Título del Documento	**Declaración de Prácticas de Certificación**
Versión	13
Grupo de Trabajo	Comité de Gerencia
Estado del documento	Final
Fecha de emisión	01/11/2016
Fecha de inicio de vigencia	31/05/2022
OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.1.13
Ubicación de la DPC	https://gse.com.co/documentos/calidad/DPC/Declaracion_de_Practicas_de_Certificacion_V13.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
2	04-10-2017	• Actualización de datos de contacto de la ECD y Logo • Actualización de las entidades de Enrolamiento • Actualización datos de contacto Proveedores de servicios de certificación • Información referente al Director General de GSE. Actualización datos TSA GSE.
3	03-04-2018	Actualización información y ajustes con relación al CEA-4.1-10 de acuerdo con la revisión de las matrices de requisitos.
4	27-11-2018	Se cambio de la V3 a V4 del 27/11/2018 Actualización de tabla de contenido, información y ajustes con relación a nuevos cargos, tarifas, rutas de acceso a la página web, corrección de la subordinada, se incluye la frase establecido y probado, se amplía el numeral 8.7.4 nombrando los mecanismos tecnológicos empleados para la protección de datos, se relacionaron todas las políticas de certificación, cambio de términos y actualización del representante legal.
5	12-04-2019	Se elimino el numeral de la EE, se aclaró que, para el uso del certificado de firma centralizada, es necesario la adquisición de una plataforma tecnológica con costos adicionales. Se hace la aclaración en el numeral 1.6.2 de los requisitos y restricciones de la RA y de Criterios y métodos de evaluación de la Solicitudes. Se actualizaron los roles de la RA
6	07/06/2019	Aclaración del alcance de la acreditación en el marco de la DPC 1.1 Resumen 4.1 Solicitud del certificado, se aclara el procedimiento de como acceder al servicio. 4.1.1 Aclaración de no discriminación al acceder al servicio. 8.9.3 Aclaración de derechos del suscriptor o responsable
7	31/03/2020	Se ajusta la DPC a los cambios generados por las nuevas plataformas, se agregan los numerales de objetivo y alcance, se ajusta la lista de precios, se modifican los links para que apunten a las nuevas rutas, se realiza el cambio del Represéntate Legal y se relaciona de manera más específica los servicios acreditados por ONAC.
8	14/08/2020	Se elimina todo lo relacionado con el servicio de Generación de firmas digitales, se agrega otra condición en el numeral 5.2.2 Autenticación de la identidad de una entidad, para la renovación de certificados de firma digital y se mencionan los servicios utilizados para la validación de identidad.
9	12/02/2021	Se incluyo el enlace para consultar en línea el Certificado de Existencia y Representación Legal para la ECD y la CA actual (Paynet SAS).

Versión	Fecha	Cambio/Modificación
		Se incluyó la información detallada de las CA actual (Paynet SAS) e histórica (Indenova) de acuerdo con lo establecido en el ítem 1 del numeral 10.7 del CEA 4.1-10. Se modificó la información de los datacenter de acuerdo con lo establecido en el certificado de acreditación de la ONAC. Se elimino el párrafo sobre la renovación de los certificados digitales del numeral 5.2.2 y 5.2.3. Se actualizaron los siguientes numerales: • 6.4.2 Aprobación o rechazo de las solicitudes de certificado • 6.4.3 Plazo para procesar las solicitudes de certificado • 7.10.1 Roles de confianza • 8.1.4 Entrega de la llave pública de la ECD a terceros aceptantes Se actualizaron los links para que apunten a las nuevas rutas
10	16/07/2021	Se actualizaron los numerales: 3.6.1 Autoridad de Certificación (CA), datos proveedor datacenter. 4.1 Repositorios Se actualizo el numeral 6.5.6. 6.5.7 Plazo para procesar las solicitudes de certificado 6.8.2 Uso de la llave privada y del certificado por terceros de buena fe 6.12 Revocación y suspensión de certificados 6.12.3 Procedimiento de solicitud de revocación 6.13.1 Descripción del contenido de los certificados Autoridad Subordinada 01 GSE 6.13.1.8 Identificadores de objeto (OID) de los algoritmos 6.14.1.3 Disponibilidad CRL 6.14.1.7 Disponibilidad OCSP 6.14.3 Características opcionales 7.10.1 Roles de confianza 8.1.4 Entrega de la llave pública de la ECD a terceros aceptantes 8.1.5 Tamaño de las llaves 8.1.6 Parámetros de generación de la llave pública y verificación de la calidad 8.2.4 Backup de la llave privada 8.2.5 Archivo de la llave privada 8.2.6 Transferencia de la llave privada desde el módulo criptográfico 8.2.7 Almacenamiento de las llaves privadas en un módulo criptográfico 8.5.3 Acciones en caso de un evento o incidente de seguridad de la información

Versión	Fecha	Cambio/Modificación
		10. DESCRIPCION DE PRODUCTOS Y SERVICIOS, Servicio de Archivo, Registro, Conservación, Custodia y Anotación para los Documentos Electrónicos 11.7.1 Política de Tratamiento de Datos Personales 11.3 Imparcialidad y No Discriminación 14. ANEXO 1 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS DIGITALES 15. ANEXO 2 TÉRMINOS Y CONDICIONES Se actualizan OID y links de consulta de: • Declaración de Practicas de Certificación • Políticas de Certificado para Certificados Digitales • Políticas de Certificado para Servicio de Estampado Cronológico • Políticas de Certificado para Servicio de Archivo, registro, Conservación, Custodia y Anotación de Documentos Electrónicos Transferibles y Mensajes de Datos. • Políticas de Certificado para Servicio de Correo Electrónico Certificado
11	5/10/2021	• Se actualizaron los numerales incluyendo firma electrónica: 6.1 Solicitud del certificado 6.5 Validación inicial de la identidad 6.5.1 Método para demostrar la posesión de la llave privada 10 Descripción de Productos y Servicios 11.1.1 Tarifas de emisión o renovación de certificados 11.9.3 Obligaciones del Suscriptor y/o Responsable. • Se incluyeron los siguientes numerales haciendo referencia a firma electrónica: 5.1.1.1.1 Firma Electrónica 5.1.1.2.2 Certificados de suscriptor de ECD GSE (Matriz Perfil técnico de certificados firma electrónica) 13 Políticas de Certificación 16 Anexo 3 DPC matriz perfil técnico certificados firma electrónica • Se incluyo una nota aclaratoria de la validación del OCSP en los numerales 4.1, 4.3, 6.12.9, 6.12.10, 6.14.3. • Se actualizó el numeral 6.12.3 Procedimiento de solicitud de revocación adicionando un nuevo canal de revocación en línea. • Se actualizo el numeral 8.3.2 dando claridad del periodo de valide e las llaves raíz y subordinadas del algoritmo RSA y ECDSA • Se actualizan OID y links de consulta

Versión	Fecha	Cambio/Modificación
12	27/10/2021	• Se modifico el numeral 6.5 de Validación de Identidad • Se actualizó los OID y el link de la PC de Certificados Digitales • Se actualizó el OID y el link de la DPC con esta nueva versión.
13	31/05/2022	De acuerdo con la nueva versión de CEA se hicieron los ajustes a los siguientes numerales: • 3.1 Resumen: Se elimino el 4.1-10 dejando únicamente CEA. • 3.2. Petición, queja, reclamo y solicitudes: Se eliminó el termino apelación. • 3.6 PKI Participantes: Se elimina como CA a Indenova. • 5.1.1.1 – 5.1.1.2 Tipos de Nombres: Se eliminan los certificados raíz y subordinados de Indenova y se incluyen los relacionados a curva elíptica. • 6.5 Validación inicial de Identidad: Se incluyo un párrafo final sobre el consumo de confronta en los servicios. • 6.13.1 Descripción de contenido de los certificados: Se incluyo el campo nombre alternativo del sujeto. • 6.13.1.7 Se eliminaron 3 propósitos de la llave. • 7.10.1 Roles de confianza: se modificaron los roles de los agentes RA, Administrador RA y Auditor RA: • 7.16 Cese de una ECD: Se modifico de acuerdo con lo requerido en el nuevo CEA. • 9.2 Identidad/cualificación del auditor: Se modificaron los requisitos de aseguramiento. • 10. Descripción de productos y servicios: Se eliminó el certificado de firma centralizada, se modificó el nombre de servicio de Archivo y se modificó el servicio de generación de firmas electrónicas de acuerdo con el certificado de acreditación. • 11.4. Se modifico exoneración por límites de responsabilidad. • 11.9.6 Obligación de otros participantes: Se modifico el ítem r) eliminando el 4.1-10 dejando únicamente CEA. • 15. Se modifico el nombre del anexo sobre términos y condiciones. • 16. Se incluyo este ítem del anexo técnico de certificado de firma electrónica. • Se actualizó los OID y el link de la PC de Certificados Digitales • Se actualizó el OID y el link de la DPC con esta nueva versión. • Se incluyo el código de calidad en el encabezado del documento.

TABLA DE CONTENIDO

1. OBJETIVO

Dar a conocer al público en general los lineamientos establecidos por Gestión de Seguridad Electrónica para prestar los servicios como Entidad 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, en el territorio de Colombia.

2. ALCANCE

Este documento aplica para los productos y servicios acreditados por el Organismo Nacional de Acreditación de Colombia - ONAC.

3. INTRODUCCIÓN

3.1 Resumen

La Declaración de Prácticas de Certificación (DPC)- Global Certification Authority Root GSE (en adelante DPC) 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, declaraciones sobre las políticas y procedimientos que la **Entidad de Certificación Digital (en adelante ECD GSE)** como **Prestador de Servicios de Certificación digital (PSC)** aplica como lineamiento para prestar los servicios de certificación digital 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.

La DPC está conforme con los siguientes lineamientos:

i. Criterios Específicos de Acreditación para las Entidades de Certificación Digital (en adelante CEA) que deben ser cumplidos para obtener la Acreditación como Entidad de Certificación Digital - ECD, ante el Organismo Nacional de Acreditación de Colombia – ONAC;
ii. La DPC está organizada bajo la estructura definida en el documento RFC3647 Internet x.509 Public Key Infraestructure Certificate Policy and Certification Practice Framework de grupo de trabajo IETF - The Internet Engineering Task Force, (que sustituye a la RFC2527) http://www.ietf.org/rfc/rfc3647.txt?number=3647.
iii. ETSI EN 319 411-1 V1.2.0 (2017-08).

La actualización y/o modificación de la DPC, se realizará a través del procedimiento establecido por GSE de información documentada, cualquier cambio o adecuación sobre el documento deberá ser revisado, analizado y aprobado por el Comité de Gerencia.

DATOS DE GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.:

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

3.2 Peticiones, Quejas, Reclamos y Solicitudes

Las peticiones, quejas, reclamos y solicitudes sobre los servicios prestados por ECD GSE o entidades subcontratadas, explicaciones sobre esta DPC y sus políticas; 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.

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.

3.3 Nombre del documento e identificación

La **DPC** para **ECD GSE** se denominará "Declaración de Prácticas de Certificación (DPC)" La versión cambia de acuerdo con las modificaciones sobre el mismo documento.

GSE es una empresa registrada (Registered Private Enterprise) ante la organización internacional IANA (Internet Assigned Numbers Authority), con el código privado No 31136 bajo la rama 1.3.6.1.4.1 (iso.org.dod.internet.private.enterprise). La anterior información puede ser consultada en la URL, haciendo la búsqueda por el código 31136 http://www.iana.org/assignments/enterprise-numbers

La jerarquía de OIDs fue establecida por ECD GSE a partir de la raíz 1.3.6.1.4.1.31136 definida por la IANA y está conforme a los siguientes parámetros:

JERARQUIA OID	DESCRIPCION	NOMBRE
1	Formato ISO	No varia
3	Organización	No varia
6	Publico	No varia
1	Internet	No varia
4.1 (31136)	Identificación de la organización	No varia, definida por la IANA
1	Tipo de documento	Cambia dependiendo si son políticas, procedimientos, manuales entre otros
1	Número del documento	Este es el número asignado al documento entre su grupo
13	Versión del documento	Se modifica de acuerdo con cada versión del documento

De conformidad con esta jerarquía, la presente DPC se ha identificado con el OID: **1.3.6.1.4.1.31136.1.1.13**

3.4 Marco Jurídico

La ejecución, interpretación, modificación o validez de la presenta DPC y sus correspondientes anexos se regirá por lo dispuesto en la legislación colombiana vigente.

