

# POLÍTICAS DE CERTIFICADO PARA CERTIFICADOS DIGITALES

| Código | Nombre | Versión | Clasificación de la información |
|---|---|---|---|
| POP-PL-55 | **Políticas de Certificado para Servicio de Certificados Digitales** | 19 | Pública |

| | |
|---|---|
| **Título del Documento** | **Políticas de Certificado para Servicio de Certificados Digitales** |
| **Versión** | 19 |
| **Grupo de Trabajo** | Comité de Gerencia |
| **Estado del documento** | Final |
| **Fecha de emisión** | 15/02/2010 |
| **Fecha de inicio de vigencia** | 28/10/2026 |
| **OID (Object Identifier)** | 1.3.6.1.4.1.31136.1.4.19 |
| **Ubicación de la Política** | https://gse.com.co/documentos/calidad/politicas/Politica_de_certificado_para_certificados_digitales_V19.pdf |
| **Elaboró** | Project & Operations Manager |
| **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 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 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.<br>Se actualizaron los links para que apunten a las nuevas rutas.<br>Se actualizaron los siguientes numerales:<br>• 7.6. Requerimiento específico tramitación del certificado |
| 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<br>7.7. Requisitos específicos tramitación del certificado<br>8.1.1 Se modificó la imagen de los dispositivos criptográficos<br>Se incluyeron los numerales:<br>7.6 Prohibiciones de Uso de los Certificados<br>8.1.2 Compromisos de seguridad<br>8.1.3 Cuidados del dispositivo criptográfico |

| | | |
|---|---|---|
| | | 8.1.4 Riesgos asociados.<br>7.9.3. Características Técnicas de los Certificados Digitales<br>10. Protección de la información personal<br>11. Imparcialidad y no discriminación<br>Se actualiza el OID y el link de consulta de la política. |
| 11 | 27/10/2021 | • Se modificó el numeral 7.7 Requisitos Específicos Tramitación del Certificado incluyendo en la sección final de Nota una aclaración sobre el RUT actualizado de la DIAN el cual debe tener el código QR.<br>• Se ajustó el OID y el link de la PC |
| 12 | 31/05/2022 | De acuerdo con la nueva versión del CEA se hicieron los siguientes ajustes:<br><br>• 4.4 Peticiones, Quejas, Reclamos y Solicitudes: Se eliminó el término Apelación.<br>• 5.2 Contenido de los Certificados: Se eliminó el certificado de firma centralizada.<br>• 6. Tipos de Certificados: Se modificó el objeto del certificado de persona jurídica.<br>• 7.4. Usos de los certificados: Se modificó el atributo del certificado de persona jurídica.<br>• 7.7. Requisitos técnicos tramitación del certificado: Se modificó la descripción de la documentación de solicitud del certificado de facturación electrónica y el certificado persona jurídica.<br>• 7.9. Actividades y referencias técnicas: Se modificaron las actividades y los documentos normativos de cada uno de los tipos de certificados de acuerdo con el certificado de acreditación con ONAC.<br>• 9.1.6. Obligaciones de otros participantes de la ECD: Se modificó el ítem r) dejando únicamente CEA eliminando el 4.1-10.<br>• Se ajustó el OID y el link de consulta de la Política.<br>• Se le incluyó el código de calidad en el encabezado del documento |
| 13 | 23/09/2022 | • Se modificó el numeral 3.1 Resumen incluyendo los capítulos del DURSCIT.<br>• Se modificó la dirección de la ECD en los numerales 3.1 y 4.4.<br>• Se modificó la dirección de Paynet SAS en el numeral 3.1.<br>• Se modificó el ITU X509 de 2016 al ITU X509 octubre de 2019 en los estándares de cada servicio acreditado en el numeral 7.9 al igual que se eliminaron los estándares ITU –T-X.500 octubre 2019 y FIPS PUB 186-4 Julio 2013<br>• Se modificó el numeral 9.1.1 incluyendo los ítems o) a la y).<br>• Se incluyeron los numerales 13 al 16.<br>• Se modificó el numeral 7.7 de representante legal incluyéndole un párrafo en la documentación solicitada.<br>• Se ajustó el OID y el link de consulta de la Política |
| 14 | 16/05/2023 | • Se modificó todo el orden del documento de acuerdo con los numerales del RFC 3647.<br>• Se eliminó a Paynet SAS como la autoridad CA ya |

| | | |
|---|---|---|
| | | que se trasladó la PKI a la ECD de GSE.<br>• Se ajustó el numeral 1.3.8.4 el responsable de las PQRS quedando Servicio al Cliente.<br>• Se modificó al Director de Operaciones por el Gerente de Operaciones<br>• Se modificaron los datos de los datacenter principal y alterno quedando Hostdime y Claro.<br>• Se actualizó el OID y el link de consulta de la Política<br>• Se ajustó el numeral 1.9.1 en tipo de certificado digital (Persona) el registro solicitado. |
| 15 | 23/10/2023 | • Se modificó el numeral 1.3.8.1 cambios en el Comité de Gerencia: Se cita el reglamento de comité de gerencia.<br>• Se modificó el numeral 1.9.1 Solicitud de certificado<br>• 1.14.11.2 Obligaciones de la RA: Se actualiza los literales C y E<br>• Se modificó el numeral 6 Perfil de los certificados: Se actualizó el OID y el link de consulta de la Política |
| 16 | 08/07/2024 | • Se actualiza la numeración y orden de acuerdo con el numeral 6 Esquema de un conjunto de disposiciones del RFC 3647<br>• Se actualizó el OID y el link de consulta de la Política |
| 17 | 22/10/2025 | •**Características de los dispositivos criptográficos**: Se incluye **FIPS 140-2 Nivel 3 o superior**.<br>•**Características técnicas de los certificados digitales**:<br>Se mantiene la **generación de claves**.<br>Se ajusta a **HSM**: FIPS 140-2 Nivel 3 o superior (Firma Centralizada).<br>Se ajustó plantilla del documento.<br>Se ajusta el cargo Gerente de Operaciones a Coordinador de Operaciones |
| 18 | 09/12/2025 | 1.3.1 Autoridad de Certificación (CA).<br>Se actualiza la información asociada a los datacenter |
| 19 | 28/10/2026 | • Se ajustó el **apartado 1.3.1 – Jerarquía de las CA:** se ajusta la imagen suprimiendo "S.A.".<br>• Se ajustó el **canal de atención:** se incluye "Felicitaciones" en el ítem de PQRS.<br>• Se ajustaron los **apartados 1.5.2 y 1.5.4:** se reemplaza el cargo "Coordinador de Operaciones" por "Project & Operations Manager".<br>• Se ajustó el **apartado 4.1 – Solicitud del certificado:** se actualiza la tabla de información solicitada por tipo de certificado. |

