Título del Documento	**Políticas de Certificado para Servicio de Certificados Digitales**
Versión	11
Grupo de Trabajo	Comité de Gerencia
Estado del documento	Final
Fecha de emisión	15/02/2010
Fecha de inicio de vigencia	16/07/2021
OID (Object Identifier)	1.3.6.1.4.1.31136.1.4.11
Ubicación de la Política	https://gse.com.co/documentos/calidad/politicas/Politicas_de_Certificado_para_Certificados_Digitales_V11.pdf
Elaboró	Director de Operaciones
Revisó	Sistema Integrado de Gestión
Aprobó	Comité de Gerencia

Control de Cambios

Versión	Fecha	Cambio/Modificación
1	01-11-2016	Documento inicial conforme al desarrollo del plan de acción de la auditoria 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 auditoria 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.
9	12/02/2021	Se incluyeron los datos de la ECD y CA(Paynet) con los enlaces para consultar en línea el Certificado de Existencia y Representación Legal. Se actualizaron los links para que apunten a las nuevas rutas. Se actualizaron los siguientes numerales: • 7.6. Requerimiento específico tramitación del certificado.

Versión	Fecha	Cambio/Modificación
10	16/07/2021	Se actualizaron los numerales: 3.1. Resumen, proveedor de servicios de infraestructura PKI, url de consulta de CERL y teléfonos de contacto. 5.3. OID de las Políticas 7. Requisitos de los certificados digitales de la ECD GSE 7.7. Requisitos específicos tramitación del certificado 7.9. Actividades y referencias técnicas de los certificados, documentos normativos o técnicos Anexos CEA-4.1-10, se incluyó EC384, EC256 en todos los servicios de certificación digital. 8.1.1 Se modifico la imagen de los dispositivos criptográficos Se incluyeron los numerales: 7.6 Prohibiciones de Uso de los Certificados 8.1.2 Compromisos de seguridad 8.1.3 Cuidados del dispositivo criptográfico 8.1.4 Riesgos asociados. 7.9.3. Características Técnicas de los Certificados Digitales 10. Protección de la información personal 11. Imparcialidad y no discriminación Se actualiza el OID y el link de consulta de la política.
11	27/10/2021	• Se modifico el numeral 7.7 Requisitos Específicos Tramitación del Certificado incluyendo en la sección final de Nota un aclaración sobre el RUT actualizado de la DIAN el cual debe tener el código QR. • Se ajusto el OID y el link de la PC

TABLA DE CONTENIDO

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 prevalecía 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.

DATOS DE LA ENTIDAD PRESTADORA DE SERVICIOS DE CERTIFICACIÓN DIGITAL:

Razón Social:	GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.
Sigla:	GSE S.A.
Número de Identificación Tributaria:	900.204.272 – 8
Registro Mercantil No:	01779392 de 28 de febrero de 2008
Certificado de Existencia y Representante Legal:	https://gse.com.co/documentos/marco-regulatorio/Certificado-de-Existencia-y-Representante-Legal-GSE.pdf
Estado del registro mercantil:	Activo
Dirección social y correspondencia:	Calle 73 No. 7 – 31 Piso 3 Torre B Edificio el Camino
Ciudad / País:	Bogotá D.C., Colombia
Teléfono:	+57 (1) 4050082
Fax:	+57 (1) 4050082
Correo electrónico:	info@gse.com.co
Página Web:	www.gse.com.co

GSE tiene como proveedor de servicios de infraestructura PKI - CA:

Razón Social:	PAYNET S.A.S
Sigla:	PAYNET
Número de Identificación Tributaria:	901.043.004-2
Registro Mercantil No:	02766647 de 13 de enero de 2017
Certificado de Existencia y Representante Legal:	https://www.paynet.com.co/wp-content/uploads/Certificado-de-Existencia-y-Representante-Legal-Paynet.pdf
Estado del registro mercantil:	Activo
Dirección social y correspondencia:	Cl 73 No. 7 – 31 Of 302
Ciudad / País:	Bogotá D.C., Colombia
Teléfono 1:	+57 (1) 4053224
Fax:	+57 (1) 4053224
Correo electrónico:	representante.legal@paynet.com.co
Página Web:	www.paynet.com.co

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.

Revocación: Proceso por el cual un certificado digital se deshabilita y pierde validez.