3.4.1 Mecanismo de Resolución de Diferencias

Si por alguna razón surge alguna diferencia entre las Partes (suscriptor/responsable y ECD GSE) con ocasión de:

i. La prestación de los servicios de certificación digital descritos en esta DPC.
ii. Durante la ejecución de los servicios contratados.

iii. Por la interpretación del contrato, DPC y cualquier otro documento entregado por ECD GSE.

La parte interesada notificará a la otra parte vía correo electrónico certificado la existencia de dicha diferencia, con la información completa y debidamente sustentada de la diferencia, a fin de que dentro de los quince (15) días hábiles siguientes a dicha notificación, las Partes busquen llegar a un arreglo directo entre ellas como primera instancia.

Finalizado dicho período la(s) diferencia(s) persista(n), las Partes quedaran en la libertad de acudir ante la justicia ordinaria colombiana para hacer valer sus derechos o exigencias, que se sujetará a las normas vigentes sobre la materia, los costos que se causen con ocasión de la convocatoria estarán totalmente a cargo de la Parte vencida.

3.5 Definiciones y acrónimos

3.5.1 Definiciones

Los siguientes términos son de uso común y requerido para el entendimiento de la presente DPC:

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 este 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 divulgación de la llave privada que pueda poner en riesgo el empleo y uso del certificado por parte 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:

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

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.

3.5.2 Acrónimos

CA: Certification Authority
CA Sub: Autoridad de Certificación Subordinada
CP: Política de Certificación (Certificate Policy)
DPC: Declaración de Prácticas de Certificación (Certificate 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.
HSM: Módulo de seguridad criptográfico (Hardware Security Module)
IEC: International Electrotechnical Commission
IETF: Internet Engineering Task Force (Organismo de estandarización de Internet)
IP: Internet Protocol
ISO: International Organization for Standardization
LDAP: Lightweight Directory Access Protocol
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
VA: Autoridad de validación (Validation Authority)

3.5.3 Estándares y Organismos de estandarización

CEN: Comité Europeo de Normalización
CWA: CEN Workshop Agreement
ETSI: European Telecommunications Standard Institute
FIPS: Federal Information Processing Standard
IETF: Internet Engineer Task Force
PKIX: Grupo de trabajo del IETF sobre PKI
PKCS: Public Key Cryptography Standards
RFC: Request For Comments

3.6 PKI participantes

3.6.1 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 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, 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.

GSE tiene como proveedor actual 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

El proveedor cuenta con dos datacenter (un principal y un alterno), el datacenter principal con UNE - EPM TELECOMUNICACIONES S.A. se encuentra ubicado en la autopista Medellín kilómetro 6 + 200 metros costado sur, entrada por Festo kilómetro 0 + 360 metros, Parque Industrial Siberia Real en Tenjo Cundinamarca, Colombia y el Datacenter alterno con IFX Networks Colombia S.A.S se encuentra ubicado en la Avenida el Dorado # 68c – 61 oficina 508 en Bogotá D.C., Colombia

3.6.2 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).

ECD GSE tiene como autoridad de registro RA:

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

3.6.3 Suscriptor y/o responsable

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.

3.6.4 Responsable

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.

3.6.5 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.

3.6.6 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.

3.6.7 Otros participantes

3.6.7.1 Comité de Gerencia

El comité de Gerencia es un organismo interno de ECD GSE, conformado por el Director General y directores 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.

3.6.7.2 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.

A efectos de esta DPC, la empresa PAYNET SAS en adelante Paynet SAS será el proveedor y administrador de la infraestructura de la ECD GSE.

GSE tiene como entidad proveedor del servicio de infraestructura PKI a:

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

El servicio de Infraestructura PKI prestado por Paynet SAS cuenta con un contrato de prestación de servicio que prevé la terminación condicionada a que la ECD GSE haya implementado o contratado una infraestructura o servicio tecnológico que le permita continuar prestando sus servicios sin ningún perjuicio para los suscriptores o entidades.

ECD GSE y Paynet SAS cumplen con los requisitos legales, técnicos y de infraestructura de conformidad a los Criterios Específicos de acreditación establecidos por el ONAC.

La contratación de Paynet SAS no exime a la ECD GSE de cumplir con el deber de permitir y facilitar a ONAC la realización de auditorías.

La ECD GSE tiene establecido una evaluación de proveedores para garantizar el cumplimiento de los requisitos por parte del proveedor PKI y generar un seguimiento al desempeño de este.

3.6.7.3 Entidades de Certificación Digital Reciprocas

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.

3.7 Administración de la DPC y PC

3.7.1 Organización administradora del documento

La DPC y las políticas de certificación son responsabilidad y propiedad de GSE y por tanto actúa como su administradora.

3.7.2 Persona de contacto:

Nombre: Álvaro de Borja Carreras Amoros
Cargo: Representante Legal
Dirección: Calle 73 No. 7 – 31 Piso 3 Torre B Edificio el Camino
Domicilio: Bogotá D.C., Colombia.
Teléfono: +57 (1) 4050082
Correo electrónico: info@gse.com.co

3.7.3 Persona o área que determina la adecuación de las Políticas a la DPC

Area encargada: Director de Operaciones
Dirección: Calle 73 No. 7 – 31 Piso 3 Torre B Edificio el Camino
Domicilio: Bogotá D.C., Colombia.
Teléfono: +57 (1) 4050082
Correo electrónico: info@gse.com.co

3.7.4 Procedimientos de aprobación de la DPC

El Comité de Gerencia es el órgano interno de GSE encargado de la revisión, aprobación y autorización de la publicación de la DPC en la página Web http://www.gse.com.co

3.8 Cambios que afecten los servicios de certificación digital

ECD GSE puede realizar ajustes o cambios a los servicios de certificación digital en los siguientes eventos:

a. Por cambios normativos en la legislación para ECD.
b. Por solicitud del ONAC.

c. Por solicitud de la Superintendencia de Industria y Comercio de Colombia - SIC.
d. Cambios tecnológicos que afecten los servicios de certificación digital.
e. Por solicitud de suscriptores o responsables, previa aprobación del comité de Gerencia.
   Para lo cual el Suscriptor o responsable deberá enviar comunicación dirigida a el comité de Gerencia de la ECD GSE sobre el cambio solicitado, la aceptación o rechazo estará bajo la discreción del Comité de Gerencia.

3.8.1 Procedimiento para los cambios

3.8.1.1 Cambios que no requieren notificación

a. Cuando los cambios realizados no afecten el funcionamiento de los servicios prestados a los suscriptores o responsables actuales, será labor del comité de Gerencia definir el nivel de impacto de los cambios.
b. Cuanto los cambios impliquen correcciones tipográficas o de edición en el contenido de los servicios prestados.

3.8.1.2 Cambios que requieren notificación

a. Cuando los cambios realizados afecten el funcionamiento de los servicios prestados a los suscriptores o responsables actuales, será labor del comité de Gerencia definir el nivel de impacto de los cambios.
b. Cuando los cambios impliquen actualización de datos de contacto con la ECD GSE.

3.8.2 Mecanismo y periodo de notificación

ECD GSE notificará por correo electrónico y/o portal web, a los suscriptores, responsables, ONAC y SIC con la información técnica detallada y las modificaciones a contratos, sobre el cambio realizado a los servicios de certificación digital, cuando:

a. El Comité de Gerencia y el proceso del Sistema Integrado de Gestión de la ECD GSE considere que los cambios a los servicios de certificación digital afectan el funcionamiento y aceptabilidad de estos.
b. Los cambios introduzcan nuevos requisitos para la prestación de los servicios de certificación digital por actualizaciones tecnológicas o cambios normativos que afecten los servicios.

Los suscriptores o responsables de los servicios de certificación digital afectados por los cambios realizados pueden presentar sus comentarios o rechazo a la prestación del servicio de la ECD GSE en comunicación dirigida a el comité de Gerencia dentro de los treinta (30) días siguientes a la notificación, pasados los treinta (30) días se entenderá como aceptadas las condiciones por parte de los suscriptores o responsables.

4. RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

4.1 Repositorios

- **Certificados Raíz ECD GSE**
  https://certs2.gse.com.co/CA_ROOT.crt
  https://certs2.gse.com.co/CA_ECROOT.crt
  https://certs2.gse.com.co/CA_FEROOT.crt

- **Lista de Certificados Revocados Raíz ECD GSE (CRL)**
  ¡Error! Referencia de hipervínculo no válida.https://crl2.gse.com.co/CA_ROOT.crl
  https://crl2.gse.com.co/CA_ECROOT.crl
  https://crl2.gse.com.co/CA_FEROOT.crl

- **Certificados Subordinadas ECD GSE**
  https://certs2.gse.com.co/CA_SUB01.crt
  https://certs2.gse.com.co/CA_ECSUB01.crt
  https://certs2.gse.com.co/CA_FESUB01.crt

- **Lista de Certificados Revocados Subordinadas ECD GSE (CRL)**
  https://crl2.gse.com.co/CA_SUB01.crl
  https://crl2.gse.com.co/CA_ECSUB01.crl
  https://crl2.gse.com.co/CA_FESUB01.crl

- **Validación en línea de Certificados Digitales**
  ¡Error! Referencia de hipervínculo no válida.https://ocsp2.gse.com.co

Nota: La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender las respuestas generadas por el servicio, tal es el caso de OPENSSL.

Este repositorio de la ECD GSE no contiene ninguna información confidencial o privada.

Los repositorios de la ECD GSE están referenciados por la URL. Cualquier cambio en las URLs se notificará a todas entidades que puedan verse afectadas.

Las direcciones IP correspondientes a cada URL podrán ser múltiples y dinámicas, pudiendo ser modificadas sin previo aviso por ECD GSE.

4.2 Publicación de la información de certificación

La Lista de Certificados Revocados publicada en la página web de GSE está firmada digitalmente por la ECD GSE.

La información del estado de los certificados digitales vigentes está disponible para consulta en la página Web y con el protocolo OCSP.

4.3 Plazo o frecuencia de la publicación

Certificado Raíz
El certificado raíz se publicará y permanecerá en la página Web de ECD GSE durante todo el tiempo en que se estén prestando servicios de certificación digital.

Certificado Subordinada
El certificado de la Subordinada se publicará y permanecerá en la página Web de ECD GSE durante todo el tiempo en que se estén prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)
ECD GSE publicará en la página Web, la lista de certificados revocados en los eventos y con la periodicidad definidas en el apartado *Frecuencia de emisión de las CRLs.*

Declaración de Prácticas de Certificación (DPC)- Global Certification Authority Root GSE

Con autorización del Comité de Gerencia, la validación por parte de la firma de Auditoría, la emisión del informe de cumplimiento de la auditoria y finalmente con la acreditación expresa del ONAC, se publicará la versión finalmente aprobada para la prestación del servicio de certificación digital y las publicaciones posteriores estarán sujetas a las modificaciones a que haya lugar con aprobación del comité de Gerencia. Los cambios generados en cada nueva versión serán informados a ONAC y publicados en la página Web de ECD GSE junto con la nueva versión. La Auditoria anual validará estos cambios y emitirá el informe de cumplimiento.

Validación en línea de Certificados Digitales
ECD GSE publicará los certificados emitidos en un repositorio en formato X.509 V3 los cuales podrán ser consultados en la dirección https://ocsp2.gse.com.co

La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender las respuestas generadas por el servicio, tal es el caso de OPENSSL.

4.4 Controles de acceso a los repositorios

La consulta a los repositorios disponibles en la página Web de GSE antes mencionados, es de libre acceso al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de ECD GSE, que cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta.