# Tabla de contenido


Tabla de contenido

1. INTRODUCCIÓN

1.1 Descripción General

1.2. Nombre e identificación del documento

Criterio de Identificación de las Políticas (OID)

El contenido de los certificados, distinguiendo:

OID de las Políticas

Políticas asignadas a este documento.
1.3. Participantes PKI.
1.3.1. Autoridad de Certificación (CA).
Jerarquía de las CA.
1.3.2. Autoridad de Registro (RA).
1.3.3. Suscriptores.
1.3.4. Partes de Confianza.
Precauciones que deben observar los terceros:
Solicitante.
Entidad a la cual se encuentra vinculado el suscriptor o responsable.
1.3.5. Otros participantes.
Comité de Gerencia.
Proveedores de servicios.
Entidades de Certificación Digital Recíprocas.
Peticiones, Quejas, Reclamos, Solicitudes y Felicitaciones
1.4. Uso del Certificado.
1.4.1. Uso apropiado de los certificados
1.4.2. Uso prohibido de los certificados
Vigencia de los certificados
Tipos de certificados ECD GSE
1.5. Administración de Políticas.
1.5.1. Organización que administra el documento:
1.5.2. Contacto (Responsable de la ECD):
1.5.3. Persona que determina la idoneidad de la DPC para la póliza
1.5.4. Procedimientos de aprobación de la DPC.
Responsabilidades de publicación
1.6. Definiciones y acrónimos
Definiciones
Acrónimos
2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.
2.1. Repositorios.
2.2. Publicación de información sobre certificación.
2.3. Plazo o frecuencia de la publicación.
2.4. Controles de acceso a los repositorios.
3. IDENTIFICACIÓN Y AUTENTICACIÓN.
3.1. Nombres.
3.2. Validación inicial de identidad.
3.3. Identificación y Autenticación para renovación de llaves.
3.4. Identificación y autenticación para la solicitud de revocación.
4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS.

4.1. Solicitud de certificado.
Requisitos Genéricos
Requisitos Específicos
4.2. Procesamiento de solicitud de certificado.
4.3. Emisión del Certificado.
4.4. Aceptación del Certificado.
4.5. Uso de pares de llaves y certificados.
4.6. Renovación del Certificado.
4.7. Reúso de llave del certificado.
4.8. Modificación de Certificado.
4.9. Revocación y Suspensión del Certificado.
4.10. Servicios de Estado del Certificado.
4.11. Fin de la Suscripción.
4.12. Custodia y Recuperación de Llaves.
5. INSTALACIONES, GESTIÓN Y CONTROLES OPERACIONALES.
5.1. Controles de Seguridad Física.
5.2. Controles de Procedimiento.
5.3. Controles de personal.
5.4. Procedimientos de Registro de Auditoría.
5.5. Archivo de Registros.
5.6. Cambio de Llaves.
5.7. Compromiso y Recuperación de Desastres.
5.8. Cese de la CA o la RA.
6. CONTROLES TÉCNICOS DE SEGURIDAD.
6.1. Generación e Instalación de Pares de Llaves.
6.2. Protección de llave privada y controles de ingeniería de módulos criptográficos.
6.3. Otros Aspectos de la Gestión del Par de Llaves.
6.4. Datos de Activación.
6.5. Controles de Seguridad Informática.
6.6. Controles de Técnicos del Ciclo de Vida.
6.7. Controles de Seguridad de Red.
6.8. Estampado Cronológico.
7. PERFILES DE CERTIFICADO, CRL Y OCSP.
7.1. Perfil del Certificado.
7.2. Perfil de CRL.
7.3. Perfil OCSP.
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.
8.1. Frecuencia o Circunstancias de la Evaluación.
8.2. Identidad y cualificaciones del evaluador.
8.3. Relación del evaluador con la entidad evaluada.

8.4. Temas objeto de evaluación.
8.5. Acciones tomadas como resultado de la deficiencia.
8.6. Comunicación de Resultados.
9. OTROS ASUNTOS COMERCIALES Y LEGALES.
9.1. Honorarios.
9.2. Responsabilidad Financiera.
9.3. Confidencialidad de la Información Comercial.
9.4. Privacidad de la Información Personal.
9.5. Derechos de Propiedad Intelectual.
9.6. Representaciones y Garantías.
9.7. Renuncias de Garantías.
9.8. Limitaciones de Responsabilidad.
9.9. Indemnizaciones.
9.10. Duración y Terminación.
9.11. Notificaciones y comunicaciones individuales a los participantes.
9.11.1. Obligaciones de la ECD GSE
9.11.2. Obligaciones de la RA
9.11.3. Obligaciones (Deberes y Derechos) del Suscriptor y/o Responsable
9.11.4. Obligaciones de los Terceros de buena fe
9.11.5. Obligaciones de la Entidad (Cliente)
9.11.6. Obligaciones de otros participantes de la ECD
9.12. Enmiendas.
9.13. Disposiciones sobre resolución de disputas.
9.14. Legislación aplicable.
9.15. Cumplimiento de la legislación aplicable
9.16. Disposiciones varias.
9.17. Otras Disposiciones.
10. CARACTERÍSTICAS DE LOS DISPOSITIVOS CRIPTOGRÁFICOS
10.1. Certificado Digital en Token
*10.2. Características*
*10.3. Compromisos de seguridad*
*10.4. Cuidados del dispositivo criptográfico*
*10.5. Riesgos asociados*
10.6. Certificado Digital en HSM – Hardware Security Module (Firma Centralizada)
*10.7. Características Técnicas de los Certificados Digitales*
10.8. TARIFAS DEL SERVICIO DE EMISIÓN DE CERTIFICADOS DIGITALES
10.9. IMPARCIALIDAD Y NO DISCRIMINACIÓN
10.10. MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES
10.11. PERFIL DE LOS CERTIFICADOS

