provider

**DNS:** Domain Name System

**FIPS:** Federal Information Processing Standard

**HTTP:** El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

**HTTPS:** Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por su acrónimo HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

**IEC:** International Electrotechnical Commission

**IETF:** Internet Engineering Task Force (Organismo de estandarización de Internet)

**IP:** Internet Protocol

**ISO:** International Organization for Standardization

**OCSP:** Online Certificate Status Protocol.

**OID:** Object identifier (Identificador de objeto único)

**PIN:** Personal Identification Number

**PUK:** Personal Unlocking Key

**PKCS:** Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.

**PKI:** Public Key Infrastructure (Infraestructura de Llave Pública)

**PKIX:** Public Key Infrastructure (X.509)

**RA:** Registration Authority

**RFC:** Request For Comments (Estándar emitido por la IETF)

**URL:** Uniform Resource Locator

### 4. ADMINISTRACION DE POLITICAS

La administración de las Políticas de Certificación (PC) estarán a cargo del proceso de Operaciones:

#### 4.1 Persona de contacto:

**Nombre de contacto:** Víctor Armando Ibañez Palacios

**Cargo del contacto:** Director de Operaciones

**Teléfonos de contacto:** 4050082 - 3232085095

**Correo electrónico:** [victor.ibanez@gse.com.co](mailto:victor.ibanez@gse.com.co)  
[info@gse.com.co](mailto:info@gse.com.co)

#### 4.2 Procedimiento de aprobación de las Políticas

Las políticas deben ser aprobadas en todos los casos por el Comité de Gerencia.

#### 4.3 Responsabilidades de publicación

Una vez realizado y aprobados los cambios de las políticas, es responsabilidad del Director de Operaciones y/o el Proceso del Sistema Integrado de Gestión solicitar al proceso encargado la actualización en los portales WEB de las políticas en su última versión.

#### 4.4 Peticiones, Quejas, Reclamos, Solicitudes y Apelaciones

Las peticiones, quejas, reclamos, solicitudes y apelaciones sobre los servicios prestados por ECD GSE o entidades subcontratadas, explicaciones sobre esta Política de



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

Certificación; son recibidas y atendidas directamente por GSE como ECD y serán resueltas por las personas pertinentes e imparciales o por los comités que tengan la competencia técnica necesaria, para lo cual se disponen de los siguientes canales para la atención a suscriptores, responsables y terceros.

**Teléfono:** +57 (1) 4050082  
**Correo electrónico:** [pqrs@gse.com.co](mailto:pqrs@gse.com.co)  
**Dirección:** Calle 73 No. 7 – 31 Piso 3 Torre B  
**Página Web:** [www.gse.com.co](http://www.gse.com.co)  
**Responsable:** Sistema Integrado de Gestión

Una vez presentado el caso, este es transmitido con la información concerniente al proceso del Sistema Integrado de Gestión según procedimiento interno establecido para la investigación y gestión de estas. Del mismo modo, se determina qué área es responsable de tomar acciones correctivas o preventivas, caso en el cual se debe aplicar el procedimiento de acciones.

Generada la investigación se procede a evaluar la respuesta para posteriormente tomar la decisión que resuelve la PQRSA y su comunicación final al suscriptor, responsable o parte interesada.

### 5. IDENTIFICACIÓN DE POLÍTICAS

#### 5.1. Criterio de Identificación de las Políticas (OID)

La forma de identificar los distintos tipos de certificados digitales de ECD GSE es a través de identificadores de objeto (OID's). Un OID concreto permite a las aplicaciones distinguir claramente el certificado que se presenta.

El identificador de la PC está compuesto por una serie de números separados entre sí por puntos y con un significado concreto de cada uno de ellos.

Partiendo del OID, se distingue el certificado genérico ECD GSE, y su vez, partiendo de este certificado de ECD GSE se definen diferentes subtipos en función a algunas características específicas, como son:

#### 5.2. El contenido de los certificados, distinguiendo:

Si son certificados de firma que, a su vez, se clasifican en otros subtipos dependiendo de si contienen o no atributo.

El atributo constituye la característica específica de la persona natural titular del certificado digital que aparece contenida en el certificado y que puede ser de distintos tipos:

- de Pertenencia a Empresa
- de Representación Empresa



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

- de Función Pública
- de Profesional Titulado
- de Persona Natural
- de Firma Centralizada
- de Persona Jurídica
- de Factura Electrónica

Quien genere las claves del certificado digital, distinguiendo entre la persona titular del certificado o la propia ECD GSE.

### 5.3. OID de las Políticas

El siguiente cuadro muestra los diferentes certificados emitidos por la ECD GSE, y los OID de sus correspondiente PC, en función de las distintas variables definidas en el anterior apartado:

OID	DESCRIPCIÓN
1.3.6.1.4.1.31136.1.4.8	Política de Certificados de certificado para certificados digitales

### 5.4. Políticas asignadas a este documento.

Este documento en concreto da respuesta a las PC de los siguientes certificados y de sus diferentes subtipos:

- GSE-PE
- GSE-RE
- GSE-FP
- GSE-PT
- GSE-PN
- GSE-FC
- GSE-PJ
- GSE-FE

## 6. TIPOS DE CERTIFICADOS ECD GSE

Los distintos tipos de certificados emitidos por ECD GSE se clasifican atendiendo al criterio de "contenido" y de los campos definidos en los mismos y establecidos en los perfiles técnicos definidos en el Anexo 1 de la DPC.

En virtud de este criterio se garantiza una u otra información que constituye el objeto del certificado.