5. IDENTIFICACIÓN Y AUTENTICACIÓN

5.1 Nombres

5.1.1 Tipos de nombres

El documento guía que ECD GSE utiliza para la identificación única de los suscriptores o responsables de certificados emitidos está definido en la estructura del Nombre Distintivo "*Distinguished Name* (DN)" de la norma ISO/IEC 9595 (X.500).

Los certificados emitidos por ECD GSE contienen el nombre distintivo (*distinguished name* o DN) X.500 del emisor y el destinatario del certificado en los campos *issuer name* y *subject name* respectivamente.

5.1.1.1 Certificados raíz de la ECD GSE

El DN del 'issuer name' del certificado raíz, tiene los siguientes campos y valores fijos:
C = CO
O = GSE
OU = PKI
CN = Autoridad Raiz GSE
E = info@gse.com.co

En el DN del 'subject name' se incluyen los siguientes campos:
C = CO
O = GSE
OU = PKI
CN = Autoridad Raiz GSE
E = info@gse.com.co

5.1.1.1.1 Curva Elíptica (ECDSA)

El DN del 'issuer name' del certificado raíz, tiene los siguientes campos y valores fijos:
C = CO
S = Distrito Capital
L = Bogota D.C.

O = GESTION DE SEGURIDAD ELECTRONICA S.A
OU = GSE CA RAIZ R2
SERIALNUMBER = 900204278
CN = GSE ECDSA RAIZ
E = info@gse.com.co
STREET = www.gse.com.co

En el DN del 'subject name' se incluyen los siguientes campos:
C = CO
S = Distrito Capital
L = Bogota D.C.
O = GESTION DE SEGURIDAD ELECTRONICA S.A
OU = GSE CA RAIZ R2
SERIALNUMBER = 900204278
CN = GSE ECDSA RAIZ
E = info@gse.com.co
STREET = www.gse.com.co

5.1.1.1.2 Firma Electrónica

STREET=www.gse.com.co,
E=info@gse.com.co,
CN=GSE FIRMA ELECTRONICA RAIZ,
SN=900204272,
OU=GSE FIRMA ELECTRONICA R1,
O=GESTION DE SEGURIDAD ELECTRONICA S.A,
L=BOGOTA D.C.,
ST=DISTRITO CAPITAL,
C=CO

5.1.1.2 Certificados de las Subordinadas

El DN del 'issuer name' de los certificados de las subordinadas de ECD GSE, tienen las siguientes características:
C = CO
O = GSE
OU = PKI
CN = Autoridad Raiz GSE
E = info@gse.com.co

En el DN del 'subject name' se incluyen los siguientes campos:
C = CO
L = Bogota D.C.

O = GSE
OU = PKI
CN = Autoridad Subordinada 01 GSE
E = info@gse.com.co

5.1.1.2.1 Curva Elíptica (ECDSA)

El DN del 'issuer name' de los certificados de las subordinadas de ECD GSE, tienen las siguientes características:
C = CO
S = Distrito Capital
L = Bogota D.C.
O = GESTION DE SEGURIDAD ELECTRONICA S.A
OU = GSE CA RAIZ R2
SERIALNUMBER = 900204278
CN = GSE ECDSA RAIZ
E = info@gse.com.co
STREET = www.gse.com.co

En el DN del 'subject name' se incluyen los siguientes campos:
C = CO
S = Distrito Capital
L = Bogota D.C.
O = GESTION DE SEGURIDAD ELECTRONICA S.A
OU = GSE ECDSA R2 SUB1
SERIALNUMBER = 900204278
CN = GSE ECDSA SUBORDINADA
E = info@gse.com.co
STREET = www.gse.com.co

5.1.1.2.2 Certificados de suscriptor de ECD GSE (Matriz Perfil técnico de certificados)

El DN del 'issuer name' de los certificados de suscriptor de ECD GSE, tienen las siguientes características generales:
C = CO
L = Bogota D.C.
O = GSE
OU = PKI
CN = Autoridad Subordinada 01 GSE
E = info@gse.com.co

En el DN del 'subject name' está determinado por el ANEXO 1 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS DIGITALES

5.1.1.2.3 Certificados de suscriptor de ECD GSE (Matriz Perfil técnico de certificados firma electrónica)

STREET=www.gse.com.co,
E=info@gse.com.co,
CN=GSE FIRMA ELECTRONICA INTERMEDIA,
SN=900204272,
OU=GSE FIRMA ELECTRONICA R1,
O=GESTION DE SEGURIDAD ELECTRONICA S.A,
L=BOGOTA D.C.,
ST=DISTRITO CAPITAL,
C=CO

5.1.2 Nombres Distintivos

Los nombres distintivos (DN) de los certificados emitidos por ECD GSE son únicos y permiten establecer un vínculo entre la llave pública y el número de identificación del suscriptor. Debido a que una misma persona o entidad puede solicitar varios certificados a su nombre, estos se diferenciarán por el uso de un valor único en el campo DN.

5.1.3 Anonimato y seudoanonimato del suscriptor o responsables

No se podrán utilizar alias en los campos de suscriptor o responsable ya que dentro del certificado debe figurar el verdadero nombre, razón social sigla o denominación del solicitante del certificado.

5.1.4 Reglas para la interpretación de varias formas de nombre

La regla utilizada para interpretar los nombres distintivos del emisor y de los suscriptores o responsables de certificados digitales que emite ECD GSE es el estándar ISO/IEC 9595 (X.500) Distinguished Name (DN).

5.1.5 Singularidad de los nombres

El DN de los certificados digitales emitidos es único para cada suscriptor.

5.1.6 Reconocimiento, autenticación y papel de las marcas reconocidas

Reconocimiento, autenticación y papel de las marcas reconocidas ECD GSE no está obligada a recopilar o solicitar evidencia en relación con la posesión o suscripción o responsabilidad de marcas registradas u otros signos distintivos antes de la emisión de los certificados digitales. Esta política se extiende al uso y empleo de nombres de dominio

5.2 Identificación y autenticación para peticiones de renovación de llaves

5.2.1 Identificación y autenticación para renovación.

ECD GSE realiza en todos los eventos el proceso de autenticación del solicitante incluso en los de renovación y con base en ello emite los certificados digitales. Solo aquellas solicitudes firmadas digitalmente por el suscriptor, se les realizará la renovación del certificado digital sin pasar por un nuevo proceso de identificación y autenticación garantizando siempre la validación documental.

5.2.2 Identificación y autenticación tras una revocación

El proceso de reposición de un certificado de firma digital en consecuencia de la revocación por las diferentes causales definidas en esta DPC, exigen un proceso de verificación para esa solicitud (Reposición).

5.3 Identificación y autenticación para peticiones de revocación

ECD GSE, atiende las peticiones de revocación de conformidad con las causales de revocación especificadas en el apartado *Circunstancias para la revocación de un certificado de esta DPC* y autentica la identidad de quien solicita la revocación de certificado. De acuerdo con lo establecido en el procedimiento de revocaciones.

6. REQUISITOS OPERACIONALES PARA EL TIEMPO DE VIDA DE LOS CERTIFICADOS

6.1 Solicitud del certificado

Cualquier persona que requiera la prestación del servicio de certificación digital, lo podrá hacer utilizando los canales dispuestos por GSE, aceptando el documento términos y condiciones de la ECD y aportarlos junto con la documentación requerida para autenticar la información suministrada. Una vez completada y confirmada la información por parte del solicitante, el formulario de solicitud es enviado a la Autoridad de Registro quien se encargará de validar la información suministrada y aprobarla de conformidad con el cumplimiento de los requisitos exigidos en las Políticas de Certificación.

La solicitud de un servicio de certificación digital deberá radicarse a través de los canales electrónicos que para el efecto disponga ECD GSE.

Los usuarios que solicitan nuestros servicios de Certificación Digital aceptan los términos y condiciones del servicio especificadas en la presente DPC.

El solicitante aporta los documentos necesarios escaneados o en original electrónico, preservando la legibilidad para el uso de la información y se surten los procedimientos establecidos por ECD GSE, para la obtención de su certificado digital.

ECD GSE, se reserva el derecho de solicitar documentos adicionales a los exigidos, en original o copia; con el fin de verificar la identidad del solicitante, también puede eximir de la presentación de cualquier documento cuando la identidad del solicitante haya sido suficientemente verificada por ECD GSE a través de otros medios. La documentación suministrada será validada de acuerdo con los Criterios y Métodos de Evaluación de Solicitudes establecidos por GSE.

El solicitante acepta que ECD GSE tiene el derecho discrecional de rechazar una solicitud de certificado digital cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial, buen nombre de GSE o idoneidad legal o moral de todo el sistema de certificación digital, notificando la no aprobación.

Para la solicitud de certificado de firma electrónica se tiene establecido el Procedimiento de Firma Electrónica (PTI-PD-20).

6.2 Quién puede solicitar un certificado

Toda persona natural o jurídica legalmente facultada y debidamente identificada puede tramitar la solicitud de emisión de un certificado digital.

6.2.1 Proceso de registro y responsabilidades

La RA de GSE previamente cumplidos los requisitos de autenticación y verificación de los datos del solicitante, aprobará y firmará digitalmente la constancia de emisión de los certificados digitales. Toda la información relacionada quedará registrada en el sistema de la RA GSE.

6.3 Usos del Certificado

6.3.1 Usos adecuados del certificado

Los usos adecuados de los Certificados emitidos por ECD GSE vienen especificados en Políticas de Certificado para Certificado Digitales.

Los Certificados emitidos bajo esta DPC pueden ser utilizados con los siguientes propósitos:

- **Identificación del Suscriptor:** El Suscriptor del Certificado Digital puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado Digital.
- **Integridad:** La utilización del Certificado Digital para aplicar firmas digitales garantiza que el documento firmado es integro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Suscriptor. Se certifica que el mensaje

recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Suscriptor.

- **No repudio:** Con el uso de este Certificado Digital también se garantiza que la persona que firma digitalmente el documento no puede repudiarlo, es decir, el Suscriptor que ha firmado no puede negar la autoría o la integridad de este.

La clave pública contenida en un Certificado Digital puede utilizarse para cifrar mensajes de datos, de tal manera que únicamente el poseedor de la clave privada puede descifrar dicho mensaje de datos y acceder a la información. Si la clave privada utilizada para descifrar se pierde o se destruye, la información que haya sido cifrada no podrá ser descifrada. El suscriptor, responsables y los terceros de buena fe, reconocen y aceptan los riesgos que representa hacer uso de los certificados digitales para realizar procesos de cifrado y en especial la utilización de las claves para cifrar mensajes de datos es de exclusiva responsabilidad del suscriptor o responsable en caso de materializar una pérdida o destrucción de la clave.

ECD GSE no asume ninguna responsabilidad por el uso de los certificados digitales para procesos de cifrado.

Cada política de certificación está identificada por un único identificador de objeto (OID) que además incluye el número de versión.

Cualquier otro uso que no esté descrito en esta DPC se considerará una violación a esta DPC y constituirá una causal de revocación inmediata del servicio de certificación digital y terminación del contrato con el suscriptor o responsable, sin perjuicio de las acciones penales o civiles a las que haya lugar por parte de la ECD GSE.

6.3.2 Usos prohibidos del certificado y exclusión de responsabilidad

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta DPC y concretamente en las Políticas De Certificado para Certificados Digitales.

Se consideran usos indebidos aquellos que no están definidos en esta DPC y en consecuencia para efectos legales, 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 esta DPC, dentro de los que se incluyen, pero sin limitarse a los siguientes usos prohibidos:

- Fines u operaciones ilícitas bajo cualquier régimen legal del mundo.
- Cualquier práctica contraria a la legislación colombiana.
- Cualquier práctica contraria a los convenios internacionales suscritos por el estado Colombiano.