# 1. INTRODUCCIÓN

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

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

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

## 1.1 Descripción General

**Política para Certificado de Certificados Digitales** , en adelante **Política** es un documento elaborado por **Gestión de Seguridad Electrónica (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 con lo establecido en la Ley 527 de 1999, el Decreto Ley 0019 de 2012, el Decreto 333 de 2014, el Decreto 1471 de 2014, los capítulos 47 y 48 del título 2 de la parte 2 del libro 2 del Decreto Único del Sector Comercio, Industria y Turismo – DURSCIT 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 |
| **Sigla:** | GSE |
| **Número de Identificación Tributaria:** | 900.204.272 – 8 |
| **Registro Mercantil No:**<br>**Certificado de Existencia y Representante Legal:** | 01779392 de 28 de febrero de 2008<br>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 77 No. 7 – 44 Oficina 701 |
| **Ciudad / País:** | Bogotá D.C., Colombia |
| **Teléfono:** | +57 (601) 4050082 |
| **Correo electrónico:**<br>**Página Web:** | info@gse.com.co<br>www.gse.com.co |

## 1.2. Nombre e identificación del documento

### 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). 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 a su vez, partiendo de este certificado de ECD GSE se definen diferentes subtipos en función de algunas características específicas, como son:

### 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 Persona Jurídica
- de Factura Electrónica

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

El procedimiento para realizar la actualización de la información contenida en los certificados se debe ejecutar de acuerdo con lo establecido en la DPC “Renovación del certificado con cambio de llaves”, para realizar la renovación de certificados digitales se debe ejecutar el procedimiento de solicitud de un certificado nuevo. El suscriptor debe acceder al portal web de solicitud de productos y servicios de GSE e iniciar el proceso de solicitud de renovación del certificado de la misma forma que lo hizo cuando solicitó el certificado por primera vez. Su información será nuevamente validada con el fin de actualizar datos si se requiere.

### OID de las Políticas

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

| OID | DESCRIPCIÓN |
|---|---|
| 1.3.6.1.4.1.31136.1.4.19 | Política de Certificados para Certificados Digitales |

## 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-PJ
- GSE-FE

## 1.3. Participantes PKI.

### 1.3.1. Autoridad de Certificación (CA).

Es aquella persona jurídica, acreditada conforme a la ley 527 de 1999 y el Decreto 333 de 2014, facultada por el Gobierno colombiano o el Organismo Nacional de Acreditación en Colombia para prestar servicios de certificación digital de acuerdo con 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, es el origen de la jerarquía de certificación digital que le permite prestar los servicios relativos a las comunicaciones basadas en infraestructuras de clave pública.

### Jerarquía de las CA.

La jerarquía de certificación de GSE está compuesta por las siguientes Autoridades Certificadoras (CA):




GSE tiene dos datacenter, el datacenter (Activo) con Sencinet Latam Colombia S.A ICD Nimbus, ubicado en la Carrera 106 No. 15A25 Manzana 4 Lote 38 Zona Franca, Bogotá, Colombia y el Datacenter (Activo) con Claro se encuentra ubicado en la Autopista Medellín Km 7.5 Celta Trade Park – Datacenter Triara, Cota, Cundinamarca, Colombia.

### 1.3.2. Autoridad de Registro (RA).

Es el área de GSE encargada de certificar la validez de la información suministrada por el solicitante de un servicio de certificación digital, mediante la verificación de la entidad del suscriptor o responsable de los servicios de certificación digital, en la RA se decide sobre la emisión o activación del servicio de certificación digital. Para ello, tiene definidos los criterios y métodos de evaluación de solicitudes.

Bajo esta DPC, la figura de RA hace parte de la propia ECD y podrá actuar como Subordinada de ECD GSE.

GSE en ninguna circunstancia delega las funciones de Autoridad de Registro (RA).

### 1.3.3. Suscriptores.

Suscriptor es la persona natural a la cual se emiten o activan los servicios de certificación digital y por tanto actúa como suscriptor o responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC.

La figura de Suscriptor será diferente dependiendo de los servicios prestados por la ECD GSE conforme lo establecido en las Políticas de Certificado para certificados digitales.

### 1.3.4. Partes de Confianza.

Responsable es la persona natural a la cual se activan los servicios de certificación digital de una persona jurídica y por tanto actúa como responsable de este confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC.

La figura de responsable será diferente dependiendo de los servicios prestados por la ECD GSE conforme lo establecido en el Anexo 1 de esta DPC.

### Precauciones que deben observar los terceros:

1. Verificar el alcance del certificado en la política de certificación asociada.
2. Consulte la normatividad asociada a los servicios de certificación digital
3. Verificar el estatus de acreditación de la ECD ante ONAC.
4. Verificar que la firma digital se generó correctamente.
5. Verificar el origen del certificado (Cadena de certificación)
6. Verificar su conformidad con el contenido del certificado.
7. Verificar la integridad de un documento firmado digitalmente.

### Solicitante.

Se entenderá por Solicitante, la persona natural o jurídica interesada en los servicios de certificación digital emitidos bajo esta DPC. Puede coincidir con la figura del Suscriptor.

### Entidad a la cual se encuentra vinculado el suscriptor o responsable.

En su caso, la persona jurídica u organización a la que el suscriptor o responsable se encuentra estrechamente relacionado mediante la vinculación acreditada en el servicio de certificación digital.

## 1.3.5. Otros participantes.

### Comité de Gerencia.

El comité de Gerencia es un organismo interno de ECD GSE, que está conformado de acuerdo con el reglamento del comité de gerencia quienes tienen la responsabilidad de la aprobación de la DPC como documento inicial, así como autorizar los cambios o modificaciones requeridas sobre la DPC aprobada y autorizar su publicación.

### Proveedores de servicios.

Los proveedores de servicios son terceros que prestan infraestructura o servicios tecnológicos a ECD GSE, cuando GSE así lo requiere y garantiza la continuidad del servicio a los suscriptores, entidades durante todo el tiempo en que se hayan contratado los servicios de certificación digital.

### Entidades de Certificación Digital Recíprocas.

De acuerdo con lo previsto en el artículo 43 de la Ley 527 de 1999, los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

Actualmente ECD GSE no cuenta con acuerdos vigentes de reciprocidad.