Así pues, los certificados digitales definidos bajo esta política son los siguientes:



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

TIPO DE CERTIFICADO	OBJETO
<b>Certificado de Pertenencia a Empresa</b>	Garantiza la identidad de la persona natural titular del certificado, así como su vinculación a una determinada entidad jurídica en virtud del cargo que ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual.
<b>Certificado de Representación Empresa</b>	Es emitido a favor de una persona natural representante de una determinada entidad jurídica. El titular del certificado se identifica no únicamente como persona física perteneciente a una empresa, sino que añade su cualificación como representante legal de la misma.
<b>Certificados de Función Pública</b>	Garantiza la identidad de la persona natural titular del certificado, así como su vinculación a una Administración Pública en virtud del rango como funcionario público. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual.
<b>Certificados de Profesional Titulado</b>	Garantiza la identidad de la persona natural titular del certificado, así como su condición de profesional titulado. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual en el ámbito de su profesión.
<b>Certificados de Persona Natural</b>	Garantiza únicamente la identidad de la Persona natural.
<b>Certificados de Factura Electrónica para persona natural</b>	Garantiza únicamente la identidad de la Persona natural.
<b>Certificados de Factura Electrónica para persona jurídica</b>	Certificado exclusivo para facturación electrónica atendiendo a la necesidad de las empresas que buscan la seguridad del certificado para la emisión de facturas electrónicas.
<b>Certificado de Persona Jurídica</b>	Realización de trámites empresariales por parte de una aplicación ejecutándose en una máquina en procesos de firma automáticos y desatendidos en nombre de una persona Jurídica de derecho público o privado que requieran garantizar la autenticidad y la integridad de los datos enviados o almacenados digitalmente junto con en el establecimiento de canales de comunicación seguros entre clientes, y que será representada por medio de una persona física (Responsable), poseedor del certificado emitido bajo esta política y denominado Responsable.
<b>Certificados Firma Centralizada</b>	Certificados de firma digital de cualquiera de los perfiles antes mencionados. Este tipo de certificados son entregados en HSM de modo que con un usuario, contraseña y PIN se pueda firmar digitalmente sin la necesidad de un token físico. Para poder usar este tipo de certificados, es necesario la adquisición de una plataforma tecnológica con costos adicionales.

### 7. REQUERIMIENTOS DE LOS CERTIFICADOS DIGITALES DE LA ECD GSE

ECD GSE no impide o inhibe el acceso de los solicitantes a los servicios como ECD, por lo anterior un certificado digital puede ser solicitado sin importar el tamaño del solicitante o suscriptor, el tipo de vinculación existente con ECD GSE, ni de la membresía con cualquier

asociación o grupo, tampoco depende del número de certificados digitales ya emitidas o cualquier otra que discrimine el acceso a la solicitud del servicio prestado por ECD GSE.

### 7.1. Requerimientos genéricos

El conjunto de información detallada en la DPC sobre su sistema de seguridad, soporte, administración y emisión de los Certificados, además sobre la relación de confianza entre el Suscriptor o Responsable, el Solicitante, la Entidad que recibe o Tercero de buena fe y la ECD constituye los requerimientos genéricos para la emisión de los certificados ECD GSE.

No obstante, en virtud de las características específicas de los distintos certificados estos requerimientos tienen en algunas ocasiones particularidades propias para cada tipo de certificado digital. Estas particularidades se definen como requerimientos específicos y se definen en el siguiente apartado.

### 7.2. Requerimientos específicos

Dependiendo del objeto de los distintos certificados, se dan requerimientos específicos relativos a los siguientes aspectos:

PKI participantes (Ver PKI participantes): Dependiendo de los distintos certificados variara el Suscriptor, Responsable, la Entidad y la vinculación (atributo) entre estas dos figuras.

Usos del Certificado (Ver Usos del Certificado): Dependiendo de los distintos certificados variara el uso ó ámbito de aplicación.

Tramitación del Certificado (Ver Tramitación del Certificado): Dependiendo de los distintos certificados varía la documentación acreditativa del contenido de los mismos.

### 7.3. Requerimiento específico: PKI participantes

Partiendo de las definiciones genéricas establecidas en la DPC relativas a las figuras de Suscriptor y/o Responsable y Entidad, se establece a continuación el detalle de las personas naturales o jurídicas que desempeñan estas funciones por cada tipo de certificado, así como el atributo o vinculación entre estas dos figuras que delimitan los requisitos, revisión y decisión conforme con el alcance de acreditación otorgado por ONAC.

TIPO DE CERTIFICADO	SUSCRIPTOR / RESPONSABLE	ATRIBUTO	ENTIDAD
<b>Certificado de Pertenencia a Empresa</b>	Persona natural que pertenece a la empresa y que es titular del certificado	Vinculación de pertenencia a empresa	Empresa a la que está vinculada el Suscriptor
<b>Certificado de Representación Empresa</b>	Persona natural que representa legalmente a la empresa y que es titular del certificado	Vinculación de representación legal a empresa	Empresa a la que representa el Suscriptor

<b>Certificados de Función Pública</b>	Persona natural que pertenece a una Administración Pública y que es titular del certificado	Vinculación funcional respecto a una Administración Pública	Administración Pública a la que está vinculada el Suscriptor
<b>Certificados de Profesional Titulado</b>	Persona natural que ejerce una profesión titulada y que es titular del certificado	Ejercicio de una profesión colegiada y vinculación con el Colegio Profesional	Colegio Profesional al que está vinculada el Suscriptor
<b>Certificados de Persona Natural</b>	Persona natural titular del certificado	No aplica	No aplica
<b>Certificados de Factura Electrónica persona natural</b>	Garantiza únicamente la identidad de la Persona natural.	Vinculación para la realización de la facturación electrónica de la empresa	Suscriptor que requiere realizar facturación electrónica
<b>Certificados de Factura Electrónica persona Jurídica</b>	Responsable del certificado que obra en nombre de una Persona Jurídica	Vinculación para la realización de la facturación electrónica de la empresa	Empresa que autoriza al Suscriptor para realizar la facturación electrónica de la empresa
<b>Certificado de Persona Jurídica</b>	Responsable del certificado que obra en nombre de una Persona Jurídica	Vinculación de representación legal a empresa	Empresa a la que representa el Suscriptor
<b>Certificados de Firma Centralizada</b>	Persona natural o jurídica que puede pertenecer a una empresa y se encuentra autorizada por la misma para firma centralizada y que es titular del certificado	Vinculación para la realización de la facturación electrónica de la empresa	Empresa que autoriza al Suscriptor para realizar procesos de firma digital

#### 7.4. Requerimiento específico: Uso de certificado

Partiendo de las definiciones genéricas establecidas en la DPC relativas a los usos del certificado se establecen a continuación el ámbito de aplicación de cada tipo de certificado con objeto de delimitar responsabilidades, compromisos o derechos por parte del Suscriptor o Responsable, y en su caso, también por parte de la Entidad en la medida en que se deduzca por la propia naturaleza del atributo del certificado.