- Cualquier práctica contraria a las normas supranacionales.
- Cualquier práctica contraria a las buenas costumbres y prácticas comerciales.
- Cualquier uso en sistemas cuyo fallo pueda ocasionar:
  - Muerte
  - Lesiones a personas
  - Perjuicios al medio ambiente
- Como sistema de control para actividades de alto riesgo como son:
  - Sistemas de navegación marítimo
  - Sistemas de navegación de transporte terrestre
  - Sistemas de navegación aéreo
  - Sistemas de control de tráfico aéreo
  - Sistemas de control de armas

6.4 Tramitación de solicitud de certificados

6.4.1 Realización de las funciones de identificación y autenticación

Las funciones de autenticación y verificación de la identidad del solicitante son realizadas por la RA de GSE, encargada de autorizar la emisión del certificado, quien comprueba si la información suministrada es auténtica y si la documentación anexa cumple con los requisitos definidos para cada tipo de certificado de acuerdo con esta DPC.

La documentación que la RA de GSE deberá comprobar para la correcta emisión de cada tipo de certificado se define en las Políticas de Certificado para Certificado Digitales.

6.5 Validación Inicial de la Identidad

La ECD GSE, se reserva el derecho de declinar la aceptación de una solicitud o el mantenimiento de un contrato para la certificación cuando a su juicio existen razones que puedan poner en riesgo la credibilidad, valor comercial, idoneidad legal o moral de la ECD, así mismo la participación demostrada del solicitante en actividades ilegales, o temas similares relacionados con el solicitante, será razón suficiente para rechazar la solicitud.

Los datos del solicitante: tipo de identificación, número de identificación, nombres, apellidos, nit (aplica para empresa), razón social (aplica para empresa), datos de domicilio: departamento, municipio, dirección y correo electrónico son revisados y/o validados en conjunto con el formulario de solicitud y la documentación suministrada para cada tipo de certificado digital.

La validación de identidad se realiza de manera análoga a la validación presencial consumiendo los servicios ampliamente usados para tal fin enumerados a continuación:

- Archivo Nacional de Identificación - Registraduría Nacional del Estado Civil.

- Muisca (Modelo Único de Ingresos, Servicio y Control Automatizado) de la DIAN (Dirección de impuestos y Aduanas Nacionales).
- Confronta.
- Registro Único Empresarial y Social (Para Persona Jurídica).

El documento Registro Único Tributario – RUT se solicitará en el formato actualizado de DIAN que incluye código QR.

Estos servicios están relacionados en el Procedimiento de emisión de certificados digitales.

Para los servicios de certificación digital (Estampado Cronológico, Correo Electrónico Certificado, Generación de Firmas Electrónicas Certificadas, Archivo y Conservación de Documentos Electrónicos Transferibles y Mensajes de Datos no se consumirá el servicio de validación de identidad Confronta pero si los demás mecanismos de validación.

La ECD GSE, se reserva el derecho de solicitar documentos adicionales, en original o copia; con el fin de verificar la identidad del solicitante, también puede eximir la presentación de cualquier documento cuando la identidad del solicitante haya sido suficientemente verificada por la ECD GSE a través de otros medios.

Para el caso de los certificados de firma electrónica no se realiza la validación de identidad del suscriptor sino una verificación de los datos registrados al momento de la solicitud de la firma mediante el envío de un código OTP al correo electrónico registrado.

6.5.1 Método para demostrar la posesión de la llave privada

Para garantizar la emisión, posesión y control de la llave privada por parte del suscriptor y/o responsable, se hace entrega directamente de un dispositivo criptográfico seguro token en el cual el suscriptor y/o responsable genera el par de llaves y transmite mediante un canal seguro el archivo en formato PKCS#10 donde demuestra que está en posesión de la llave privada.

En caso de que el certificado sea centralizado la generación del par de llaves se lleva a cabo en un dispositivo HSM de propiedad de la ECD GSE y se le hace entrega al suscriptor y/o responsable de un conjunto de credenciales (usuario y contraseña) para el uso exclusivo de las mismas.

Dado que los certificados de firma electrónica son efímeros y se usan únicamente para la generación de la firma, las credenciales para uso de estos certificados no son entregadas al suscriptor y en cambio son generadas automática y aleatoriamente por la plataforma y desechadas una vez se genera la firma electrónica.

6.5.2 Autenticación de la identidad de una entidad (Persona jurídica)

Para asegurar la identidad de una persona jurídica, RA GSE exige la presentación del documento oficial que acredite la existencia legal de la misma y su representante legal o apoderados quienes serán las únicas personas que puedan solicitar el certificado digital a nombre de dicha organización. Para el caso que la solicitud se realice por un tercero, se debe entregar escaneada la constancia de delegación del proceso al apoderado. Los documentos se recibirán escaneados, preservando la legibilidad para el uso de la información.

No obstante, lo anterior, ECD GSE, se reserva el derecho de emisión de certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial o idoneidad legal o moral de la Entidad de Certificación Digital.

6.5.3 Autenticación de una identidad individual (Persona Natural)

Para asegurar la identidad de una persona natural, RA GSE, exige la presentación documento de identidad del suscriptor escaneado y verifica su existencia y correspondencia contra bases de datos propias o de terceros, sean oficiales o privadas. Cuando el servicio es solicitado por un menor de edad, su identidad será asegurada con el documento de identidad (tarjeta de identidad) autenticado y documento que respalde el vínculo del solicitante y el menor de edad. Para el caso que la solicitud se realice por un tercero, se debe entregar escaneada la constancia de delegación del proceso al apoderado. Los documentos se recibirán escaneados, preservando la legibilidad para el uso de la información.

No obstante, lo anterior, ECD GSE, se reserva el derecho de emisión de certificados cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial o idoneidad legal o moral de la Entidad de Certificación Digital.

6.5.4 Información de suscriptor o responsable no verificada

En ninguna circunstancia ECD GSE omitirá las labores de verificación que conduzcan a la identificación del suscriptor o responsable y que se traduce en la solicitud y exigencia de los documentos mencionados para organizaciones y personas individuales.

6.5.5 Criterios para la interoperabilidad

ECD GSE únicamente emitirá certificados digitales a ECD Subordinadas, donde la decisión de emitir o activar el servicio de certificación digital sea de la ECD GSE a través de la RA GSE.

6.5.6 Aprobación o rechazo de las solicitudes de certificado

Si una vez verificada la identidad del solicitante, la información suministrada cumple con los requisitos establecidos por esta DPC, se aprueba la solicitud. Si no es posible la identificación plena de la identidad del solicitante o no existe autenticidad plena de la información suministrada, se niega la solicitud y no se emite el certificado. ECD GSE no asume ninguna responsabilidad por las consecuencias que puedan derivarse de la no

aprobación de la emisión de un certificado digital y así lo acepta y reconoce el solicitante al que le haya sido negada la expedición del respectivo certificado.

Igualmente, ECD GSE se reserva el derecho de no emitir certificados a pesar de que la identificación del solicitante o la información suministrada por este haya sido plenamente autenticada, cuando la emisión de un certificado en particular por razones de orden legal o de conveniencia comercial, buen nombre o reputación de GSE pueda poner en peligro el sistema de certificación digital.

Si posterior a la radicación de una solicitud y el proceso no aprobó la revisión de la solicitud o el solicitante no realizo la validación de identidad, pasados quince (15) días sin que se subsane la novedad, se rechazará la solicitud y se notificara al solicitante para que instancie una nueva solicitud.

Para lo cual ECD GSE notificara al solicitante la aprobación o rechazo de la solicitud.

6.5.7 Plazo para procesar las solicitudes de certificado

El plazo para procesar una solicitud por parte de la RA de GSE, es de uno (1) a cinco (5) días hábiles desde el momento en que se recibe la documentación e información solicitada y el solicitante haya aprobado la validación de identidad.
El tiempo de entrega del certificado digital emitido en un dispositivo criptográfico, depende del lugar de destino, sin exceder los ocho (8) días hábiles para su entrega.

6.6 Emisión de certificados

6.6.1 Actuaciones de la ECD GSE durante la emisión de certificados

El paso final del proceso de expedición de certificados digitales es la emisión del certificado por parte de ECD GSE y su entrega de manera segura al suscriptor y/o responsable.

La RA de GSE genera la documentación formal de la certificación digital, cuando se ha tomado la decisión de otorgar el certificado digital.

El proceso de emisión de certificados digitales vincula de una manera segura la información de registro y la llave pública generada.

6.6.2 Notificación al solicitante por la ECD GSE de la emisión del certificado

Mediante correo electrónico se notifica al suscriptor la emisión de su certificado digital y por consiguiente el suscriptor acepta y reconoce que una vez reciba el citado correo electrónico, se entenderá que ha sido emitido el certificado. Se entenderá que se ha recibido el correo electrónico donde se notifica la emisión de un certificado, cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección de correo electrónico que el suscriptor reportó en el formulario de solicitud. En el caso en que el suscriptor solicite que la emisión de la firma sea en un dispositivo criptográfico, se entenderá

como entregado una vez firme la carta de entrega y/o la guía de envió al operador logístico o mensajería.

La publicación de un certificado en el repositorio de certificados constituye la prueba y una notificación pública de su emisión.

6.7 Aceptación del certificado

6.7.1 Forma en la que se acepta el certificado

No se requiere confirmación por parte del suscriptor o responsable como aceptación del certificado recibido. Se considera que un certificado es aceptado por el suscriptor o responsable desde el momento que solicita su emisión, por ello, si la información contenida en el certificado expedido no corresponde al estado actual de la misma o no fue suministrada correctamente, es responsabilidad del suscriptor solicitar su revocación.

6.8 Uso de la llave privada y del certificado

6.8.1 Uso de la llave privada y del certificado por parte del suscriptor o responsable

El suscriptor o responsable del certificado digital y de la llave privada asociada, acepta las condiciones de uso establecidas en esta DPC por el solo hecho de haber solicitado la emisión del certificado y solo podrá emplearlos para los usos explícitamente mencionados y autorizados en la presente DPC y de acuerdo con lo establecido en los campos “Key Usage” de los certificados. Por consiguiente, los certificados emitidos y la llave privada no deberán ser usados en otras actividades que estén por fuera de los usos mencionados. Una vez expirada la vigencia del certificado, el suscriptor o responsable está obligado a no seguir usando la llave privada asociada al mismo. Con base en lo anterior, desde ya acepta y reconoce el suscriptor, que en tal sentido será el único responsable por cualquier perjuicio pérdida o daño que cause a terceros por el uso de la llave privada una vez expirada la vigencia del certificado. ECD GSE no asume ningún tipo de responsabilidad por los usos no autorizados.

6.8.2 Uso de la llave privada y del certificado por terceros de buena fe

El suscriptor al que se le haya expedido un certificado se obliga a que cada vez que haga uso del certificado con destino a terceras personas deberá informarles que es necesario que consulten el estado del certificado en el repositorio de certificados revocados, así como en el de emitidos a fin de verificar su vigencia y que se esté aplicando dentro de sus usos permitidos establecidos en esta DPC.

En este sentido deberá:

- Comprobar que el certificado asociado no incumple las fechas de inicio y final de vigencia.
- Comprobar que el certificado asociado a la llave privada no está revocado.

- Comprobar que la huella digital (***fingerprint)*** del certificado de la ECD raíz y la del certificado de la subordinada de ECD GSE coinciden con el publicado por GSE en su página Web.