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.
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:	Victor Armando Ibañez Palacios
Cargo del contacto:	Director de Operaciones
Teléfonos de contacto:	4050082 - 3232085095
Correo electrónico:	victor.ibanez@gse.com.co 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 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
Dirección:	Calle 73 No. 7 – 31 Piso 3 Torre B Edificio el Camino
Página Web:	www.gse.com.co
Responsable:	Sistema Integrado de Gestión

Una vez presentado el caso, este es trasmitido 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. Para el caso de las disputas toman el mismo camino como una PQRSA según el procedimiento establecido.

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
- 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
1.3.6.1.4.1.31136.1.4.11	Política de Certificados 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:

TIPO DE CERTIFICADO	OBJETO
Certificado de Pertenencia a Empresa	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.
Certificado de Representación Empresa	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.
Certificados de Función Pública	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.
Certificados de Profesional Titulado	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.
Certificados de Persona Natural	Garantiza únicamente la identidad de la Persona natural.
Certificados de Factura Electrónica para persona natural	Garantiza únicamente la identidad de la Persona natural.
Certificados de Factura Electrónica para persona jurídica	Certificado exclusivo para facturación electrónica atendiendo a la necesidad de las empresas que buscan la seguridad del certificado para la emisión de facturas electrónicas.
Certificado de Persona Jurídica	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.
Certificados Firma Centralizada	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. REQUISITOS 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. Requisitos 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. Requisitos 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. Requisitos Específicos: 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
Certificado de Pertenencia a Empresa	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

TIPO DE CERTIFICADO	SUSCRIPTOR / RESPONSABLE	ATRIBUTO	ENTIDAD
Certificado de Representación Empresa	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
Certificados de Función Pública	Persona natural que pertenece a una Administración Pública y que es titular del certificado	Vinculación funcionarial respecto a una Administración Publica	Administración Pública a la que está vinculada el Suscriptor
Certificados de Profesional Titulado	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
Certificados de Persona Natural	Persona natural titular del certificado	No aplica	No aplica
Certificados de Factura Electrónica persona natural	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
Certificados de Factura Electrónica persona Jurídica	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
Certificado de Persona Jurídica	Responsable del certificado que obra en nombre de una Persona Jurídica	Vinculación de representación legal a empresa	Empresa a la que representa el Suscriptor
Certificados de Firma Centralizada	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. Usos de los Certificados

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
Certificado de Pertenencia a Empresa	Realización de trámites empresariales por parte del Firmante/Suscriptor sin que implique representación. La empresa puede establecer limitaciones de uso.
Certificado de Representación Empresa	Realización de trámites empresariales por parte del Firmante/Suscriptor en nombre y representación de la empresa. La empresa puede establecer limitación de uso.
Certificados de Función Pública	Realización de trámites por parte del Suscriptor en el ejercicio de sus funciones como funcionario público. La Administración Pública puede establecer limitaciones de uso.
Certificados de Profesional Titulado	Realización de trámites por parte del Suscriptor en el ejercicio de sus funciones como profesional colegiado.
Certificados de Persona Natural	Realización de trámites por parte del Suscriptor en su calidad de ciudadano. No existe vinculación alguna con ninguna entidad.
Certificados de Factura Electrónica persona natural	Realización por parte del responsable de la facturación electrónica en nombre propio
Certificados de Factura Electrónica persona jurídica	Realización por parte del responsable de la facturación electrónica en nombre de empresa.
Certificado de Persona Jurídica	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.
Certificados de Firma Centralizada.	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 adquiera una plataforma con costos adicionales.

7.5. 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
Certificado de Pertenencia a Empresa	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 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.
Certificado de Representación Empresa	
Certificados de Función Pública	
Certificados de Profesional Titulado	
Certificados de Persona Natural	
Certificados de Factura Electrónica persona natural	
Certificados de Factura Electrónica persona jurídica	
Certificados de Persona Jurídica	
Certificados Digitales Para Firma Centralizada	

7.6. Prohibiciones de Uso de los Certificados

La realización de operaciones no autorizadas según esta Política, por parte de terceros o suscriptores del servicio eximirá a la ECD GSE de cualquier responsabilidad por este uso prohibido.