TIPO DE CERTIFICADO	AMBITO USOS Y APLICACIONES
<b>Certificado de Pertenencia a Empresa</b>	Realización de trámites empresariales por parte del Firmante/Suscriptor sin que implique representación. La empresa puede establecer limitaciones de uso.



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

TIPO DE CERTIFICADO	AMBITO USOS Y APLICACIONES
<b>Certificado de Representación Empresa</b>	Realización de trámites empresariales por parte del Firmante/Suscriptor en nombre y representación de la empresa. La empresa puede establecer limitación de uso.
<b>Certificados de Función Pública</b>	Realización de trámites por parte del Suscriptor en el ejercicio de sus funciones como funcionario público. La Administración Pública puede establecer limitaciones de uso.
<b>Certificados de Profesional Titulado</b>	Realización de trámites por parte del Suscriptor en el ejercicio de sus funciones como profesional colegiado.
<b>Certificados de Persona Natural</b>	Realización de trámites por parte del Suscriptor en su calidad de ciudadano. No existe vinculación alguna con ninguna entidad.
<b>Certificados de Factura Electrónica persona natural</b>	Realización por parte del responsable de la facturación electrónica en nombre propio
<b>Certificados de Factura Electrónica persona jurídica</b>	Realización por parte del responsable de la facturación electrónica en nombre de empresa.
<b>Certificado de Persona Jurídica</b>	Realización de trámites empresariales por parte de una aplicación ejecutándose en una máquina en procesos de firma automáticos y desatendidos en nombre de una persona Jurídica de derecho público o privado que requieran garantizar la autenticidad y la integridad de los datos enviados o almacenados digitalmente junto con en el establecimiento de canales de comunicación seguros entre clientes, y que será representada por medio de una persona física (Suscriptor), poseedor del certificado emitido bajo esta política y denominado responsable.
<b>Certificados de Firma Centralizada.</b>	Realización de procesos de firma centralizada a través de la gestión unificada de los certificados digitales utilizados, con el objetivo de operar desde un único repositorio, controlado y seguro. Para poder hacer uso de los certificados centralizados, es necesario que se adquiriera una plataforma con costos adicionales.

### Límites de Responsabilidad de la Entidad de Certificación Abierta

Las limitaciones de Responsabilidad de la Entidad de Certificación Abierta están definidas de manera integral en la numeral exoneración de responsabilidad de la DPC, pero partiendo de los usos específicos de cada uno de los certificados establecidos en el numeral anterior. ECD GSE no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros de confianza a excepción de lo establecido por las disposiciones de la presente DPC.

La ECD GSE declinará una solicitud de un servicio de certificación digital, si el mismo no se encuentra en el alcance de la acreditación que le fue otorgado por ONAC.

TIPO DE CERTIFICADO	LÍMITE DE RESPONSABILIDAD DE LA ENTIDAD DE CERTIFICACIÓN
<b>Certificado de Pertenencia a Empresa</b>	Los certificados digitales emitidos por ECD GSE sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en la DPC y específicamente en el numeral Uso de certificado. Se consideran indebidos aquellos usos que no están definidos en la DPC
<b>Certificado de Representación Empresa</b>	



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

TIPO DE CERTIFICADO	LÍMITE DE RESPONSABILIDAD DE LA ENTIDAD DE CERTIFICACIÓN
<b>Certificados de Función Pública</b>	y en las PC y en consecuencia para efectos legales, la ECD GSE queda eximida de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de certificados digitales según la DPC, las PC y de conformidad con lo establecido en el numeral Exoneración de responsabilidad de la entidad de certificación abierta.
<b>Certificados de Profesional Titulado</b>	
<b>Certificados de Persona Natural</b>	
<b>Certificados de Factura Electrónica persona natural</b>	
<b>Certificados de Factura Electrónica persona jurídica</b>	
<b>Certificados de Persona Jurídica</b>	
<b>Certificados Digitales Para Firma Centralizada</b>	

### 7.5 Requerimiento específico tramitación del certificado

Partiendo de las definiciones genéricas establecidas en la DPC relativas a la tramitación del certificado, se establece a continuación la documentación y normativa acreditativa necesaria para la autenticación de los datos contenidos de cada certificado.

- Ley 527 de 1999, CAPITULO III Certificados.
- Ley 527 de 1999, CAPITULO IV Suscriptores de firmas digitales, ARTÍCULO 39. Deberes de los suscriptores.