Huella digital (fingerprint) del certificado de la ECD raíz:

SHA 256
Fingerprint=7C:1C:A5:51:31:2E:A0:2E:F1:D6:3A:4F:56:54:D0:3F:D0:4F:6F:32:7C:8E:2E:03:52:1A:22:69:7A:B7:98:43

SHA256
Fingerprint=9F:BF:5F:E1:A3:34:49:35:44:6A:95:EB:45:D3:DD:F3:49:36:18:41:21:71:71:65:F0:B8:42:11:85:0D:E6:F3

SHA256
Fingerprint=3F:CE:D4:24:F2:D5:70:53:6E:DA:65:2D:D7:C9:D3:6D:58:5A:10:ED:BB:58:85:1C:F8:2C:91:12:03:41:5C:0C

Huella digital (fingerprint) del certificado de la subordinada de ECD GSE Subordinate Certificate 001:

SHA 256
Fingerprint=70:99:01:C9:1D:8F:B2:92:DB:81:B7:04:8B:0B:06:E5:A2:AA:14:59:7D:CA:C4:DF:BE:6B:DD:90:49:D8:E2:01

SHA256
Fingerprint=8C:8B:17:8E:AA:D2:E9:AD:BF:2D:28:1E:91:53:3F:96:BF:7C:BE:1B:2D:8A:89:A0:D8:AE:FD:19:40:D0:35:88

SHA256
Fingerprint=6C:91:FA:BA:42:7F:0D:93:CB:B4:EB:09:4A:3F:5E:4A:64:D8:F2:5F:B8:7B:AA:75:D8:26:8D:BF:79:8E:CC:95

6.9 Renovación del certificado sin cambio de llaves

ECD GSE, no atiende requerimientos de renovación de un certificado sin cambio de llaves.

6.9.1 Circunstancias para la renovación de certificados sin cambio de llaves

No aplica por cuanto no se expiden certificados sin cambio de llaves.

6.9.2 Quién puede solicitar una renovación sin cambio de llaves

No aplica por cuanto no se expiden certificados sin cambio de llaves.

6.9.3 Trámites para la solicitud de renovación de certificados sin cambio de llaves

No aplica por cuanto no se expiden certificados sin cambio de llaves.

6.9.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado sin cambio de llaves

No aplica por cuanto no se expiden certificados sin cambio de llaves.

6.9.5 Forma en la que se acepta la renovación de un certificado sin cambio de llaves

No aplica por cuanto no se expiden certificados sin cambio de llaves.

6.9.6 Publicación del certificado renovado por la ECD sin cambio de llaves

No aplica por cuanto no se expiden certificados sin cambio de llaves.

6.9.7 Notificación de la emisión de un certificado renovado por la ECD a otras entidades

No aplica por cuanto no se expiden certificados sin cambio de llaves.

6.10 Renovación del certificado con cambio de llaves

Para ECD GSE, un requerimiento de renovación de un certificado con cambio de llaves es un requerimiento normal de solicitud de un certificado digital como si fuera uno nuevo y por consiguiente implica el cambio de llaves y así lo reconoce y acepta el solicitante.

6.10.1 Circunstancias para la renovación de certificados con cambio de llaves

Un certificado digital puede ser renovado a solicitud del suscriptor o responsable por próxima pérdida de vigencia o por revocación de conformidad con las causales mencionadas en esta DPC o cuando así lo requiera el suscriptor.

6.10.2 Quién puede solicitar una renovación con cambio de llaves

Para certificados de personas naturales, el suscriptor puede solicitar la renovación del certificado. Para personas jurídicas, puede solicitar la renovación del certificado digital el representante legal, suplentes o responsables.

6.10.3 Trámites para la solicitud de renovación de certificados con cambio de llaves

El procedimiento para renovación de certificados digitales es igual al 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.

6.10.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado con cambio de llaves

Mediante correo electrónico se notifica al suscriptor la emisión de su certificado digital y por consiguiente el suscriptor acepta y reconoce que una vez reciba el citado correo electrónico, se entenderá que ha sido emitido el certificado. Se entenderá que se ha recibido el correo electrónico donde se notifica la emisión de un certificado, cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección de correo electrónico que el suscriptor reportó en el formulario de solicitud. En el caso en que el suscriptor solicite que la emisión de la firma sea en un dispositivo criptográfico, se entenderá como entregado una vez firme la carta de entrega al operador logístico.

6.10.5 Forma en la que se acepta la renovación de un certificado

No se requiere confirmación de parte del suscriptor o responsable como aceptación de la renovación de certificado recibido. Se considera que un certificado renovado es aceptado por el suscriptor o responsable desde el momento que solicita su expedición, por ello, si la información contenida en el certificado expedido no corresponde al estado actual de la misma o no fue suministrada correctamente se debe solicitar su revocación por parte del solicitante o responsable y éste así lo acepta.

6.10.6 Publicación del certificado renovado por la ECD con cambio de llaves

No aplica por cuanto ECD GSE no publica los certificados.

6.10.7 Notificación de la emisión de un certificado renovado por la ECD a otras entidades

No existen entidades externas a las que se requiera ser notificada la emisión de un certificado renovado.

6.11 Modificación de certificados

Los certificados digitales emitidos por ECD GSE no puede ser modificados, es decir, no aplican enmiendas. En consecuencia, el suscriptor debe solicitar la emisión de un nuevo certificado digital. En este evento se expedirá un nuevo certificado al suscriptor; el costo de esta modificación será asumido completamente por el suscriptor conforme a las tarifas informadas por ECD GSE o según las condiciones definidas a nivel contractual.

6.11.1 Circunstancias para la modificación de un certificado

No aplica ya que los certificados digitales emitidos por ECD GSE no pueden ser modificados.

6.11.2 Quién puede solicitar una modificación

No aplica ya que los certificados digitales emitidos por ECD GSE no pueden ser modificados.

6.11.3 Trámites para la solicitud de modificación de un certificado

No aplica ya que los certificados digitales emitidos por ECD GSE no pueden ser modificados.

6.11.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado

No aplica ya que los certificados digitales emitidos por ECD GSE no pueden ser modificados.

6.11.5 Forma en la que se acepta la modificación de un certificado

No aplica ya que los certificados digitales emitidos por ECD GSE no pueden ser modificados.

6.11.6 Publicación del certificado modificado por la ECD

No aplica ya que los certificados digitales emitidos por ECD GSE no pueden ser modificados.

6.11.7 Notificación de la emisión de un certificado por la ECD a otras entidades

No aplica ya que los certificados digitales emitidos por ECD GSE no pueden ser modificados.

6.12 Revocación y suspensión de certificados

6.12.1 Circunstancias para la revocación de un certificado.

El suscriptor o responsable puede voluntariamente solicitar la revocación de su certificado digital en cualquier instante conforme a lo descrito en el artículo 37 de la Ley 527 de 1999, pero está obligado a solicitar la revocación de su certificado digital bajo las siguientes situaciones:

a. Por pérdida o inutilización de la clave privada o certificado digital.
b. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.
c. Cambios en las circunstancias por la cuales ECD GSE autorizó la emisión del certificado digital.
d. Si durante el periodo de vigencia parte o toda la información contenida en el certificado digital pierde actualidad o validez.

Si el suscriptor o responsable no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.

El suscriptor o responsable reconoce y acepta que los certificados deben ser revocados cuando GSE conoce o tiene indicios o confirmación de ocurrencia de alguna de las siguientes circunstancias:

a. A petición del suscriptor, responsable o un tercero en su nombre y representación.
b. Por muerte del suscriptor o responsable.
c. Por la confirmación o evidencia de que alguna información o hecho contenido en el certificado digital es falso.
d. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometida de manera material que afecte la confiabilidad del certificado.
e. Por orden judicial o de entidad administrativa competente.
f. Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
g. Por incapacidad sobrevenida del suscriptor o responsable.
h. Por liquidación de la persona jurídica representada que consta en el certificado digital.
i. Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
j. Por pérdida o inutilización del dispositivo criptográfico que haya sido entregado por ECD GSE.
k. Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato.
l. Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la confiabilidad del certificado digital.
m. Por el manejo indebido por parte del suscriptor del certificado digital.
n. Por el incumplimiento del suscriptor o de la persona jurídica que representa o a la que está vinculado a través del documento términos y condiciones o responsable de certificados digitales de la ECD GSE.
o. Conocimiento de eventos que modifiquen el estado inicial de los datos suministrados, entre otros: terminación de la Representación Legal, terminación del vínculo laboral, liquidación o extinción de la personería jurídica, cesación en la función pública o cambio a una distinta.
p. En cualquier momento que se evidencie falsedad en los datos suministrados por el solicitante, suscriptor o responsable.
q. Por incumplimiento por parte de la ECD GSE, el suscriptor o responsable de las obligaciones establecidas en la DPC.
r. Por incumplimiento en el pago de los valores por los servicios de certificación, acordados entre el solicitante y ECD GSE.

No obstante, las causales anteriores, ECD GSE, también podrá revocar certificados cuando a su juicio se pueda poner en riesgo la credibilidad, confiabilidad, valor comercial, buen nombre de la ECD GSE, idoneidad legal o moral de todo el sistema de certificación.

6.12.2 Quién puede solicitar una revocación

El suscriptor o responsable, un tercero de buena fe o cualquier persona interesada cuando tenga constancia demostrable de conocimiento de hechos y causales de revocación mencionadas en el apartado ***Circunstancias para la revocación de un certificado*** de esta DPC y que comprometan la llave privada.

Un tercero de buena fe o cualquier persona interesada que tenga constancia demostrable que un certificado digital ha sido empleado con fines diferentes a los expuestos en el aparte ***Usos adecuados del certificado*** de esta DPC.

Cualquier persona interesada que tenga constancia demostrable que el certificado no está en poder del suscriptor o responsable.

El equipo de TI de la CA como máximo ente de control que tiene atribuida la administración de la seguridad de la infraestructura tecnológica de ECD GSE, está en capacidad de solicitar la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la llave privada del suscriptor, responsable o cualquier otro hecho de acuerdo con las circunstancias para la revocacion de un certificado.

6.12.3 Procedimiento de solicitud de revocación

Las personas interesadas tendrán la oportunidad de solicitar la revocación de un certificado digital cuyas causas están especificadas en esta DPC lo pueden hacer bajo los siguientes procedimientos:

- En las oficinas de GSE.
  En horario de atención al público se reciben las solicitudes escritas de revocación de certificados digitales firmadas por los suscriptores y/o responsables suministrando el documento de identificación original.

- Solicitud de revocación en línea:
  El suscriptor y/o responsable, podrá llevar a cabo el proceso de revocación del certificado digital por medio del portal web de GSE S.A., https://gse.com.co/consultas-en-linea/ - Solicite su revocación, al diligenciar la solicitud se visualizarán los certificados digitales vigentes, se debe seleccionar el certificado a revocar y a su correo electrónico registrado, le llegará una notificación con el código de seguridad para completar el diligenciamiento de la solicitud de revocación en línea, el suscriptor y/o responsable deberá seleccionar el motivo de la revocación, ingresar el código de seguridad, aceptar los Términos y Condiciones y revocar su certificado digital; una vez la solicitud termine, el certificado seleccionado se revocará automáticamente y al correo electrónico registrado se le enviará la confirmación de revocación. Otro medio dispuesto para realizar la revocación del certificado digital por parte del suscriptor y/o responsable a través de la herramienta desde donde se radico la solicitud para la emisión del certificado digital.

- Servicio de Revocación vía correo electrónico
  Por medio de nuestro correo electrónico revocaciones@gse.com.co, los suscriptores y/o responsables pueden solicitar la revocación de certificados digitales conforme a las causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta DPC, enviando carta de solicitud de revocación firmada digitalmente o correo electrónico con los datos del suscriptor y causal de revocación.

  Nota: La ECD – GSE pone a disposición una plantilla guía para realizar la carta de solicitud de revocación la cual está disponible en la página web https://gse.com.co/guias-y-manuales, opción Revocaciones y Certificados raíz y subordinado

  La ECD por medio del área de TI y el personal designado para desarrollar las actividades de certificación de acuerdo con el procedimiento de revocación de certificados digitales realizará la verificación de la solicitud de revocación.

6.12.4 Periodo de gracia de solicitud de revocación

Previa validación de la autenticidad de una solicitud de revocación, ECD GSE procederá en forma inmediata con la revocación solicitada, dentro de los horarios de oficina de éste. En consecuencia, no existe un periodo de gracia que permita al solicitante cancelar la solicitud. Si se trató de una solicitud errónea, el suscriptor o responsable debe solicitar un nuevo certificado, pues el certificado revocado perdió su validez inmediatamente fue validada la solicitud de revocación y ECD GSE no podrá reactivarlo.