### Peticiones, Quejas, Reclamos, Solicitudes y Felicitaciones

Las peticiones, quejas, reclamos, solicitudes y felicitaciones 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 77 No. 7 – 44 Oficina 701

**Página Web:** www.gse.com.co

**Responsable:** Servicio al Cliente

Una vez presentado el caso, este es transmitido con la información concerniente al proceso del Servicio al Cliente 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 PQRS y su comunicación final al suscriptor, responsable o parte interesada.

## 1.4. Uso del 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 y/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 DIGITAL | ÁMBITO USOS Y APLICACIONES |
|---|---|
| **Pertenencia a Empresa** | Realización de trámites empresariales por parte del suscriptor y/o responsable sin que implique representación. La empresa puede establecer limitaciones de uso. |
| **Representación Empresa** | Realización de trámites empresariales por parte del suscriptor y/o responsable en nombre y representación de la empresa. La empresa puede establecer limitación de uso. |
| **Función Pública** | Realización de trámites por parte del suscriptor y/o responsable en el ejercicio de sus funciones como funcionario público. La Administración Pública puede establecer limitaciones de uso. |
| **Profesional Titulado** | Realización de trámites por parte del suscriptor y/o responsable en el ejercicio de sus funciones como profesional colegiado. |
| **Persona Natural** | Realización de trámites por parte del suscriptor y/o responsable en su calidad de ciudadano. No existe vinculación alguna con ninguna entidad. |
| **Factura Electrónica** | Realización por parte del suscriptor y/o responsable de facturación y/o nómina electrónica |
| **Persona Jurídica** | Realización de trámites empresariales por parte de una aplicación ejecutándose en una máquina en procesos de firma automáticos y/o 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 y que será representada por medio de una persona responsable del certificado emitido.<br>El uso de este certificado está permitido dentro de plataformas desatendidas una vez se haya surtido el estudio de la gestión del riesgo con respecto al manejo de las llaves criptográficas. |

## 1.4.1. Uso apropiado de los certificados

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 1.4.2. Uso prohibido 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 “Límites 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.

### Vigencia de los certificados

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

### 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 DIGITAL | OBJETO |
|---|---|
| **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. |
| **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. |
| **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. |
| **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 |

| TIPO DE CERTIFICADO DIGITAL | OBJETO |
|---|---|
| | titular que las que posee por el desempeño de su actividad habitual en el ámbito de su profesión. |
| **Persona Natural** | Garantiza únicamente la identidad de la Persona natural. |
| **Factura Electrónica** | Certificado exclusivo para facturación electrónica atendiendo a la necesidad de las empresas y/o personas naturales que buscan la seguridad del certificado para la emisión de facturas electrónicas.<br><br>Certificado exclusivo para la firma digital de facturas electrónicas, notas crédito, notas débito, soportes de pago de nómina electrónica, notas de ajuste del documento soporte de pago de nómina electrónica y otros documentos producto de los procesos de las plataformas desatendidas de los proveedores tecnológicos aprobados por la DIAN, el sistema de facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad. |
| **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 y que será representada por medio de una persona responsable del certificado emitido. |

## 1.5. Administración de Políticas.

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

## 1.5.1. Organización que administra el documento:

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 1.5.2. Contacto (Responsable de la ECD):

| | |
|---|---|
| **Cargo del contacto:** | Project & Operations Manager |
| **Teléfonos de contacto:** | 4050082 |
| **Correo electrónico:** | info@gse.com.co |

## 1.5.3. Persona que determina la idoneidad de la DPC para la póliza

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 1.5.4. Procedimientos de aprobación de la DPC.

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

### Responsabilidades de publicación

Una vez realizados y aprobados los cambios de las políticas, es responsabilidad del Project & Operations Manager 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.

## 1.6. Definiciones y acrónimos

### Definiciones

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

**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.

**Autoridad de Estampado de Tiempo (TSA):** Sigla en inglés de "Time Stamping Authority": Entidad de certificación prestadora de servicios de estampado cronológico

**Archivo confiable de datos:** Es el servicio que GSE ofrece a sus clientes por medio de una plataforma tecnológica. En esencia, consiste en un espacio de almacenamiento seguro y encriptado al cual se accede con credenciales o con un certificado digital. La documentación que se almacene en esta plataforma tendrá valor probatorio siempre y cuando esté firmada digitalmente.

**Certificado digital:** Un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Esta es la definición de la Ley 527/1999 que en este documento se extiende a los casos en que la vinculación de los datos de verificación de firma se hace a un componente informático.

**Criterios Específicos de Acreditación (CEA):** Requisitos que deben ser cumplidos para obtener la Acreditación como Entidad de Certificación Digital - ECD, ante el Organismo Nacional de Acreditación de Colombia – ONAC; es decir para prestar servicios de certificación digital de acuerdo con lo establecido en la Ley 527 de 1999, el Decreto Ley 019 de 2012, los capítulos 47 y 48 del título 2 de la parte 2 del libro 2 del Decreto Único del Sector Comercio, Industria y Turismo – DURSCIT y los reglamentos que los modifiquen o complementen.

**Clave Personal de Acceso (PIN):** Sigla en inglés de "Personal Identification Number": Secuencia de caracteres que permiten el acceso al certificado digital.

**Compromiso de la llave privada:** entiéndase por compromiso el robo, pérdida, destrucción o divulgación de la llave privada que pueda poner en riesgo el empleo y uso del certificado por parte de terceros no autorizados o el sistema de certificación.

**Correo electrónico certificado:** Servicio que permite asegurar el envío, recepción y comprobación de comunicaciones electrónicas, asegurándose en todo momento las características de fidelidad, autoría, trazabilidad y no repudio de la misma.

**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.

**Estampado cronológico:** Según el numeral 7 del Artículo 3° del Decreto 333 de 2014, se define como: Mensaje de datos con un momento o periodo de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en un momento o periodo de tiempo y que no sufrieron ninguna modificación a partir del momento que se realizó el estampado.

**Entidad de Certificación:** 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 una Entidad Certificación que ofrece servicios propios de las entidades de certificación, tales que:

1. Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, o
2. Recibe remuneración por estos.