TIPO DE CERTIFICADO	REGISTRO: DOCUMENTACIÓN ACREDITATIVA
<b>Certificado de Pertenencia Empresa</b>	<ul style="list-style-type: none"> <li>• Formulario On- line diligenciado de solicitud del certificado</li> <li>• Aceptación de términos y condiciones</li> <li>• Fotocopia de documento de identidad del suscriptor</li> <li>• Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a 30 días</li> <li>• Registro Único Tributario – RUT</li> <li>• Certificado laboral del solicitante incluyendo el cargo en papel institucional (no mayor a treinta (30) días)</li> </ul> <p>Nota: En el caso que el usuario suscriptor cuente con un certificado vigente (de acuerdo con el numeral 5.2.2 y 5.2.3 de la DPC), radicará la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos anteriormente mencionados.</p>
<b>Certificado de Representación Empresa</b>	<ul style="list-style-type: none"> <li>• Formulario On- line diligenciado de solicitud del certificado</li> <li>• Aceptación de términos y condiciones</li> <li>• Fotocopia de documento de identidad del suscriptor</li> <li>• Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a 30 días</li> <li>• Registro Único Tributario – RUT</li> </ul>

TIPO DE CERTIFICADO	REGISTRO: DOCUMENTACIÓN ACREDITATIVA
	<p>Nota: En el caso que el usuario suscriptor cuente con un certificado vigente (de acuerdo con el numeral 5.2.2 y 5.2.3 de la DPC), radicará la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos anteriormente mencionados.</p>
<b>Certificados de Función Pública</b>	<ul style="list-style-type: none"> <li>Formulario On- line diligenciado de solicitud del certificado</li> <li>Aceptación de términos y condiciones</li> <li>Fotocopia de documento de identidad del Suscriptor</li> <li>Registro Único Tributario – RUT</li> <li>Acta de posesión, acta de nombramiento o contrato de prestación de servicios del solicitante y/o Certificado laboral del solicitante incluyendo el cargo en papel institucional (no mayor a treinta (30) días).</li> </ul> <p>Nota: En el caso que el usuario suscriptor cuente con un certificado vigente (de acuerdo con el numeral 5.2.2 y 5.2.3 de la DPC), radicará la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos anteriormente mencionados.</p>
<b>Certificados de Profesional Titulado</b>	<ul style="list-style-type: none"> <li>Formulario On- line diligenciado de solicitud del certificado</li> <li>Aceptación de términos y condiciones</li> <li>Fotocopia de documento de identidad del suscriptor</li> <li>Registro Único Tributario – RUT (Si aplica)</li> <li>Fotocopia de la Tarjeta Profesional, diploma y/o acta de grado.</li> </ul> <p>Nota: En el caso que el usuario suscriptor cuente con un certificado vigente (de acuerdo con el numeral 5.2.2 y 5.2.3 de la DPC), radicará la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos anteriormente mencionados.</p>
<b>Certificados de Persona Natural</b>	<ul style="list-style-type: none"> <li>Formulario On- line diligenciado de solicitud del certificado</li> <li>Aceptación de términos y condiciones</li> <li>Fotocopia de documento de identidad del suscriptor</li> <li>Registro Único Tributario – RUT (si aplican)</li> </ul> <p>Nota: En el caso que el usuario suscriptor cuente con un certificado vigente (de acuerdo con el numeral 5.2.2 y 5.2.3 de la DPC), radicará la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos anteriormente mencionados.</p>
<b>Certificados de Factura Electrónica persona natural</b>	<ul style="list-style-type: none"> <li>Formulario On- line diligenciado de solicitud del certificado</li> <li>Aceptación de términos y condiciones</li> <li>Fotocopia de documento de identidad del suscriptor</li> <li>Registro Único Tributario – RUT (Si aplican)</li> </ul> <p>Para el caso que el proceso de facturación se realice por un tercero:</p> <ul style="list-style-type: none"> <li>Constancia delegación del proceso al tercero en papel institucional.</li> </ul> <p>Nota: En el caso que el usuario suscriptor cuente con un certificado vigente (de acuerdo con el numeral 5.2.2 y 5.2.3 de la DPC), radicará la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos anteriormente mencionados.</p>



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

TIPO DE CERTIFICADO	REGISTRO: DOCUMENTACIÓN ACREDITATIVA
<b>Certificados de Factura Electrónica persona jurídica</b>	<ul style="list-style-type: none"><li>Formulario On- line diligenciado de solicitud del certificado</li><li>Aceptación de términos y condiciones</li><li>Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a 30 días</li><li>Fotocopia de documento de identidad del suscriptor (representante legal)</li><li>Registro Único Tributario – RUT.</li><li>Certificado laboral del solicitante incluyendo el cargo en papel institucional (no mayor a treinta (30) días).</li></ul> <p>Para el caso que el proceso de facturación se realice por un tercero:</p> <ul style="list-style-type: none"><li>Constancia delegación del proceso al tercero en papel institucional.</li></ul> <p>Nota: En el caso que el usuario suscriptor cuente con un certificado vigente (de acuerdo con el numeral 5.2.2 y 5.2.3 de la DPC), radicará la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos anteriormente mencionados.</p>
<b>Certificados de Persona Jurídica</b>	<ul style="list-style-type: none"><li>Formulario On- line diligenciado de solicitud del certificado</li><li>Aceptación de términos y condiciones</li><li>Fotocopia del documento de identidad del suscriptor</li><li>Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a 30 días</li><li>Certificado laboral del solicitante incluyendo el cargo en papel institucional (no mayor a treinta (30) días).</li><li>Registro Único Tributario – RUT.</li></ul> <p>Nota: En el caso que el usuario suscriptor cuente con un certificado vigente (de acuerdo con el numeral 5.2.2 y 5.2.3 de la DPC), radicará la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos anteriormente mencionados.</p>
<b>Certificados Digitales Para Firma Centralizada</b>	<ul style="list-style-type: none"><li>Aplican todos los documentos descritos en los certificados anteriores.</li></ul> <p>Nota: En el caso que el usuario suscriptor cuente con un certificado vigente (de acuerdo con el numeral 5.2.2 y 5.2.3 de la DPC), radicará la solicitud firmada digitalmente y dicha solicitud reemplazará los documentos anteriormente mencionados.</p>