El procedimiento utilizado por ECD GSE para verificar la autenticidad de una solicitud de revocación formulada por una persona determinada, es verificar la solicitud de acuerdo con el apartado anterior.

Una vez solicitada la revocación del certificado, si se evidencia que dicho certificado es utilizado vinculado con la llave privada, el suscriptor o responsable releva de toda responsabilidad legal a ECD GSE, toda vez que reconoce y acepta que el control, custodia y confidencialidad de la llave privada es responsabilidad exclusiva de este.

6.12.5 Plazo en el que la ECD debe resolver la solicitud de revocación

La solicitud de revocación de un certificado digital debe ser atendida con la máxima urgencia, sin que su revocación tome más de tres (3) días hábiles una vez revisada la solicitud.

Una vez cumplidas las formalidades previstas para la revocación y si por alguna razón, no se hace efectiva la revocación de un certificado en los términos establecidos por esta DPC,

ECD GSE como prestador de servicios de certificación responderá por los perjuicios que se causen a los suscriptores o terceros de buena fe derivados de errores y omisiones, de mala fe de los administradores, representantes legales o empleados de ECD GSE en el desarrollo de las actividades para las cuales cuenta con autorización y para ello cuenta con un seguro de responsabilidad civil de conformidad con el *Artículo 9°. Garantías, del Decreto 333 de 2014.* ECD GSE no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante suscriptor o responsables de certificados o terceros de confianza a excepción de lo establecido por las disposiciones de la presente DPC.

6.12.6 Requisitos de verificación de las revocaciones por los terceros de buena fe

Es responsabilidad del suscriptor o responsable de un certificado digital y éste así lo acepta y reconoce, informar a los terceros de buena fe de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado. Informará igualmente el suscriptor o responsable al tercero de buena fe que, para realizar dicha consulta, dispone de la lista de certificados revocados CRL, publicada de manera de periódica por ECD GSE.

6.12.7 Frecuencia de actualización de las CRLs

La ECD GSE generará y publicará una nueva CRL cada veinticuatro (24) horas en su repositorio con una disponibilidad de consulta en línea 7x24x365, 99.9% uptime por año.

6.12.8 Tiempo máximo de latencia de las CRLs

El tiempo entre la generación y publicación de la CRL es mínimo debido a que la publicación es automática.

6.12.9 Revocación on-line/disponibilidad de verificación del estado

ECD GSE publicará tanto la CRL como el estado de los certificados revocados en repositorios de libre acceso y fácil consulta, con disponibilidad 7X24 durante todos los días del año. ECD GSE ofrece un servicio de consulta en línea basada en el protocolo OCSP en la dirección https://ocsp2.gse.com.co.

La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender la-s respuestas generadas por el servicio, tal es el caso de OPENSSL.

6.12.10 Requisitos de comprobación de la revocación on-line

Para obtener la información del estado de revocación de un certificado en un momento dado, se puede hacer la consulta en línea en la dirección https://ocsp2.gse.com.co para lo cual se debe contar con un software que sea capaz de operar con el protocolo RFC6960. La mayoría de los navegadores ofrecen este servicio.

La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender las respuestas generadas por el servicio, tal es el caso de OPENSSL.

6.12.11 Notificación de la revocación de un certificado

Dentro de las 24 horas siguientes a la revocación de un certificado, ECD GSE informa al suscriptor o responsable, mediante correo electrónico, la revocación de su certificado digital y por consiguiente el solicitante acepta y reconoce que una vez reciba el citado correo electrónico se entenderá que su solicitud fue atendida. Se entenderá que se ha recibido el correo electrónico donde se notifica la revocación de un certificado cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección correo electrónico que consta en el formulario de solicitud.
La publicación de un certificado revocado en la CRL constituye la prueba y una notificación pública de su revocación.

6.12.12 Otras formas disponibles de divulgación de información de revocación

ECD GSE mantendrá un archivo histórico hasta de tres (3) años de las CRL´s generadas y que estarán a disposición de los suscriptores mediante solicitud escrita dirigida a ECD GSE.

6.12.13 Requisitos especiales de renovación de llaves comprometidas

Si se solicitó la revocación de un certificado digital por compromiso (pérdida, destrucción, robo, divulgación) de la llave privada, el suscriptor puede solicitar un nuevo certificado digital por un periodo igual o mayor al inicialmente solicitado presentando una solicitud de renovación en relación con el certificado digital comprometido. La responsabilidad de la custodia de la llave es del suscriptor o responsable y éste así lo acepta y reconoce, por tanto, es él quien asume el costo de la renovación de conformidad con las tarifas vigentes fijadas para la renovación de certificados digitales.

6.12.14 Circunstancias para la suspensión

ECD GSE no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

6.12.14.1 Quién puede solicitar la suspensión

No aplica por cuanto ECD GSE no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

6.12.14.2 Procedimiento de solicitud de suspensión

No aplica por cuanto ECD GSE no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

6.12.14.3 Límites del periodo de suspensión

No aplica por cuanto ECD GSE no dispone del servicio de suspensión de certificados digitales, únicamente revocación.

6.13 Perfiles de certificados

Los certificados cumplen con el estándar X.509 versión 3 y para la infraestructura de autenticación se basa en el RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Contenido de los certificados. Un certificado emitido por ECD GSE, además de estar firmado digitalmente por ésta, contendrá como mínimo lo siguiente:

1. Nombre, dirección y domicilio del suscriptor o responsable.
2. Identificación del suscriptor o responsable nombrado en el certificado.
3. El nombre, la dirección y el lugar donde realiza actividades la ECD.
4. La clave pública del suscriptor o persona jurídica.
5. La metodología para verificar la firma digital del suscriptor o persona jurídica impuesta en el mensaje de datos.
6. El número de serie del certificado.
7. Fecha de emisión y expiración del certificado.

6.13.1 Descripción del contenido de los certificados

Campo	Valor o restricciones RSA	Valor o restricciones ECDSA
Versión	3 (0x2)	3 (0x2)
Número de Serie	Identificador único emitido por ECD GSE	Identificador único emitido por ECD GSE
Algoritmo de Firma	SHA256withRSAEncryption	SHA384withECDSA
Emisor	Ver sección “Reglas para la interpretación de varias formas de nombre”. Para ECD GSE como emisor se especifica: E=info@gse.com.co, CN=Autoridad Subordinada 01 GSE, OU=PKI, O=GSE, L=Bogota D.C., C=CO	Ver sección “Reglas para la interpretación de varias formas de nombre”. Para ECD GSE como emisor se especifica: STREET=www.gse.com.co, E=info@gse.com.co, CN=GSE ECDSA SUBORDINADA, SN=900204278, OU=GSE ECDSA R2 SUB1, O=GESTION DE SEGURIDAD ELECTRONICA S.A, L=Bogota D.C., S=Distrito Capital, C=CO
Válido desde	Especifica la fecha y hora a partir de la cual el certificado es válido.	Especifica la fecha y hora a partir de la cual el certificado es válido.
Válido hasta	Especifica la fecha y hora a partir de la cual el certificado deja de ser válido.	Especifica la fecha y hora a partir de la cual el certificado deja de ser válido.

Campo	Valor o restricciones RSA	Valor o restricciones ECDSA
Sujeto	Conforme a la política del Anexo 1 y las *"Reglas para la interpretación de varias formas de nombre".*	Conforme a la política del Anexo 1 y las *"Reglas para la interpretación de varias formas de nombre".*
Llave pública del Sujeto	Codificado de acuerdo con la RFC 5280. Los certificados emitidos por ECD GSE tienen una longitud de 2048 bits y algoritmo RSA.	Codificado de acuerdo con la RFC 5280. Los certificados emitidos por ECD GSE tienen una longitud de 256 bits y algoritmo EC.
Identificador de llave de la autoridad	Es utilizado para identificar el certificado raíz en la jerarquía de certificación. Normalmente referencia el campo "Subject Key Identifier" de ECD GSE como entidad emisora de certificación digital.	Es utilizado para identificar el certificado raíz en la jerarquía de certificación. Normalmente referencia el campo "Subject Key Identifier" de ECD GSE como entidad emisora de certificación digital.
Identificador de la llave del sujeto	Es usado para identificar un certificado que contiene una determinada llave pública.	Es usado para identificar un certificado que contiene una determinada llave pública.
Directivas del Certificado	Describe las políticas aplicables al certificado, especifica el OID y la dirección URL donde se encuentra disponible las políticas de certificación.	Describe las políticas aplicables al certificado, especifica el OID y la dirección URL donde se encuentra disponible las políticas de certificación.
Uso de la llave	Especifica los usos permitidos de la llave. Es un CAMPO CRÍTICO.	Especifica los usos permitidos de la llave. Es un CAMPO CRÍTICO.
Punto de distribución de la CRL	Es usado para indicar las direcciones donde se encuentra publicada la CRL de ECD GSE. En el certificado de la ECD Raíz, este atributo no se especifica.	Es usado para indicar las direcciones donde se encuentra publicada la CRL de ECD GSE. En el certificado de la ECD Raíz, este atributo no se especifica.
Acceso a la información de la Autoridad	Es usado para indicar las direcciones donde se encuentra el certificado raíz de ECD GSE. Además, para indicar la dirección para acceder al servicio de OCSP. En el certificado raíz de ECD GSE, este atributo no se especifica.	Es usado para indicar las direcciones donde se encuentra el certificado raíz de ECD GSE. Además, para indicar la dirección para acceder al servicio de OCSP. En el certificado raíz de ECD GSE, este atributo no se especifica.
Nombre alternativo del sujeto	Es usado para indicar la dirección de correo electrónico y adicionalmente para indicar el código acreditación asignado por el ONAC. Nombre RFC822=correo@empresa.com Dirección URL= https://gse.com.co/documentos/certificaciones/acreditacion/16-ECD-001.pdf	Es usado para indicar la dirección de correo electrónico y adicionalmente para indicar el código acreditación asignado por el ONAC. Nombre RFC822=correo@empresa.com Dirección URL= https://gse.com.co/documentos/certificaciones/acreditacion/16-ECD-001.pdf
Usos extendidos de la llave	Se especifican otros propósitos adicionales al uso de la llave.	Se especifican otros propósitos adicionales al uso de la llave.
Restricciones básicas	La extensión "PathLenConstraint" indica el número de sub-niveles que se admiten en la ruta del certificado. No existe restricción para ECD GSE, por tanto, es cero.	La extensión "PathLenConstraint" indica el número de sub-niveles que se admiten en la ruta del certificado. No existe restricción para ECD GSE, por tanto, es cero.

6.13.1.1 Número de versión

Los certificados emitidos por ECD GSE cumplen con el estándar X.509 Versión 3.

6.13.1.2 Extensiones del certificado

En el Anexo 1 de esta DPC se describe de forma detallada los certificados emitidos por GSE.

6.13.1.3 Key Usage

El "key usage" es una extensión crítica que indica el uso del certificado de acuerdo con el RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

6.13.1.4 Extensión de política de certificados

La extensión de "certificatepolicies" del X.509 versión 3 es el identificador del objeto de esta DPC de acuerdo con la sección identificador de objeto de la Política de Certificación de esta DPC. La extensión no es considerada como crítica.

6.13.1.5 Nombre alternativo del sujeto

La extensión "sujectAltName" es opcional y el uso de esta extensión es "No crítico".

6.13.1.6 Restricciones básicas

Para el caso de ECD GSE en el campo "PathLenConstraint" de certificado de las subordinadas tiene un valor de 0, para indicar que la ECD GSE no permite más sub-niveles en la ruta del certificado. Es un campo crítico.

6.13.1.7 Uso extendido de la llave

Esta extensión permite definir otros propósitos adicionales de la llave. Es considerada no crítica. Los propósitos más comunes son:

OID	Descripción	Tipos de Certificados
1.3.6.1.5.5.7.3.4	Protección de correo	Firma Digital de persona natural y Agente Electrónico
1.3.6.1.5.5.7.3.8	Sellado de tiempo	Sellado de tiempo
1.3.6.1.5.5.7.3.34	Autenticación servidor web TLS	Todos los tipos de certificado

6.13.1.8 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption

El identificador de objeto del algoritmo de la clave pública es: 1.2.840.113549.1.1.1 rsaEncryption

El identificador de objeto del algoritmo de firma es:
1.2.840.10045.4.3.3 SHA384WITHECDSA.