**Entidad de certificación cerrada:** Entidad que ofrece servicios propios de las entidades de certificación solo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello.

**Infraestructura de Llave Pública (PKI):** Sigla en inglés de "Public Key Infrastructure": una PKI es una combinación de hardware y software, políticas y procedimientos de seguridad que permite, a los usuarios de una red pública básicamente insegura como el Internet, el intercambio de mensajes de datos de una manera segura utilizando un par de llaves criptográficas (una privada y una pública) que se obtienen y son compartidas a través de una autoridad de confianza.

**Iniciador:** Persona que, actuando por su cuenta, o en cuyo nombre se haya actuado, envíe o genere un mensaje de datos.

**Jerarquía de confianza:** Conjunto de autoridades de certificación que mantienen relaciones de confianza por las cuales una ECD de nivel superior garantiza la confiabilidad de una o varias de nivel inferior.

**Lista de Certificados Revocados (CRL):** Sigla en inglés de "Certificate Revocation List": Lista donde figuran exclusivamente los certificados revocados no vencidos.

**Llave Pública y Llave Privada:** La criptografía asimétrica en la que se basa la PKI. Emplea un par de llaves en la que se cifra con una y solo se puede descifrar con la otra y viceversa. A una de esas llaves se la denomina pública y se incluye en el certificado digital, mientras que a la otra se denomina privada y es conocida únicamente por el suscriptor o responsable del certificado.

**Llave privada (Clave privada):** Valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.

**Llave pública (Clave pública):** Valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada de quien actúa como iniciador.

**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.

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

**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.

**Protocolo de Estado de los Certificados en línea:** En inglés "Online Certificate Status Protocol" (OCSP): Protocolo que permite verificar en línea el estado de un certificado digital

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

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

**Solicitante:** Toda persona natural o jurídica que solicita 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 suscriptor y/o responsable que decide aceptar y confiar en un certificado digital emitido por ECD GSE.

**TSA GSE:** Corresponde al término utilizado por ECD GSE, en la prestación de su servicio de Estampado cronológico, como Autoridad de Estampado Cronológico.

## 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

# 2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.

## 2.1. Repositorios.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 2.2. Publicación de información sobre certificación.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 2.3. Plazo o frecuencia de la publicación.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 2.4. Controles de acceso a los repositorios.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

# 3. IDENTIFICACIÓN Y AUTENTICACIÓN.

## 3.1. Nombres.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 3.2. Validación inicial de identidad.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 3.3. Identificación y Autenticación para renovación de llaves.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 3.4. Identificación y autenticación para la solicitud de revocación.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

# 4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS CERTIFICADOS.

## 4.1. Solicitud de certificado.

Cualquier persona que requiera la prestación del servicio de certificación digital, lo podrá hacer utilizando los canales, medios o mecanismos dispuestos por GSE, en los que se obtendrá la información necesaria para gestionar la solicitud del servicio de certificación digital requerido, aceptando el documento términos y condiciones de la ECD.

| TIPO DE CERTIFICADO DIGITAL | REGISTRO: INFORMACIÓN SOLICITADA |
|---|---|
| Para todo tipo de certificado se solicitará la siguiente información:<br><br>· Formulario de la solicitud diligenciado.<br>· Aceptación de términos y condiciones.<br>· Aceptación de Tratamiento de datos.<br>· Documento y/o información que certifique la identificación del solicitante. | |
| **Pertenencia Empresa** | · Documento de Identificación.<br>· Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) días.<br>· Certificado laboral del solicitante incluyendo el cargo en papel institucional (no mayor a treinta (30) días).<br>· Registro Único Tributario – RUT. |
| **Representación Empresa** | · Documento de Identificación.<br>· Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) días.<br>· Registro Único Tributario – RUT<br><br>Para el caso en que la solicitud sea delegada por el Representante Legal y/o Suplente a un tercero debe adjuntar la carta de delegación para la solicitud del certificado digital.<br>Si el solicitante no cuenta con el documento de existencia y representación legal y es una entidad pública o estatal se solicitará la información y/o los documentos equivalentes en los que se pueda validar la creación de la entidad de acuerdo con la normativa vigente y el respectivo acto administrativo (ley, decreto, resolución, entre otros). |
| **Función Pública** | · Para confirmar la información de relación del solicitante con la Empresa se solicitará alguno de los siguientes documentos:<br>Ø Acta de posesión. |

| TIPO DE CERTIFICADO DIGITAL | REGISTRO: INFORMACIÓN SOLICITADA |
|---|---|
| | Ø Resolución de nombramiento o decreto.<br>Ø Contrato de prestación de servicios.<br>Ø Certificado laboral del solicitante incluyendo el cargo en papel institucional (no mayor a treinta (30) días desde la radicación de la solicitud).<br>· Cédula de Ciudadanía<br>· Registro Único Tributario – RUT |
| **Profesional Titulado** | · Cédula de Ciudadanía<br>· Registro Único Tributario – RUT<br>· Información de domicilio del solicitante<br>· Tarjeta Profesional y/o documento equivalente.<br>· Diploma de grado (opcional)<br>· Acta de grado |
| **Persona Natural** | · Cédula de ciudadanía<br>· Información de domicilio del solicitante<br>· El documento Registro Único Tributario – RUT se solicitará en el formato actualizado de DIAN que incluye código QR (si aplica; opcional).<br>Para el caso en que la solicitud del servicio de certificación digital sea generada desde una fuente o un tercero confiable ejemplo la Registraduría Nacional del Estado Civil, no se solicitará información y/o documentación adicional siempre y cuando la información venga firmada por la misma entidad y subsista contrato, convenio, acuerdo, alianza, y/o cualquier medio de relación contractual y/o comercial, directa y/o indirecta |
| **Factura Electrónica** | Persona Natural<br>· Cédula de ciudadanía<br>· Carta de representación para menores de edad (de 14 a 17 años)<br>·Información de domicilio del solicitante.<br><br>Para el caso en que la solicitud sea delegada por el Representante Legal y/o Suplente a un tercero debe adjuntar la carta de delegación para la solicitud del certificado digital. |
| | Persona Jurídica<br>· Registro Único Tributario – RUT Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) días.<br><br>Si el solicitante no cuenta con el documento de existencia y representación legal y es una entidad pública o estatal se solicitará la información y/o los documentos equivalentes en los que se pueda validar la creación de la entidad de acuerdo con la normatividad vigente y el respectivo acto administrativo (ley, decreto, resolución, entre otros).<br><br>Para el caso en que la solicitud sea delegada por el Representante Legal y/o Suplente a un tercero debe adjuntar la carta de delegación para la solicitud del certificado digital.<br><br>Para los menores de edad de catorce (14) años o menos, se deberá presentar una carta de representación que acredite la autorización del representante legal para realizar la solicitud del servicio. |
| **Persona Jurídica** | · Documento de Identidad<br>· Documento de Existencia y Representación Legal de la Empresa con vigencia no mayor a treinta (30) días.<br>· Registro Único Tributario – RUT |