Requerimiento específico: Vigencia de los certificados

**Los certificados emitidos por ECD GSE tienen una vigencia máxima de dos (2) años.**



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

### 7.6 Actividades y referencias técnicas de los certificados

SERVICIOS DE CERTIFICACION DIGITAL	ACTIVIDADES DE CERTIFICACIÓN Artículo 161 del Decreto Ley 0019 de 2012	DOCUMENTOS NORMATIVOS O TÉCNICOS Anexos CEA-4.1-10
<p style="text-align: center;"><b>CERTIFICADOS DIGITALES PARA PERTENENCIA EMPRESA</b></p> <p>Garantiza la identidad de la persona natural titular del certificado, así como su vinculación a una determinada entidad jurídica en virtud del cargo que ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual.</p>	<p>Emisión de certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.</p> <p>Emisión de certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.</p> <p>Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.</p>	<p style="text-align: center;">RSA 2048 RSA 4096</p> <p>SHA-256 Tamaño de clave mínimo 2048 bits agosto 2002 RFC 5280 mayo 2008 ITU-T-X509 octubre 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 noviembre 2003 FIPS 140-2 Nivel 3 mayo 2001</p>
<p style="text-align: center;"><b>CERTIFICADOS DIGITALES PARA REPRESENTACION EMPRESA</b></p> <p>Es emitido a favor de una persona natural representante de una determinada entidad jurídica. El titular del certificado se identifica no únicamente como persona física perteneciente a una empresa, sino que añade su cualificación como representante legal de la misma.</p>	<p>Emisión de certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.</p> <p>Emisión de certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.</p> <p>Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.</p>	<p style="text-align: center;">RSA 2048 RSA 4096</p> <p>SHA-256 Tamaño de clave mínimo 2048 bits agosto 2002 RFC 5280 mayo 2008 ITU-T-X509 octubre 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 noviembre 2003 FIPS 140-2 Nivel 3 mayo 2001</p>
<p style="text-align: center;"><b>CERTIFICADOS DIGITALES DE FUNCION PUBLICA</b></p> <p>Garantiza la identidad de la persona natural titular del certificado, así como su vinculación a una Administración Pública en virtud del rango como funcionario público. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual.</p>	<p>Emisión de certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.</p> <p>Emisión de certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.</p> <p>Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.</p>	<p style="text-align: center;">RSA 2048 RSA 4096</p> <p>SHA-256 Tamaño de clave mínimo 2048 bits agosto 2002 RFC 5280 mayo 2008 ITU-T-X509 octubre 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 noviembre 2003 FIPS 140-2 Nivel 3 mayo 2001</p>
<p style="text-align: center;"><b>CERTIFICADOS DIGITALES DE PROFESIONAL TITULADO</b></p> <p>Garantiza la identidad de la persona natural titular del certificado, así como su condición de profesional titulado. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que</p>	<p>Emisión de certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.</p> <p>Emisión de certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.</p>	<p style="text-align: center;">RSA 2048 RSA 4096</p> <p>SHA-256 Tamaño de clave mínimo 2048 bits agosto 2002 RFC 5280 mayo 2008 ITU-T-X509 octubre 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 noviembre 2003</p>



# POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

SERVICIOS DE CERTIFICACION DIGITAL	ACTIVIDADES DE CERTIFICACIÓN Artículo 161 del Decreto Ley 0019 de 2012	DOCUMENTOS NORMATIVOS O TÉCNICOS Anexos CEA-4.1-10
posee por el desempeño de su actividad habitual en el ámbito de su profesión.	Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.	FIPS 140-2 Nivel 3 mayo 2001
<b>CERTIFICADOS DIGITALES DE PERSONA NATURAL</b> Garantiza la identidad de la Persona natural.	Emisión de certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.  Emisión de certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.  Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.	RSA 2048 RSA 4096 SHA-256 Tamaño de clave mínimo 2048 bits agosto 2002 RFC 5280 mayo 2008 ITU-T-X509 octubre 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 noviembre 2003 FIPS 140-2 Nivel 3 mayo 2001
<b>CERTIFICADOS DIGITALES DE FACTURA ELECTRONICA PERSONA NATURAL</b> Certificado exclusivo para facturación electrónica atendiendo a la necesidad de las empresas que buscan la seguridad del certificado para la emisión de facturas electrónicas.	Emisión de certificados en relación con las firmas electrónicas o digitales de personas naturales.  Emisión de certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.  Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.	RSA 2048 RSA 4096 SHA-256 Tamaño de clave mínimo 2048 bits agosto 2002 RFC 5280 mayo 2008 ITU-T-X509 octubre 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 noviembre 2003 FIPS 140-2 Nivel 3 mayo 2001
<b>CERTIFICADOS DIGITALES DE FACTURA ELECTRONICA PERSONA JURIDICA</b> Certificado exclusivo para facturación electrónica atendiendo a la necesidad de las empresas que buscan la seguridad del certificado para la emisión de facturas electrónicas.	Emisión de certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.  Emisión de certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.  Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.	RSA 2048 RSA 4096 SHA-256 tamaño de clave mínimo 2048 bits Agosto 2002 RFC 5280 Mayo 2008 ITU-T-X509 V3 octubre 2012 ETSI TS 102 042 Febrero 2013 RFC 3647 Noviembre 2003 RFC 4523 Junio 2006 FIPS 140-2 Nivel 3 Mayo 2001
<b>CERTIFICADOS DIGITALES DE PERSONA JURIDICA</b> Realización de trámites empresariales por parte de una aplicación ejecutándose en una máquina en procesos de firma	Emisión de certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.	RSA 2048 RSA 4096 SHA-256 Tamaño de clave mínimo 2048 bits agosto 2002 RFC 5280 mayo 2008

	<b>POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES</b>	Versión	8
		Implementación	14/08/2020