- No se permite el uso del certificado para firmar otros certificados o listas de revocación (CRL)
- Está prohibido utilizar el certificado para usos distintos a los estipulados en el apartado “Uso del Certificado” y “Limites de Responsabilidad de la Entidad de Certificación Digital Abierta” de la presente Política.
- Las alteraciones sobre certificados no están permitidas y el certificado debe usarse tal y como fue suministrado por la ECD GSE.
- Se prohíbe el uso de certificados en sistemas de control o sistemas intolerantes a fallos que puedan ocasionar daños personales o medioambientales.
- Se considera prohibida toda aquella acción que infrinja las disposiciones, obligaciones y requisitos estipulados en la presente Política.
- No es posible por parte de la ECD GSE emitir valoración alguna sobre el contenido de los documentos que firma el suscriptor, por lo tanto la responsabilidad del contenido del mensaje es responsabilidad única del signatario.
- No es posible por parte de la ECD GSE recuperar los datos cifrados en caso de pérdida de la llave privada del suscriptor porque la CA por seguridad no guarda

copia de la llave privada de los suscriptores, por lo tanto es responsabilidad del suscriptor la utilización de cifrado de datos.

- Fines u operaciones ilícitas bajo cualquier régimen legal del mundo.

7.7. Requisitos Específicos 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 SOLICITADA
Para todo tipo de certificado se solicitarán los siguientes documentos: • Formulario On- line de la solicitud diligenciado. • Aceptación de términos y condiciones. • Documento de identificación del solicitante • Registro Único Tributario – RUT	
Certificado de Pertenencia Empresa	• Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) días. • Certificado laboral del solicitante incluyendo el cargo en papel institucional (no mayor a treinta (30) días.
Certificado de Representación Empresa	• Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) día.
Certificados de Función Pública	• Para confirmar la información de relación del solicitante con la Empresa se solicitará alguno de los siguientes documentos: ➢ Acta de posesión ➢ Resolución de nombramiento ➢ Contrato de prestación de servicios. ➢ Certificado laboral del solicitante incluyendo el cargo en papel institucional (no mayor a treinta (30) días desde la radicación de la solicitud).
Certificados de Profesional Titulado	• Tarjeta Profesional y/o documento equivalente. • Diploma de grado (opcional),
Certificados de Persona Natural	• En caso de que el solicitante no tenga Registro Único Tributario – RUT debe presentar un documento donde se registre la información de domicilio que sea expedido por un tercero que lo verifique.
Certificados de Factura Electrónica persona natural	• En caso de que el solicitante no tenga Registro Único Tributario – RUT debe presentar un documento donde se registre la información de domicilio que sea expedido por un tercero que lo verifique. Para el caso que el proceso de facturación se realice por un tercero: • Constancia delegación del proceso al tercero en papel institucional

TIPO DE CERTIFICADO	REGISTRO: DOCUMENTACIÓN SOLICITADA
Certificados de Factura Electrónica persona jurídica	• Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) días. Para el caso que el proceso de facturación se realice por un tercero: • Constancia delegación del proceso al tercero en papel institucional
Certificados de Persona Jurídica	• Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) días.
Certificados Digitales Para Firma Centralizada	• Aplican todos los documentos descritos en los certificados anteriores.

Notas:

- Los documentos se recibirán escaneados o en original electrónico, preservando la legibilidad para el uso de la información.
- El documento Registro Único Tributario – RUT se solicitará en el formato actualizado de DIAN que incluye código QR.
- La información de domicilio del solicitante: país, departamento, municipio y dirección se revisará en los documentos: Documento de Existencia y Representación Legal o Registro Único Tributario – RUT.
- Para los tipos de certificado donde se solicita el Documento de Existencia y Representación Legal dicho documento será válido con una vigencia no mayor a treinta (30) días desde la radicación de la solicitud.
- Para los tipos de certificados donde se solicita el Documento de Existencia y Representación Legal de la Empresa, en los casos que sea requerido será válido un documento equivalente donde se pueda validar la existencia y representación legal de la empresa, de ser el caso se solicitará el documento debidamente autenticando.
- Para los tipos de certificados donde se solicita el Registro Único Tributario – RUT del solicitante, en los casos que sea requerido será válido un documento equivalente donde se pueda validar la existencia y representación legal del solicitante y los datos de domicilio del mismo, de ser el caso se solicitará el documento debidamente autenticando.
- Todo documento que se reciba autenticado, la autenticación debe tener una vigencia no mayor a sesenta (60) días desde la radicación de la solicitud.