| TIPO DE CERTIFICADO DIGITAL | REGISTRO: INFORMACIÓN SOLICITADA |
|---|---|
| | Si el solicitante no cuenta con el documento de existencia y representación legal y es una entidad pública o estatal se solicitará la información y/o los documentos equivalentes en los que se pueda validar la creación de la entidad de acuerdo con la normativa vigente y el respectivo acto administrativo (ley, decreto, resolución, entre otros).<br>Para el caso en que la solicitud sea delegada por el Representante Legal y/o Suplente a un tercero debe adjuntar la carta de delegación para la solicitud del certificado digital. |
| **Notas:**<br>· Los documentos cuando aplique se recibirán escaneados o en original electrónico, preservando la legibilidad para el uso de la información.<br>· El documento Registro Único Tributario – RUT cuando aplique, se solicitará en el formato actualizado de DIAN que incluye código QR.<br>· En caso de que el solicitante no tenga Registro Único Tributario – RUT (cuando aplique) debe presentar un documento donde se registre la información de domicilio que sea expedido por un tercero que lo verifique o la información de domicilio será consultada por la ECD GSE consumiendo servicio de datos de fuentes externas.<br>· 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.<br>· 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 autenticado.<br>· Todo documento que se reciba autenticado, la autenticación debe tener una vigencia no mayor a sesenta (60) días desde la radicación de la solicitud.<br>· En los casos que se presenten solicitudes de certificados digitales con documentos adicionales y/o equivalentes a la documentación y/o información solicitada, se tendrá en cuenta para la revisión de las solicitudes los documentos mencionados en el Anexo Documental de Validación de Solicitudes publicado en la página web en la sección Soporte-Guías y Manuales-Validación de Solicitudes. | |

La ECD-GSE cuenta con un sistema de gestión de seguridad para proteger la información que se recopila con el fin de expedir los certificados el cual está establecido en la DPC en “Controles de seguridad informática”.

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 emitidos o cualquier otra que discrimine el acceso a la solicitud del servicio prestado por ECD GSE.

## Requisitos Genéricos

Es 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 Solicitante, Suscriptor y/o Responsable, 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.

## Requisitos Específicos

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 de la solicitud y decisión conforme con el alcance de acreditación otorgado por ONAC.

| TIPO DE CERTIFICADO DIGITAL | SUSCRIPTOR / RESPONSABLE | ATRIBUTO | ENTIDAD |
|---|---|---|---|
| **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 vinculado el Suscriptor |
| **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 |
| **Función Pública** | Persona natural que pertenece a una Administración Pública y que es titular del certificado | Vinculación funcionarial respecto a una Administración Pública | Administración Pública a la que está vinculado el Suscriptor |
| **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 vinculado el Suscriptor |
| **Persona Natural** | Persona natural titular del certificado | No aplica | No aplica |
| **Factura Electrónica** | Garantiza únicamente la identidad del suscriptor y/o responsable | Vinculación para la realización de facturación y/o nómina electrónica | Suscriptor y/o responsable que requiere realizar facturación y/o nómina electrónica |
| **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 y/o responsable. |

## 4.2. Procesamiento de solicitud de certificado.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 4.3. Emisión del Certificado.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 4.4. Aceptación del Certificado.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 4.5. Uso de pares de llaves y certificados.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 4.6. Renovación del Certificado.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 4.7. Reúso de llave del certificado.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 4.8. Modificación de Certificado.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 4.9. Revocación y Suspensión del Certificado.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 4.10. Servicios de Estado del Certificado.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 4.11. Fin de la Suscripción.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 4.12. Custodia y Recuperación de Llaves.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 5. INSTALACIONES, GESTIÓN Y CONTROLES OPERACIONALES.

### 5.1. Controles de Seguridad Física.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 5.2. Controles de Procedimiento.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 5.3. Controles de personal.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 5.4. Procedimientos de Registro de Auditoría.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 5.5. Archivo de Registros.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 5.6. Cambio de Llaves.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 5.7. Compromiso y Recuperación de Desastres.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 5.8. Cese de la CA o la RA.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 6. CONTROLES TÉCNICOS DE SEGURIDAD.

### 6.1. Generación e Instalación de Pares de Llaves.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 6.2. Protección de llave privada y controles de ingeniería de módulos criptográficos.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 6.3. Otros Aspectos de la Gestión del Par de Llaves.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 6.4. Datos de Activación.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 6.5. Controles de Seguridad Informática.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 6.6. Controles de Técnicos del Ciclo de Vida.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 6.7. Controles de Seguridad de Red.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 6.8. Estampado Cronológico.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 7. PERFILES DE CERTIFICADO, CRL Y OCSP.

### 7.1. Perfil del Certificado.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 7.2. Perfil de CRL.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

### 7.3. Perfil OCSP.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

# 8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

## 8.1. Frecuencia o Circunstancias de la Evaluación.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 8.2. Identidad y cualificaciones del evaluador.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 8.3. Relación del evaluador con la entidad evaluada.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 8.4. Temas objeto de evaluación.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 8.5. Acciones tomadas como resultado de la deficiencia.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 8.6. Comunicación de Resultados.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

# 9. OTROS ASUNTOS COMERCIALES Y LEGALES.

## 9.1. Honorarios.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.2. Responsabilidad Financiera.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.3. Confidencialidad de la Información Comercial.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.4. Privacidad de la Información Personal.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.5. Derechos de Propiedad Intelectual.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.6. Representaciones y Garantías.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.7. Renuncias de Garantías.