SERVICIOS DE CERTIFICACION DIGITAL	ACTIVIDADES DE CERTIFICACIÓN Artículo 161 del Decreto Ley 0019 de 2012	DOCUMENTOS NORMATIVOS O TÉCNICOS Anexos CEA-4.1-10
<p>automáticos y desatendidos en nombre de una persona Jurídica de derecho público o privado que requieran garantizar la autenticidad y la integridad de los datos enviados o almacenados digitalmente junto con en el establecimiento de canales de comunicación seguros entre clientes, y que será representada por medio de una persona física (Responsable), poseedor del certificado emitido bajo esta política y denominado Responsable.</p>	<p>Emisión de certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.</p> <p>Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.</p>	<p>ITU-T-X509 octubre 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 noviembre 2003 FIPS 140-2 Nivel 3 mayo 2001</p>
<p><b>CERTIFICADOS DIGITALES PARA FIRMA CENTRALIZADA</b></p> <p>Garantiza la identidad de la persona natural o jurídica titular del certificado, así como su vinculación a una determinada entidad jurídica en virtud del cargo que ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual</p>	<p>Certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.</p> <p>Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas.</p> <p>Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.</p> <p>Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas</p>	<p>RSA 2048 RSA 4096 SHA-256 Tamaño de clave mínimo 2048 bits agosto 2002 RFC 5280 mayo 2008 ITU-T-X509 octubre 2016 ETSI EN 319 411-1 V1.2.0 (2017-08) RFC 3647 noviembre 2003 FIPS 140-2 Nivel 3 mayo 2001</p>

## 7.7 Características de los dispositivos criptográficos

Para la emisión y almacenamiento de los certificados digitales, GSE utiliza dispositivos criptográficos certificados FIPS 140-2 nivel 3, que proporciona mayor seguridad física y lógica al dispositivo, protegiendo el contenido del mismo.

### 7.7.1 Certificado Digital en Token

CARACTERÍSTICA	ESPECIFICACIÓN TECNICA
<b>Sistemas Operativos soportados</b>	 32bit and 64bit Windows XP SP3, Vista, 7, 8, 10. Mac OS. Server2003, Server2008, Server2008 R2, Server 2012 R2.
<b>Estándar</b>	X.509 v3, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID
<b>Funciones Criptográficas</b>	Generación de par de claves Firma digital y verificación Cifrado y descifrado de datos



Token  
ePass2003

<b>Procesador</b>	16 bit smart card chip (Common Criteria EAL 5+ certificado)
<b>Memoria</b>	64KB (EEPROM)
<b>Conectividad</b>	<ul style="list-style-type: none"> <li>Token USB 2.0 velocidad total, Conector tipo A</li> </ul>
<b>Bloqueo del Dispositivo</b>	Se bloqueará al tercer intento de uso con clave incorrecta
<b>Temperatura en Operación</b>	0°C ~ 70°C (32°F ~ 158°F)
<b>Temperatura de Almacenamiento</b>	-20°C ~ 85°C (-4°F ~ 185°F)

### 7.7.2 Certificado Digital en HSM – Hardware Security Module (FirmaCentralizada)

CARACTERÍSTICA	ESPECIFICACIÓN TÉCNICA
<b>Sistemas Operativos soportados</b>	 32bit and 64bit <ul style="list-style-type: none"> <li>Windows XP SP3, Vista, 7, 8, 10.</li> <li>Server2003, Server2008, Server2008 R2, Server 2012 R2.</li> </ul>
<b>Estándar</b>	<ul style="list-style-type: none"> <li>X.509 v3, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID</li> </ul>
<b>Funciones Criptográficas</b>	<ul style="list-style-type: none"> <li>Generación de par de claves</li> <li>Firma digital y verificación</li> <li>Cifrado y descifrado de datos</li> </ul>
<b>Conectividad</b>	<ul style="list-style-type: none"> <li>Web, con Usuario/Contraseña</li> </ul>
<b>Bloqueo de Sesión</b>	<ul style="list-style-type: none"> <li>Se bloquea la sesión desde la IP del usuario, al tercer intento de acceso con contraseña incorrecta</li> </ul>

### 7.7.3 Características Técnicas de los Certificados Digitales

CARACTERÍSTICA	ESPECIFICACIÓN TÉCNICA
Algoritmo de Firma	<i>Función Hash</i> SHA256 con RSA Encryption.
	<i>Función de Cifrado</i> <ul style="list-style-type: none"> <li>RSA con longitud de clave de 4096 para CA RAIZ</li> <li>RSA con longitud de clave de 4096 para SUBORDINADA CA</li> <li>RSA con longitud de clave suscriptores / responsables de 2048.</li> </ul>
Contenido del Certificado Digital	<ul style="list-style-type: none"> <li>RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Mayo 2008.</li> <li>ITU-T-X509 octubre 2016</li> <li>ETSI TS 102 042 - Policy requirements for certification authorities issuing public key.</li> </ul>

Ciclo de vida de los certificados	<ul style="list-style-type: none"> <li>• RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.</li> </ul>
Generación de claves	<ul style="list-style-type: none"> <li>• Token FIPS 140-2 Nivel 3</li> <li>• HSM FIPS 140-2 Nivel 3 (Firma Centralizada)</li> </ul>
Actividades de certificación artículo 161 del decreto ley 0019 de 2012	<ul style="list-style-type: none"> <li>• Emisión de certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.</li> <li>• Emisión de certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.</li> <li>• Emisión de certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.</li> </ul>

## 7.8 Obligaciones

### 7.8.1 Obligaciones de la ECD GSE

ECD GSE como entidad de prestación de servicios de certificación está obligada según normativa vigente, en lo dispuesto en las Políticas de Certificado y en la DPC a:

1. Respetar lo dispuesto en la normatividad vigente, la DPC y en las Políticas de Certificado.
2. Publicar la DPC y cada una de las Políticas de Certificado en la página Web de GSE.
3. Informar a ONAC sobre las modificaciones de la DPC y de las Políticas de Certificado.
4. Mantener la DPC y Políticas de Certificado con su última versión publicadas en la página Web de GSE.
5. Proteger y custodiar de manera segura y responsable su llave privada.
6. Emitir certificados conforme a las Políticas de Certificado y a los estándares definidos en la DPC.
7. Generar certificados consistentes con la información suministrada por el solicitante o suscriptor.
8. Conservar la información sobre los certificados emitidos de conformidad con la normatividad vigente.
9. Emitir certificados cuyo contenido mínimo este de conformidad con la normativa vigente para los diferentes tipos de certificados.
10. Publicar el estado de los certificados emitidos en un repositorio de acceso libre.
11. No mantener copia de la llave privada del solicitante o suscriptor.
12. Revocar los certificados según lo dispuesto en la Política de revocación de certificados digitales.