7.8. Requerimiento Específico: Vigencia de los Certificados

Los certificados emitidos por la ECD GSE tienen una vigencia máxima de veinticuatro (24) meses.

7.9. 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
CERTIFICADOS DIGITALES PARA PERTENENCIA EMPRESA Garantiza la identidad de la persona natural titular del certificado, así como su vinculación a una determinada entidad	Emisión de certificados en relación con las firmas electrónicas o digitales de personas natura les o jurídicas.	RSA 2048 RSA 4096 SHA-256 Tamaño de clave mínimo 2048 bits agosto 2002 RFC 5280 mayo 2008

SERVICIOS DE CERTIFICACION DIGITAL	ACTIVIDADES DE CERTIFICACIÓN Artículo 161 del Decreto Ley 0019 de 2012	DOCUMENTOS NORMATIVOS O TÉCNICOS Anexos CEA-4.1-10
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.	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.	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 EC 384 EC 256
CERTIFICADOS DIGITALES PARA REPRESENTACION EMPRESA 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.	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 EC 384 EC 256
CERTIFICADOS DIGITALES DE FUNCION PUBLICA 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.	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 EC 384 EC 256
CERTIFICADOS DIGITALES DE PROFESIONAL TITULADO 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.	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 EC 384 EC 256

SERVICIOS DE CERTIFICACION DIGITAL	ACTIVIDADES DE CERTIFICACIÓN Artículo 161 del Decreto Ley 0019 de 2012	DOCUMENTOS NORMATIVOS O TÉCNICOS Anexos CEA-4.1-10
CERTIFICADOS DIGITALES DE PERSONA NATURAL 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 EC 384 EC 256
CERTIFICADOS DIGITALES DE FACTURA ELECTRONICA PERSONA NATURAL 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 EC 384 EC 256
CERTIFICADOS DIGITALES DE FACTURA ELECTRONICA PERSONA JURIDICA 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 EC 384 EC 256
CERTIFICADOS DIGITALES DE PERSONA JURIDICA 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	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	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 EC 384 EC 256

SERVICIOS DE CERTIFICACION DIGITAL	ACTIVIDADES DE CERTIFICACIÓN Artículo 161 del Decreto Ley 0019 de 2012	DOCUMENTOS NORMATIVOS O TÉCNICOS Anexos CEA-4.1-10
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.	con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.	
CERTIFICADOS DIGITALES PARA FIRMA CENTRALIZADA 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	Certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas. Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas. 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. Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas	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 EC 384 EC 256

8. 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.

8.1. Certificado Digital en Token

8.1.1 Características

CARACTERÍSTICA	ESPECIFICACIÓN TECNICA
Sistemas Operativos soportados	32bit and 64bit Windows XP SP3, Vista, 7, 8, 10. Mac OS. Server2003, Server2008, Server2008 R2, Server 2012 R2.
Estándar	X.509 v3, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID
Funciones Criptográficas	Generación de par de claves Firma digital y verificación Cifrado y descifrado de datos
Soporte de Algoritmos	RSA 512/1024/2048, DES, 3DES, SHA-1, SHA-256/384/512, AES 128/192/256
Procesador	16 bit smart card chip (Common Criteria EAL 5+ certificado)
Memoria	64KB (EEPROM)
Conectividad	Token USB 2.0 velocidad total, Conector tipo A
Bloqueo del Dispositivo	Se bloqueará al tercer intento de uso con clave incorrecta
Temperatura en Operación	0°C ~ 70°C (32°F ~ 158°F)
Humedad	0% ~ 100% sin condensación
Temperatura de Almacenamiento	-20°C ~ 85°C (-4°F ~ 185°F)
Peso Neto	8.1 gr
Dimensiones	54.5x17x8.5 mm

8.1.2 Compromisos de seguridad

Por circunstancias que afectan la seguridad del dispositivo criptográfico:

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación del Firmante o del responsable de certificado

8.1.3 Cuidados del dispositivo criptográfico

- Mantenerlo en un lugar seco y alejado de las variaciones ambientas y/o de temperatura.
- No exponerlo a campos magnéticos.
- Evitar que sea golpeado o sometido a algún esfuerzo físico.
- No intentar abrirlo, retirar la protección plástica o placa de circuitos, ya que ocasionara su mal funcionamiento.