No Aplica

## 9.8. Limitaciones de Responsabilidad.

Las limitaciones de Responsabilidad de la Entidad de Certificación Abierta están definidas de manera integral en el numeral Límites 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 PC.

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 DIGITAL | LÍMITE DE RESPONSABILIDAD DE LA ENTIDAD DE CERTIFICACIÓN |
|---|---|
| **Pertenencia a Empresa, representación empresa, Función Pública, Profesional Titulado, Profesional Titulado, Persona Natural, Factura Electrónica, Persona Jurídica** | 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.<br>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 uso 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 Límites de Responsabilidad de la entidad de certificación abierta. |

## 9.9. Indemnizaciones.

No Aplica

## 9.10. Duración y Terminación.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.11. Notificaciones y comunicaciones individuales a los participantes.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.11.1. 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 digitales emitidos de conformidad con la normatividad vigente.
9. Emitir certificados cuyo contenido mínimo esté de conformidad con la normativa vigente para los diferentes tipos de certificados.

10. Publicar el estado de los certificados digitales emitidos en un repositorio de acceso libre.
11. No mantener copia de la llave privada del solicitante o suscriptor.
12. Revocar los certificados digitales según lo dispuesto en la Política de revocación de certificados digitales.
13. Actualizar y publicar la lista de certificados digitales 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 digital de conformidad con la política de revocación de certificados digitales.
15. Informar a los suscriptores la proximidad del vencimiento de su certificado digital.
16. Disponer de personal calificado, con el conocimiento y experiencia necesaria para la prestación del servicio de certificación ofrecido por la ECD GSE.
17. Proporcionar al solicitante en la página web de la ECD GSE la siguiente información de manera gratuita y acceso libre:
    - Las Políticas y Declaración de Prácticas de certificación y todas sus actualizaciones.
    - Obligaciones del suscriptor y la forma en que han de custodiarse los datos
    - Procedimiento para solicitar la emisión de certificado.
    - El procedimiento de revocación de su certificado.
    - Mecanismos para garantizar la fiabilidad de la firma electrónica a lo largo del tiempo.
    - Las condiciones y límites del uso del certificado
18. Comprobar por sí o por medio de una persona diferente que actúe en nombre y por cuenta suya, la identidad y cualesquiera otras circunstancias de los solicitantes o de datos de los certificados, que sean relevantes para los fines propios del procedimiento de verificación previo a su expedición.
19. Informar a la Superintendencia de Industria y Comercio y al ONAC, de manera inmediata, la ocurrencia de cualquier evento que comprometa o pueda comprometer la prestación del servicio.
20. Informar oportunamente la modificación o actualización de servicios incluidos en el alcance de su acreditación, en los términos que establezcan los procedimientos, reglas y requisitos del servicio de acreditación del ONAC
21. Actualizar la información de contacto cada vez que haya cambio o modificación en los datos suministrados.
22. Capacitar y advertir a sus usuarios sobre las medidas de seguridad que deben observar y sobre la logística que se requiere para la utilización de los mecanismos de la prestación del servicio.
23. Garantizar la protección, integridad, confidencialidad y seguridad de la información suministrada por el suscriptor conservando la documentación que respalda los certificados emitidos.
24. Garantizar las condiciones de integridad, disponibilidad, confidencialidad y seguridad, de acuerdo con los estándares técnicos nacionales e internacionales vigentes y con los criterios específicos de acreditación que para el efecto establezca el ONAC.
25. Disponer en la página web de la ECD GSE los servicios que se encuentran acreditados.

## 9.11.2. 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. Revisar y/o comprobar los registros de validación inicial de la identidad de los Solicitantes, Responsables o Suscriptores de certificados digitales.
4. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante mediante los protocolos descritos en la DPC
5. Archivar y custodiar la información y/o documentación suministrada por el solicitante o suscriptor para la emisión del certificado digital, 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.

## 9.11.3. Obligaciones (Deberes y Derechos) del Suscriptor y/o Responsable

El Suscriptor y/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:

1. Usar su certificado digital según los términos de la DPC.
2. Verificar dentro del día siguiente hábil que la información del certificado digital es correcta. En caso de encontrar inconsistencias, notificar a la ECD.
3. Abstenerse de: prestar, ceder, escribir, publicar la contraseña de uso de su certificado digital y tomar todas las medidas necesarias, razonables y oportunas para evitar que este sea utilizado por terceras personas.
4. No transferir, compartir ni prestar el dispositivo criptográfico a terceras personas.
5. Suministrar toda la información requerida en el Formulario de la Solicitud para facilitar su oportuna y plena identificación.
6. Solicitar la revocación del Certificado Digital ante el cambio de nombre y/o apellidos.
7. Solicitar la revocación del Certificado Digital cuando el Suscriptor haya variado su nacionalidad.
8. Cumplir con lo aceptado y firmado en el documento términos y condiciones o responsable de certificados digitales.
9. Proporcionar con exactitud y veracidad la información requerida.
10. Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del certificado.
11. Custodiar y proteger de manera responsable su llave privada.
12. Dar uso al certificado de conformidad con lo establecido en esta PC para cada uno de los tipos de certificado.
13. 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.
14. No hacer uso de la llave privada ni del certificado digital una vez cumplida su vigencia o se encuentre revocado.
15. 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.
16. Informar al tercero de buena fe para verificar el estado de un certificado dispone de la lista de certificados revocados CRL, publicada de manera periódica por ECD GSE.
17. No utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para la ECD.
18. No realizar ninguna declaración relacionada con su certificación digital que la ECD GSE pueda considerar engañosa o no autorizada, conforme a lo dispuesto por la DPC y PC.

19. 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.
20. 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.
21. 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.

Por otro lado, tiene los siguientes derechos:

1. Recibir el certificado digital en los tiempos establecidos en la DPC.
2. 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.
3. Solicitar información referente a las solicitudes en proceso.
4. Solicitar revocación del certificado digital aportando la documentación necesaria.
5. Recibir el certificado digital de acuerdo con el alcance otorgado por ONAC a GSE.

## 9.11.4. 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 están en la obligación de:

1. Conocer lo dispuesto sobre Certificación Digital en la Normatividad vigente.
2. Conocer lo dispuesto en la DPC y PC.
3. Verificar el estado de los certificados antes de realizar operaciones con certificados digitales.
4. Verificar la Lista de certificados Revocados CRL antes de realizar operaciones con certificados digitales.
5. Conocer y aceptar las condiciones sobre garantías, usos y responsabilidades al realizar operaciones con certificados digitales.