13. Actualizar y publicar la lista de certificados revocados CRL con los últimos certificados revocados.
14. Notificar al Solicitante, Suscriptor o Entidad la revocación del certificado digital dentro de las 24 horas siguientes a la revocación del certificado de conformidad con la política de revocación de certificados digitales.

### 7.8.2 Obligaciones de la RA

La RA de la ECD GSE está facultada para realizar la labor de identificación y registro, por lo tanto, está obligada en los términos definidos en la Declaración de Prácticas de Certificación a:

1. Conocer y dar cumplimiento a lo dispuesto en la DPC y en la Política de Certificado correspondiente a cada tipo de certificado.
2. Custodiar y proteger su llave privada.
3. Comprobar la identidad de los Solicitantes, Responsables o Suscriptores de certificados digitales.
4. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
5. Archivar y custodiar la documentación suministrada por el solicitante o suscriptor, durante el tiempo establecido por la legislación vigente.
6. Respetar lo dispuesto en los contratos firmados entre ECD GSE y el suscriptor.
7. Identificar e informar a la ECD GSE las causas de revocación suministradas por los solicitantes sobre los certificados digitales vigentes.

### 7.8.3 Obligaciones y derechos del suscriptor y/o responsable

El Suscriptor como suscriptor o responsable de un certificado digital está obligado a cumplir con lo dispuesto por la normativa vigente y lo dispuesto en la DPC como es:

- a. Usar su certificado digital según los términos de la DPC.
- b. Verificar dentro del día siguiente hábil que la información del certificado digital es correcta. En caso de encontrar inconsistencias, notificar a la ECD.
- c. Abstenerse de: prestar, ceder, escribir, publicar la contraseña de uso su certificado digital y tomar todas las medidas necesarias, razonables y oportunas para evitar que éste sea utilizado por terceras personas.
- d. No transferir, compartir ni prestar el dispositivo criptográfico a terceras personas.
- e. Suministrar toda la información requerida en el Formulario de Solicitud de Certificados digitales para facilitar su oportuna y plena identificación.
- f. Solicitar la revocación del Certificado Digital ante el cambio de nombre y/o apellidos.
- g. Solicitar la revocación del Certificado Digital cuando el Suscriptor haya variado su nacionalidad.
- h. Cumplir con lo aceptado y firmado en el documento términos y condiciones o responsable de certificados digitales.
- i. Proporcionar con exactitud y veracidad la información requerida.
- j. Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del certificado.
- k. Custodiar y proteger de manera responsable su llave privada.

- l. Dar uso al certificado de conformidad con lo establecido en esta PC para cada uno de los tipos de certificado.
- m. Solicitar como suscriptor o responsable de manera inmediata la revocación de su certificado digital cuando tenga conocimiento que existe una causal definida en numeral *Circunstancias para la revocación de un certificado* de la DPC.
- n. No hacer uso de la llave privada ni del certificado digital una vez cumplida su vigencia o se encuentre revocado.
- o. Informar a los terceros de confianza de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado.
- p. Informar al tercero de buena fe para verificar el estado de un certificado dispone de la lista de certificados revocados CRL, publicada de manera de periódica por ECD GSE.
- q. No realizar ninguna declaración relacionada con su certificación digital en la ECD GSE pueda considerar engañosa o no autorizada, conforme a lo dispuesto por la DPC y PC.
- r. Una vez caducado o revocado el servicio de certificación digital el suscriptor debe inmediatamente dejar de utilizarla en todo el material publicitario que contenga alguna referencia al servicio.
- s. El suscriptor al hacer referencia al servicio de certificación digital prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, debe informar que cumple con los requisitos especificados en las PC de la DPC, indicando la versión.

Por otro lado, tiene los siguientes derechos:

- a. Recibir el certificado digital en los tiempos establecidos en la DPC.
- b. El suscriptor podrá utilizar las marcas de conformidad y la información relacionada con el servicio de certificación digital prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, desde que cumpla lo requerido en el literal anterior.
- c. Solicitar información referente a las solicitudes en proceso.
- d. Solicitar revocación del certificado digital aportando la documentación necesaria.
- e. Recibir el certificado digital de acuerdo con el alcance otorgado por ONAC a GSE.

#### 7.8.4 Obligaciones de la Entidad (Cliente)

La entidad cliente es la encargada de solicitar los servicios para sus funcionarios y los suscriptores son las personas que hacen uso del servicio.

Conforme lo establecido en las Políticas de Certificado, en el caso de los certificados donde se acredite la vinculación del Suscriptor o Responsable con la misma, será obligación de la Entidad:

- a. Solicitar a la RA GSE la suspensión/revocación del certificado cuando cese o se modifique dicha vinculación.
- b. Todas aquellas obligaciones vinculadas al responsable del servicio de certificación digital.

- c. La entidad al hacer referencia al servicio de certificación digital prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, debe informar que cumple con los requisitos especificados en las PC de la DPC.
- d. La entidad podrá utilizar las marcas de conformidad y la información relacionada con el servicio de certificación digital prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, desde que cumpla lo requerido en el literal anterior.