- No introducirlo en agua o otros líquidos.
- Notificar a la ECD – GSE en caso de hurto, robo, perdida y/o fraude del token con el fin de revocar el certificado digital.

8.1.4 Riesgos asociados

Los dispositivos criptográficos admitidos por la ECD – GSE pueden presentar los siguientes riesgos:

- Perdida del dispositivo.
- Compromiso de la llave.
- Daño por manipulación inadecuada.
- Daño por el no cuidado del dispositivo frente a las condiciones ambientales.
- Daño por variación del voltaje.

Para mitigar los riesgos asociados deben tenerse en cuenta:

- El certificado digital de firma es personal e intransferible, el PIN es confidencial.
- Se recomienda cambiar el PIN periódicamente.
- No ingresar incorrectamente el PIN más de tres (3) veces, bloqueará el dispositivo.
- Los dispositivos criptográficos deben mantenerse en condiciones ambientas adecuadas.
- En caso de compromiso o perdida de la llave privada debe solicitar la revocación del certificado digital.

8.2. Certificado Digital en HSM – Hardware Security Module (Firma Centralizada)

CARACTERÍSTICA	ESPECIFICACIÓN TÉCNICA
Sistemas Operativos soportados	32bit and 64bit • Windows XP SP3, Vista, 7, 8, 10. • Server2003, Server2008, Server2008 R2, Server 2012 R2.
Estándar	• X.509 v3, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID
Funciones Criptográficas	• Generación de par de claves • Firma digital y verificación • Cifrado y descifrado de datos
Conectividad	• Web, con Usuario/Contraseña
Bloqueo de Sesión	• Se bloquea la sesión desde la IP del usuario, al tercer intento de acceso con contraseña incorrecta

8.2.1. Características Técnicas de los Certificados Digitales

CARACTERÍSTICA	ESPECIFICACIÓN TÉCNICA
Algoritmo de Firma	*Función Hash* SHA256 con RSA Encryption. *Función Hash* SHA384 con ECDSA
	Función de Cifrado • RSA con longitud de clave de 4096 para CA RAIZ • RSA con longitud de clave de 4096 para SUBORDINADA CA • RSA con longitud de clave suscriptores / responsables de 2048. • ECDSA con longitud de clave de 384 para CA RAIZ • ECDSA con longitud de clave de 384 para SUBORDINADA CA • ECDSA con longitud de clave suscriptores / responsables de 256.
Contenido del Certificado Digital	• RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Mayo 2008. • ITU-T-X509 octubre 2016 • ETSI TS 102 042 - Policy requirements for certification authorities issuing public key.
Ciclo de vida de los certificados	• RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
Generación de claves	• Token FIPS 140-2 Nivel 3 • HSM FIPS 140-2 Nivel 3 (Firma Centralizada)
Actividades de certificación artículo 161 del decreto ley 0019 de 2012	• 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.

9. OBLIGACIONES

9.1.1. 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:

a) Respetar lo dispuesto en la normatividad vigente, la DPC y en las Políticas de Certificado.

b) Publicar la DPC y cada una de las Políticas de Certificado en la página Web de GSE.
c) Informar a ONAC sobre las modificaciones de la DPC y de las Políticas de Certificado.
d) Mantener la DPC y Políticas de Certificado con su última versión publicadas en la página Web de GSE.
e) Proteger y custodiar de manera segura y responsable su llave privada.
f) Emitir certificados conforme a las Políticas de Certificado y a los estándares definidos en la DPC.
g) Generar certificados consistentes con la información suministrada por el solicitante o suscriptor.
h) Conservar la información sobre los certificados emitidos de conformidad con la normatividad vigente.
i) Emitir certificados cuyo contenido mínimo este de conformidad con la normativa vigente para los diferentes tipos de certificados.
j) Publicar el estado de los certificados emitidos en un repositorio de acceso libre.
k) No mantener copia de la llave privada del solicitante o suscriptor.
l) Revocar los certificados según lo dispuesto en la Política de revocación de certificados digitales.
m) Actualizar y publicar la lista de certificados revocados CRL con los últimos certificados revocados.
n) 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.

9.1.2. 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:

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

9.1.3. Obligaciones (Deberes 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 utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para la ECD.
r) 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.
s) 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.
t) 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.