## 9.11.5. 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:

1. Solicitar a la RA GSE la suspensión/revocación del certificado cuando cese o se modifique dicha vinculación.
2. Todas aquellas obligaciones vinculadas al responsable del servicio de certificación digital.
3. 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.
4. 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.

## 9.11.6. Obligaciones de otros participantes de la ECD

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

1. Revisar la consistencia de la DPC con la normatividad vigente.
2. 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.
3. Aprobar la notificación de cualquier cambio a los suscriptores y/o responsables analizando su impacto legal, técnico o comercial.
4. Revisar y tomar acciones sobre cualquier comentario realizado por suscriptores y/o responsables cuando un cambio en el servicio de certificación digital se realice.
5. 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 RAC-3.0-01.
6. Autorizar los cambios o modificaciones requeridas sobre la DPC.
7. Autorizar la publicación de la DPC en la página Web de la ECD GSE.
8. Aprobar los cambios o modificaciones a las Políticas de Seguridad de la ECD GSE.
9. Asegurar la integridad y disponibilidad de la información publicada en la página Web de la ECD GSE.
10. Asegurar la existencia de controles sobre la infraestructura tecnológica de la ECD GSE.
11. 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.
12. Conocer y tomar acciones pertinentes cuando se presenten incidentes de seguridad.
13. 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.
14. Revisar, aprobar y autorizar cambios sobre los servicios de certificación digital acreditados por el organismo competente.
15. 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.
16. Velar que las condiciones de acreditación otorgadas por el organismo competente se mantengan.
17. 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.
18. 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, en los numerales que correspondan.
19. 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.
20. 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.
21. Documentar y demostrar el compromiso de imparcialidad y no discriminación.

22. 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.
23. Velar por mantener informados a sus proveedores críticos como la ECD recíproca 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.

## 9.12. Enmiendas.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.13. Disposiciones sobre resolución de disputas.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.14. Legislación aplicable.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.15. Cumplimiento de la legislación aplicable

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.16. Disposiciones varias.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 9.17. Otras Disposiciones.

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

# 10. CARACTERÍSTICAS DE LOS DISPOSITIVOS CRIPTOGRÁFICOS

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

## 10.1. Certificado Digital en Token




## *10.2. Características*

| CARACTERÍSTICA | ESPECIFICACIÓN TÉCNICA |
|---|---|
| **Sistemas Operativos soportados** | 32bit and 64bit<br>Windows XP SP3, Vista, 7, 8, 10. Mac OS.<br>Server2003, Server2008, Server2008 R2, Server 2012 R2. |
| **Estándar** | X.509 Oct 2019, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID |

| CARACTERÍSTICA | ESPECIFICACIÓN TÉCNICA |
|---|---|
| **Funciones Criptográficas** | Generación de par de claves<br>Firma digital y verificación<br>Cifrado y descifrado de datos |
| **Soporte de Algoritmos** | RSA 512/1024/2048, DES, 3DES, SHA-1,<br>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<br>(32°F ~ 158°F) |
| **Humedad** | 0% ~ 100% sin condensación |
| **Temperatura de Almacenamiento** | -20°C ~ 85°C<br>(-4°F ~ 185°F) |
| **Peso Neto** | 8.1 gr |
| **Dimensiones** | 54.5×17×8.5 mm |

## *10.3. 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

## *10.4. Cuidados del dispositivo criptográfico*

- Mantenerlo en un lugar seco y alejado de las variaciones ambientales 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 ocasionará su mal funcionamiento.
- No introducirlo en agua u otros líquidos.
- Notificar a la ECD – GSE en caso de hurto, robo, pérdida y/o fraude del token con el fin de revocar el certificado digital.

## *10.5. Riesgos asociados*

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

- Pérdida 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 ambientales adecuadas.
- En caso de compromiso o pérdida de la llave privada debe solicitar la revocación del certificado digital.

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

| CARACTERÍSTICA | ESPECIFICACIÓN TÉCNICA |
|---|---|
| **Sistemas Operativos soportados** | 32bit and 64bit<br>· Windows XP SP3, Vista, 7, 8, 10.<br>· Server2003, Server2008, Server2008 R2, Server 2012 R2. |
| **Estándar** | · X.509 oct 2019, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID |
| **Funciones Criptográficas** | · Generación de par de claves<br>· Firma digital y verificación<br>· 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 |

## *10.7. Características Técnicas de los Certificados Digitales*

| CARACTERÍSTICA | ESPECIFICACIÓN TÉCNICA |
|---|---|
| Algoritmo de Firma | *Función Hash* SHA256 con RSA Encryption.<br>*Función Hash* SHA384 con ECDSA |
| | *Función de Cifrado*<br>RSA con longitud de clave de 4096 para CA RAÍZ<br>RSA con longitud de clave de 4096 para SUBORDINADA CA<br>RSA con longitud de clave suscriptores / responsables de 2048.<br>ECDSA con longitud de clave de 384 para CA RAÍZ<br>ECDSA con longitud de clave de 384 para SUBORDINADA CA<br>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.<br>ITU-T-X509 octubre 2019<br>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<br>HSM FIPS 140-2 Nivel 3 o superior (Firma Centralizada) |
| Actividades de certificación artículo 161 del decreto ley 0019 de 2012 | 1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.<br>2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.<br>3. 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 |

## 10.8. TARIFAS DEL SERVICIO DE EMISIÓN DE CERTIFICADOS DIGITALES

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 10.9. IMPARCIALIDAD Y NO DISCRIMINACIÓN

De acuerdo con lo establecido en la Declaración de Prácticas de Certificación

## 10.10. MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES

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

## 10.11. PERFIL DE LOS CERTIFICADOS

Consultar el Anexo 1 de la DPC Matriz Perfil Técnico de los Certificados

| | |
|---|---|
| **OID (Object Identifier)** | 1.3.6.1.4.1.31136.1.4.19 |
| **Ubicación de la PC** | https://gse.com.co/documentos/calidad/politicas/Politica_de_certificado_para_certificados_digitales_V19.pdf |