### 7.8.5 Obligaciones de otros participantes

La Comité de Gerencia y el proceso Sistema Integrado de Gestión como organismos internos de ECD GSE está en la obligación de:

- a. Revisar la consistencia de la DPC con la normatividad vigente.
- b. Aprobar y decidir sobre los cambios a realizar sobre los servicios de certificación digital, por decisiones de tipo normativo o por solicitudes de suscriptores o responsables.
- c. Aprobar la notificación de cualquier cambio a los suscriptores y/ responsables analizando su impacto legal, técnico o comercial.
- d. Revisar y tomar acciones sobre cualquier comentario realizado por suscriptores o responsables cuando un cambio en el servicio de certificación digital se realice.
- e. Informar los planes de acción a ONAC y SIC sobre todo cambio que tenga impacto sobre la infraestructura PKI y que afecte los servicios de certificación digital, de acuerdo con el R-AC-01.
- f. Autorizar los cambios o modificaciones requeridas sobre la DPC.
- g. Autorizar la publicación de la DPC en la página Web de la ECD GSE.
- h. Aprobar los cambios o modificaciones a las Políticas de Seguridad de la ECD GSE.
- i. Asegurar la integridad y disponibilidad de la información publicada en la página Web de la ECD GSE.
- j. Asegurar la existencia de controles sobre la infraestructura tecnológica de la ECD GSE.
- k. Solicitar la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la llave privada del suscriptor, entidad o cualquier otro hecho que tienda al uso indebido de llave privada del suscriptor, entidad o de la propia ECD.
- l. Conocer y tomar acciones pertinentes cuando se presenten incidentes de seguridad.
- m. Realizar con una frecuencia máxima anual, una revisión de la DPC para verificar que las longitudes de las llaves y periodos de los certificados que se estén empleando son adecuados.
- n. Revisar, aprobar y autorizar cambios sobre los servicios de certificación digital acreditados por el organismo competente.
- o. Revisar, aprobar y autorizar la propiedad y el uso de símbolos, certificados y cualquier otro mecanismo que requiera ECD GSE para indicar que el servicio de certificación digital está acreditado.
- p. Velar que las condiciones de acreditación otorgado por el organismo competente se mantengan.
- q. Velar por el uso adecuado en documentos o en cualquier otra publicidad que los símbolos, los certificados, y cualquier otro mecanismo que indique que ECD GSE

cuenta con un servicio de certificación acreditado y cumple con lo dispuesto en las Reglas de Acreditación de ONAC el RAC-3.0-01 y RAC-3.0-03.

- r. Velar por mantener informados a sus proveedores críticos y ECD recíproca en caso de existir, de la obligación de cumplimiento de los requisitos del CEA-4.1-10, en los numerales que correspondan.
- s. El proceso del Sistema Integrado de Gestión ejecutará planes de acción preventivos y correctivos para responder ante cualquier riesgo que comprometa la imparcialidad de la ECD, ya sea que se derive de las acciones de cualquier persona, organismo, organización, actividades, sus relaciones o las relaciones de su personal o de sí misma. Para lo cual utiliza la norma ISO 31000 para la identificación de riesgos que comprometa la imparcialidad de la ECD.
- t. Velar que todo el personal y los comités de la ECD (sean internos o externos), que puedan tener influencia en las actividades de certificación actúen con imparcialidad y no discriminación, especialmente aquellas que surjan por presiones comerciales, financieras u otras comprometan su imparcialidad.
- u. Documentar y demostrar el compromiso de imparcialidad y no discriminación.
- v. Velar que el personal administrativo, de gestión, técnico de la PKI, de la ECD asociado a las actividades de consultoría, mantenga completa independencia y autonomía respecto al personal del proceso de revisión y toma de decisión sobre la certificación de la misma ECD.

### 7.9 Tarifas del servicio de emisión de certificados digitales

#### 7.9.1 Tarifas de emisión o renovación de certificados

Detalle del producto	Tiempo de entrega	Vigencia	Precio sin iva	IVA	Total
Certificado Persona Natural	Normal	1	\$ 191.597	\$ 36.403	\$ 228.000
Certificado Persona Natural	Normal	2	\$ 277.310	\$ 52.689	\$ 329.999
Certificado Perteneiente a empresa	Normal	1	\$ 191.597	\$ 36.403	\$ 228.000
Certificado Perteneiente a empresa	Normal	2	\$ 277.310	\$ 52.689	\$ 329.999
Certificado Profesional Titulado	Normal	1	\$ 191.597	\$ 36.403	\$ 228.000
Certificado Profesional Titulado	Normal	2	\$ 277.310	\$ 52.689	\$ 329.999
Certificado Representante Legal	Normal	1	\$ 191.597	\$ 36.403	\$ 228.000
Certificado Representante Legal	Normal	2	\$ 277.310	\$ 52.689	\$ 329.999
Certificado Función Publica	Normal	1	\$ 191.597	\$ 36.403	\$ 228.000
Certificado Función Publica	Normal	2	\$ 277.310	\$ 43.907	\$ 274.999
Certificado Persona Jurídica	Normal	1	\$ 504.202	\$ 95.798	\$ 600.000



## POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

Versión

8

Implementación

14/08/2020

Detalle del producto	Tiempo de entrega	Vigencia	Precio sin iva	IVA	Total
Certificado Persona Jurídica	Normal	2	\$ 857.143	\$ 162.857	\$ 1.020.000

\*Estos precios no incluyen I.V.A y están calculados sobre vigencia de un año. Las cifras aquí indicadas para cada tipo de certificado podrán variar según acuerdos comerciales especiales a los que se pueda llegar con los suscriptores, entidades o solicitantes, en desarrollo de campañas promocionales adelantadas por GSE.

\*Para poder usar el certificado de firma centralizada, es necesario la adquisición de una plataforma tecnológica con costos adicionales.

### 7.9.2 Modelos y minutas de los documentos de términos y condiciones

De acuerdo con lo enunciado en el Anexo 2 de la DPC.

### 7.10 Perfil de los certificados

Consultar el Anexo 1 de la DPC Matriz perfil técnico de los Certificados

<b>OID (Object Identifier)</b>	1.3.6.1.4.1.31136.1.4.8
<b>Ubicación de la PC</b>	<a href="https://gse.com.co/documentos/calidad/politicas/Politicas_de_Certificado_para_Certificados_Digitales.pdf">https://gse.com.co/documentos/calidad/politicas/Politicas_de_Certificado_para_Certificados_Digitales.pdf</a>