9.1.4. Obligaciones de los Terceros de buena fe

Los Terceros de buena fe en su calidad de parte que confía en los certificados digitales emitidos por ECD GSE está en la obligación de:

a) Conocer lo dispuesto sobre Certificación Digital en la Normatividad vigente.
b) Conocer lo dispuesto en la DPC y PC.
c) Verificar el estado de los certificados antes de realizar operaciones con certificados digitales.
d) Verificar la Lista de certificados Revocados CRL antes de realizar operaciones con certificados digitales.
e) Conocer y aceptar las condiciones sobre garantías, usos y responsabilidades al realizar operaciones con certificados digitales.

9.1.5. 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.

9.1.6. Obligaciones de otros participantes de la ECD

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 subscriptor, 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 y no discriminación 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.
w) Velar por mantener informados a sus proveedores críticos como la ECD reciproca y datacenter que cumplen con los requisitos de acreditación para ECD como soporte para su contratación y del cumplimiento de los requisitos solicitados tanto administrativos como técnicos.

10. PROTECCION DE LA INFORMACION PERSONAL

10.1. Política de Tratamiento de Datos Personales

La ECD GSE tiene como Política de Tratamiento de Datos Personales de acuerdo con lo establecido en la Ley 1581 de 2012, la cual podrá ser consultada en nuestra página web https://gse.com.co/politicas/ en la sección Política de Tratamiento de Datos Personales, al igual se puede consultar la autorización para el tratamiento de los datos personales.

11. IMPARCIALIDAD Y NO DISCRIMINACION

ECD GSE, en cabeza del Comité de Gerencia y sus colaboradores se comprometen a salvaguardar la imparcialidad e independencia en los procesos y servicios de certificación digital, con el fin de prevenir conflictos de interés al interior de la empresa, con las partes interesadas pertinentes y externos, actuando dentro del marco legal Ley 527 de 1999, Decretos 019 de 2012, 333 de 2014 y 1471 de 2014, y de los criterios específicos de acreditación del Organismo Nacional de Acreditación de Colombia (ONAC), por lo que se establecen los siguientes mecanismos de cumplimiento:

- El Comité de Gerencia y los colaboradores de GSE declaran que no participan directa o indirectamente en servicios o actividades, que puedan poner en peligro la libre competencia, la responsabilidad, la transparencia.
- Los colaboradores utilizarán el levantamiento de acciones preventivas y correctivas para responder a cualquier riesgo que comprometa la imparcialidad de la empresa.
- Los colaboradores que hacen parte de los servicios de certificación digital acreditados no podrán prestar servicios de consultoría, ni involucrar al equipo desarrollador a prestar servicio de soporte técnico al suscriptor o cliente.
- GSE es responsable de la imparcialidad en el desarrollo de sus actividades y no permite que las presiones comerciales, financiera u otras comprometan su imparcialidad.
- GSE no emitirá certificados de firma digital a persona natural o jurídica que tenga relación con grupos al margen de la ley o que desarrollen actividades ilícitas.

- GSE podrá declinar la aceptación de una solicitud o el mantenimiento de un contrato para la certificación cuando existan razones fundamentadas, demostradas o indebidas por parte del solicitante y/o suscriptor.
- GSE ofrece acceso a un servicio de certificación digital que no depende del tamaño del solicitante o suscriptor ni de la membresía de cualquier asociación o grupo, tampoco debe depender del número de certificaciones ya emitidas.

Nota: Cualquier caso que ponga en riesgo la imparcialidad de la ECD GSE como ECD o de su personal, organismo u organización, se pondrá en conocimiento del Proceso del Sistema Integrado de Gestión.

De acuerdo con lo establecido en la Política de Imparcialidad y No discriminación de la ECD de GSE, la cual se encuentra en el siguiente enlace: https://gse.com.co/wp-content/uploads/2021/03/Politica-de-imparcialidad.pdf

12. TARIFAS DEL SERVICIO DE EMISIÓN DE CERTIFICADOS DIGITALES

12.1.1. 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 Perteneciente a empresa	Normal	1	$ 191.597	$ 36.403	$ 228.000
Certificado Perteneciente 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
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.

13. MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES

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

14. PERFIL DE LOS CERTIFICADOS

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

OID (Object Identifier)	1.3.6.1.4.1.31136.1.4.11
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politicas_de_Certificado_para_Certificados_Digitales_V11.pdf