El identificador de objeto del algoritmo de la clave pública es:
1.2.840.10045.2.1 id-ecPublicKey

6.13.1.9 Formatos de nombres

De conformidad con lo especificado en el apartado **Tipos de nombres** de esta DPC.

6.13.1.10 Restricciones de los nombres

Los nombres se deben escribir en mayúsculas y sin tildes.

El código del país se asigna de acuerdo con el estándar ISO 3166-1 “Códigos para la representación de los nombres de los países y sus subdivisiones. Parte 1: Códigos de los países”. Para el caso de Colombia es “CO”.

6.13.1.11 Identificador de objeto de la Política de Certificación

El identificador de objeto de la Política de certificado correspondiente a cada tipo de certificado es una subclase de la clase definida en el numeral **Nombre del documento e identificación** de esta DPC, conforme se establece en las Políticas de Certificado para certificados digitales.

6.13.1.12 Uso de la extensión Policy Constrains

No se estipula.

6.13.1.13 Sintaxis y semántica de los Policy Qualifiers

El calificador de la política está definido en la extensión de “Certificate Policies” y contiene una referencia al URL donde esta publicada la DPC.

6.13.1.14 Tratamiento semántico para la extensión Certificate Policies

No se estipula.

6.14 Servicios de información del estado de certificados

6.14.1 Perfil de CRL

Las CRL´s emitidas por ECD GSE cumplen con la RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile V2” y contienen los siguientes elementos básicos:

6.14.1.1 Número de versión

Las CRL´s emitidas por ECD GSE cumplen con el estándar X.509 versión 2.

6.14.1.2 CRL y extensiones CRL

La información sobre el motivo de la revocación de un certificado estará incluida en la CRL, utilizando las extensiones de la CRL y más específicamente en el campo de motivos de revocación (reasonCode).

6.14.1.3 Disponibilidad CRL

Conforme a lo indicado en el numeral 6.12.9 Revocación on-line/disponibilidad de verificación del estado.

6.14.1.4 Perfil OCSP

El servicio OCSP cumple con lo estipulado en el RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

6.14.1.5 Número de versión

Cumple con la OCSP Versión 1 del RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”.

6.14.1.6 Extensiones OCSP

No aplica

6.14.1.7 Disponibilidad OCSP

Conforme a lo indicado en el numeral 6.12.9 Revocación on-line/disponibilidad de verificación del estado.

6.14.2 Características operacionales

Para la consulta del estado de los certificados emitidos por ECD GSE, se dispone de un servicio de consulta en línea basada en el protocolo OCSP en la dirección https://ocsp2.gse.com.co. El suscriptor o responsable de enviar una petición de consulta sobre el estado del certificado a través del protocolo OCSP, que, una vez consultada la base de datos, es atendida mediante una respuesta vía http o la consulta via CRL.

6.14.3 Características opcionales

Para obtener la información del estado de certificado en un momento dado, se puede hacer la consulta en línea en la dirección https://ocsp2.gse.com.co, para lo cual se debe contar con un software que sea capaz de operar con el protocolo OCSP. La mayoría de los navegadores ofrecen este servicio o consulta a la CRL publicada en el portal https://crl2.gse.com.co.

La validación en línea de certificados digitales mediante OCSP se debe realizar con una herramienta que implemente el protocolo OCSP y sea capaz de entender las respuestas generadas por el servicio, tal es el caso de OPENSSL.

6.15 Finalización de la vigencia de un certificado

ECD GSE da por finalizada la vigencia de un certificado digital emitido ante las siguientes circunstancias:

- Pérdida de validez por revocación del certificado digital.
- Vencimiento del periodo para el cual un suscriptor contrató la vigencia del certificado.

6.16 Custodia y recuperación de llaves

6.16.1 Almacenamiento de la clave privada del suscriptor

La clave privada del suscriptor solo puede ser almacenada en un dispositivo criptográfico hardware (token o HSM). Los dispositivos criptográficos en hardware utilizados por ECD GSE cumplen con las certificaciones como chip criptográfico: nivel de seguridad CC EAL5+ PP 9806, BSI-PP-002-2001, FIPS 140-2 NIVEL 3 y las certificaciones SO del chip criptográfico: nivel de seguridad CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3) – BSI –DSZ-CC-0422-2008 y soportan los estándares PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPsec/IKE.

La ECD GSE publica en las Políticas de Certificado Digital para Certificados Digitales las características de los dispositivos criptográficos que ofrece a los suscriptores que así lo solicitan para creación y almacenamiento de sus claves privadas.

6.16.2 Almacenamiento de la clave privada a un responsable

La clave privada del suscriptor solo puede ser almacenada en un dispositivo criptográfico hardware (token o HSM).

El dispositivo criptográfico en hardware utilizado por ECD GSE es una tarjeta criptográfica o token USB que cumple los requerimientos mínimos de la normatividad vigente y las garantías de la certificación europea Common Criteria como “dispositivo seguro de creación de firma”.

Estos dispositivos criptográficos seguros de creación de firma, cumplen con las certificaciones como chip criptográfico: nivel de seguridad CC EAL5+ PP 9806, BSI-PP-002-2001, FIPS 140-2 NIVEL 3 y las certificaciones SO del chip criptográfico: nivel de seguridad CC EAL4+ BSI-PP-0006-2002 (CWA 14169 SSCD Type-3) – BSI –DSZ-CC-0422-2008 y soportan los estándares PKCS#11, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPsec/IKE.

La ECD GSE publica en las políticas de Certificado Digital para Certificados Digitales las características de los dispositivos criptográficos que ofrece a los suscriptores que así lo solicitan para creación y almacenamiento de sus claves privadas.

6.16.3 Prácticas y políticas de custodia y recuperación de llaves

La generación de la llave privada es almacenada sobre un dispositivo seguro (hardware), del cual no se puede exportar. En consecuencia, no es posible la recuperación de la llave privada del suscriptor. La responsabilidad de la custodia de la llave privada es del suscriptor y éste así lo acepta y reconoce.

6.16.4 Prácticas y políticas de custodia y recuperación de la clave de sesión

La recuperación de la clave de sesión del suscriptor o PIN no es posible ya que el único responsable de asignarla y este así lo declara y acepta. La responsabilidad de la custodia de la clave de sesión o PIN es del suscriptor quien acepta no mantener registros digitales, escritos o en cualquier otro formato y quien se obliga a memorizarlo, por lo que su olvido requiere la solicitud de revocación del certificado y la solicitud de uno nuevo por cuenta del suscriptor.

7. CONTROLES FÍSICOS DE LA INSTALACION, GESTIÓN Y OPERACIONALES

7.1. Ubicación física y construcción

ECD GSE dispone de medidas de seguridad para el control de acceso al edificio donde se encuentra su infraestructura, los servicios de certificación digitales regulados y prestados a través de esta DPC se realizan a través de un proveedor de servicios. Solo se permite el acceso al rack que alberga los servidores a través del cual se manejan los servicios de comunicación de la ECD GSE de personas previamente identificadas y autorizadas que porten en un lugar visible el carné de visitantes.

El proveedor de la infraestructura tecnológica de la ECD GSE garantiza que los servidores de la PKI se encuentran en operación continúa de manera virtual en la nube de Amazon. Dicho proveedor cuenta con procedimientos para realizar las operaciones de administración de la infraestructura de comunicaciones de la ECD GSE y a donde únicamente tiene acceso el personal autorizado.

El área restringida del centro de comunicaciones cumple con los siguientes requisitos:

a. Ingresan únicamente personas autorizadas.
b. Los equipos de comunicación crítica están debidamente protegidos en racks.
c. No posee ventanas hacia el exterior del edificio.
d. Cuenta con un circuito cerrado de televisión las 24 horas, con cámaras tanto al interior como al exterior del centro de cómputo.
e. Cuenta con control de acceso.

f. Sistemas de protección y prevención de incendios: detectores de humo, sistema de extinción de incendios.
g. Cuenta con personal capacitado para actuar ante eventos catastróficos
h. Cuenta con un sistema detector de intrusos
i. El cableado está debidamente protegido contra daños, intentos de sabotaje o interceptación por medio de canaletas.
j. No existe tránsito frecuente de personas por los alrededores.

7.2. Acceso físico

Existen varios niveles de seguridad que restringen el acceso a la infraestructura de comunicaciones a través de la cual ECD GSE presta sus servicios y cada uno ellos disponen de sistemas de control de acceso físico. Las instalaciones cuentan con un servicio de circuito cerrado de televisión y con personal de vigilancia. Existen dentro de las instalaciones zonas restringidas que por el tipo de equipos de comunicaciones considerados críticos y operaciones sensibles que se manejan tienen acceso permitido solo a ciertas personas.

7.3. Alimentación eléctrica y aire acondicionado

El centro de comunicaciones cuenta con un sistema de aire acondicionado y dispone de un adecuado suministro de electricidad con protección contra caídas de tensión y otras fluctuaciones eléctricas que podrían eventualmente afectar sensiblemente a los equipos y producir daños graves. Adicionalmente, se cuenta con un sistema de respaldo que garantiza que no haya interrupción en el servicio con una autonomía suficiente para garantizar la continuidad en el servicio. En caso de una falla en el sistema de respaldo, se cuenta con el tiempo suficiente para hacer un apagado controlado.

7.4. Exposición al agua

El centro de comunicaciones se encuentra aislado de posibles fuentes de agua y cuenta con sensores de detección de inundaciones conectados al sistema general de alarma.

7.5. Controles físicos de la infraestructura tecnológica a través de la cual ECD GSE presta sus servicios

Los servicios de infraestructura tecnológica a través de la cual ECD GSE presta sus servicios, está contratado con el proveedor Paynet SAS.

7.6. Prevención y protección de incendios

El centro de comunicaciones cuenta de un sistema de detección de incendios y un sistema de extinción de incendios. Se cuenta con un sistema de cableado que protege las redes internas.

7.7. Sistema de almacenamiento

Se cuenta con procedimientos de toma de backups, restauración y pruebas de estos por medio de electrónicos que reposan en la nube de Google.

Los servidores misionales se encuentran en Amazon, sin embargo, los equipos locales cuentan con estas características, los Backups se realizan por medio de la plataforma de Amazon y se ejecutan pruebas de restauración sobren los mismos.

7.8. Eliminación del material de almacenamiento de la información

Todo documento en papel que contenga información sensible de la entidad y que ha cumplido su vida útil deberá ser destruido físicamente para garantizar la imposibilidad de recuperación de información. Si el documento o información está almacenado en un medio magnético se debe formatear, borrar permanentemente o destruir físicamente el dispositivo en casos extremos como daños de dispositivos de almacenamiento o dispositivos no reutilizables, siempre garantizando que no sea posible la recuperación de la información por cualquier medio conocido o no conocido por el momento.

7.9. Backup fuera de la instalación

ECD GSE mantendrá una copia de respaldo de las bases de datos en Amazon que se llevará a la réplica en caso de que se requiera para la restauración

7.10. Controles de procedimiento

7.10.1. Roles de confianza

La RA ha definido los siguientes roles, los cuales no podrán ser desempañados por la misma persona dentro del área:

- **Agentes RA:** Personas responsables de las operaciones diarias tales como los son: revisión y aprobación de las solicitudes atendiendo todas las actividades relacionadas con los servicios de certificación digital prestados por la ECD GSE a través de la RA, las funciones y responsabilidades de los agentes de la RA están definidos de acuerdo con los Perfiles y Funciones de la ECD GSE.

- **Administrador RA:** La persona responsable por administrar y configurar la RA.

- **Auditor RA:** Persona capacitada e imparcial encargada de evaluar el cumplimiento de los requisitos de la RA, auditando los sistemas de información de la RA aclarando que su rol es distinto al del auditor interno de los sistemas de gestión.

7.10.2. Número de personas requeridas por tarea

Para cada uno de los roles mencionados se requiere una persona. La ECD garantiza al menos la colaboración de dos personas para realizar las tareas que afectan a la gestión de claves criptográficas de la propia ECD.

7.10.3. Identificación y autenticación para cada rol

Los Agentes RA y Administrador RA se autentican mediante certificados digitales emitidos por ECD GSE.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales.

7.10.4. Roles que requieren segregación de funciones

El rol de Administrador RA, los Agentes RA y Auditor RA son independientes.

7.11. Controles de personal

7.11.1. Requisitos sobre la cualificación, experiencia y conocimiento profesionales

Se tiene definido un proceso de selección de personal que tiene como base el perfil de cada uno de los cargos involucrados en el proceso de emisión de certificados digitales. El candidato a un cargo debe tener la formación, experiencia, conocimientos y habilidades definidas en el documento Perfil y funciones de cargo.

7.11.2. Procedimiento de comprobación de antecedentes

Los candidatos a ocupar cargos del ciclo de certificación deben presentar su certificado de antecedentes vigente, según se tiene establecido en los procesos internos de talento humano de la ECD GSE.

7.11.3. Requisitos de formación

Los requisitos de formación para cada uno de los cargos mencionados se encuentran en el Perfil y funciones de cargo que es dado a conocer a la persona seleccionada para ocupar el cargo como parte de su inducción. Los aspectos más destacados que son parte de la formación son:

- Conocimiento de la Declaración de Prácticas de Certificación.
- Conocimiento de la normatividad vigente y relacionada con las entidades de certificación abierta y los servicios que presta.
- Conocimiento de las Políticas de Seguridad y la aceptación de un acuerdo de confidencialidad sobre la información que se maneja en virtud del cargo.
- Conocimiento de la operación del software y hardware para cada papel específico.
- Conocimiento de los procedimientos de seguridad para cada rol específico.
- Conocimiento de los procedimientos de operación y administración para cada rol específico.
- Conocimiento de los Planes de continuidad de negocio

7.11.4. Requisitos y frecuencia de actualización de formación

Dentro de la programación anual de capacitación se incluye una actualización en Seguridad de la Información para los integrantes del Ciclo de emisión de certificados digitales.

7.11.5. Frecuencia y secuencia de rotación de tareas

No existe rotación de tareas en los cargos mencionados.

7.11.6. Sanciones por actuaciones no autorizadas

Es calificada como falta grave ejecutar acciones no autorizadas y las personas serán sancionadas de conformidad con el proceso disciplinario.

7.11.7. Requisitos de contratación de terceros

Entre los requisitos de contratación de terceros está el conocimiento de las Políticas de Seguridad y una cláusula de confidencialidad sobre la información que sea suministrada o conocida por razones del vínculo contractual con GSE.

7.11.8. Documentación proporcionada al personal

La documentación mencionada en el numeral **Requisitos de Formación** está publicada para fácil consulta y forma parte de la inducción de personal.

7.12. Procedimientos de auditoría de seguridad de la PKI

Los procedimientos de auditoría de seguridad son ejecutados internamente o por proveedores de auditoría de tercera parte.

7.12.1. Tipos de eventos registrados

Las actividades más sensibles del ciclo de certificación requieren el control y seguimiento de eventos que se pueden presentar durante su operación. De conformidad con su nivel de criticidad los eventos se clasifican en:

- Informativo: Una acción terminó de manera exitosa
- Tipo marca: Inicio y finalización de una sesión
- Advertencia: Presencia de un hecho anormal pero no de una falla
- Error: Una operación generó una falla predecible
- Error fatal: Una operación generó una falla impredecible

7.12.2. Frecuencia de procesado de registros de auditoría (log)

Los registros de auditoria son revisados utilizando procedimientos manuales y/o automáticos.

La revisión de los logs se realiza una vez por semana o cuando se detecte una alerta de seguridad o existan indicios de un funcionamiento no usual de los sistemas.

7.12.3. Periodo de retención de los registros de auditoría

Los registros de auditoría se mantienen durante tres (3) años después de la última modificación del fichero, con eso se garantiza poder revisar los problemas presentados con los que se hayan presentado en el histórico. Una vez transcurridos los 3 años y con autorización del Comité de Gerencia de GSE, se puede proceder a destruirlos, no obstante, si los registros se están utilizando en procesos judiciales su retención serán por tiempo indefinido.

7.12.4. Protección de los registros de auditoría

Los logs de auditoría del sistema de información se conservan de igual manera manteniendo una copia en el sitio y otra copia fuera de las instalaciones.

7.12.5. Procedimientos de backup de los registros de auditoría

Los backups de los registros de auditoria se replican a un sitio de logs centralizados

7.12.6. Sistema de recogida de información de auditoría (interna o externa)

El sistema de recopilación de información de auditoría se basa en los registros automáticos de las aplicaciones que soportan el ciclo de certificación incluyendo los logs de aplicación, logs de seguridad y logs del sistema. Los cuales se almacenan en CloudWatch y bases de datos para su monitoreo

7.12.7. Notificación al sujeto causa del evento

A juicio del Oficial de Seguridad de la Información, se hará la notificación al sujeto causa de un incidente de seguridad detectado a través de los logs de auditoría a fin de tener respuesta formal sobre lo sucedido.

7.12.8. Análisis de vulnerabilidades

Además de las revisiones periódicas de logs, ECD GSE realiza de manera esporádica o ante actividades sospechosas la revisión de estos de conformidad con los procedimientos internos establecidos. De igual manera revisa los resultados obtenidos del Ethical Hacking y las actividades descritas para subsanación de hallazgos.

7.13. Archivo de registros y eventos de la PKI

El registro de archivo y registro de eventos es ejecutado por el proveedor de los servicios de infraestructura PKI (Paynet SAS).

7.13.1. Tipos de eventos archivados

Se mantiene un archivo de registros de los eventos más relevantes sobre las operaciones realizadas durante el proceso de emisión de los certificados digitales.

7.13.2. Periodo de conservación

El periodo de conservación de este tipo de documentación es de 3 años y/o indefinido si se tienen procesos judiciales abiertos

7.13.3. Protección de archivos

Los archivos generados se conservan bajo custodia con estrictas medidas de seguridad para conservar su estado e integridad.

7.13.4. Procedimientos de backup del archivo de registros

Las copias de respaldo de los Archivos de registros se realizan según los procedimientos establecidos para copias de respaldo y recuperación de backups del resto de sistemas de información.

7.13.5. Requisitos para el sellado de tiempo de los registros

Los servidores se mantienen actualizados con la hora UTC Time (tiempo universal coordinado). Están sincronizados mediante el protocolo NTP (Network Time Protocol). Dado que de acuerdo con lo establecido en el numeral 14 del artículo 6 del Decreto número 4175 de 2011, el Instituto Nacional de Metrología IMC, es el organismo oficial que mantiene, coordina y difunde la hora legal de la República de Colombia, adoptada mediante Decreto 2707 de 1982, la sincronización se realizará con el servidor de NTP del INM.

7.13.6. Sistema de archivo de la información de auditoría (interna o externa)

La información de auditoría tanto externa como interna es almacenada y custodiada en un sitio externo a las instalaciones de ECD GSE una vez haya sido digitalizada. Los archivos de auditoría digitalizados son accedidos únicamente por el personal autorizado mediante herramientas de visualización. En Amazon se mantiene en el servicio de CloudWatch bases de datos.

7.13.7. Procedimientos para obtener y verificar información archivada.

Los archivos de registros son accedidos únicamente por el personal autorizado mediante herramientas de visualización y gestión de eventos con el propósito de verificar integridad de estos o para auditorias ante incidentes de seguridad.

7.14. Cambio de llaves de la ECD

7.14.1. Cambio de llaves de la raíz ECD GSE

El procedimiento de cambio de llaves de la Raíz de ECD GSE es el equivalente a generar un nuevo certificado digital. Los certificados emitidos por las subordinadas con la llave anterior deben ser revocados o se debe mantener la infraestructura hasta el vencimiento del último certificado emitido. Si se opta por revocar los certificados y emitir unos nuevos, estos no tendrán costo alguno para el suscriptor o responsable.

Antes de que el uso de la llave privada de ECD GSE caduque se realizará un cambio de llaves. La anterior CA raíz y su llave privada solo se usarán para la firma de la CRL mientras existan certificados activos emitidos por las subordinadas de la CA anterior. Se generará una CA raíz con una llave privada nueva y un nuevo DN. La llave pública se publicará en el mismo repositorio con un nombre nuevo que la diferencia de la anterior.

7.14.2. Cambio de llaves de una Subordinada de ECD GSE

El procedimiento de cambio de llaves de una subordinada de ECD GSE es el equivalente a generar un nuevo certificado digital. Los certificados emitidos con la llave anterior de la subordinada deben ser revocados o se debe mantener la infraestructura hasta el vencimiento del último certificado emitido. Si se opta por revocar los certificados y emitir unos nuevos, estos no tendrán costo alguno para el suscriptor o responsable.

Antes de que el uso de la llave privada de la subordinada ECD GSE caduque se realizará un cambio de llaves. La anterior subordinada de ECD y su llave privada solo se usarán para la firma de la CRL mientras existan certificados activos emitidos por la subordinada ECD anterior. Se generará una subordinada ECD GSE con una llave privada nueva y un nuevo DN. La llave pública se publicará en el mismo repositorio con un nombre nuevo que la diferencia de la anterior.

7.15. Recuperación en caso de compromiso de una llave y desastre natural u otro tipo de catástrofe

7.15.1. Procedimientos de gestión de incidentes

ECD GSE tiene establecido y probado un **Procedimiento de incidentes de Seguridad de la Información** tanto para la RA y CA que establece las acciones a seguir en caso de producirse una vulnerabilidad o un incidente de seguridad. Una vez ejecutados de manera satisfactoria los procedimientos de restablecimiento de los sistemas, se dará servicio al público.

7.15.2. Alteración de los recursos hardware, software o datos

Ante una sospecha de alteración de los recursos hardware, software, o datos se detendrá el funcionamiento de la ECD hasta que se restablezca la seguridad del entorno. Para evitar que se repita el incidente se debe identificar la causa de la alteración. Ante una ocurrencia de este hecho ECD GSE informará a ONAC dando explicación y justificación.

7.15.3. Procedimiento de actuación ante la vulnerabilidad de la llave privada de una Autoridad

ECD GSE tiene establecido y probado un Plan de Continuidad de Negocio de la CA que define las acciones a seguir en caso de producirse una vulnerabilidad de la llave privada de la raíz de ECD GSE o de una de sus subordinadas. En estos casos se deben revocar de manera inmediata las llaves privadas comprometidas de la ECD GSE y los certificados firmados bajo su jerarquía. Se debe generar una nueva llave privada y a solicitud de los suscriptores y/ responsables se deben emitir nuevos certificados, adicionalmente, este plan se ejecutará bajo los siguientes escenarios:

a. Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
b. Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.

c. Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.
d. Cuando se presente cualquier otro evento o incidente de seguridad de la información.

En caso de compromiso de la ECD:

a) Aplicar la contención del incidente para prevenir que vuelva a ocurrir
b) Informará a todos los Suscriptores, Responsables, Tercero que confía y otras CA con los cuales tenga acuerdos u otro tipo de relación del compromiso.
c) Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.
d) Informará ONAC y a los clientes.

7.15.4. Capacidad de recuperación después de un desastre natural u otro tipo de catástrofe

ECD GSE ante un desastre natural u otro tipo de catástrofe, está en capacidad de recuperar los servicios más críticos del negocio, descritos en el documento Plan de Continuidad de Negocio de la RA y CA, dentro de las cuarenta y ocho (48) horas posteriores a la ocurrencia del evento o dentro del RTO del proceso. El restablecimiento de otros servicios como la emisión de certificados digitales se hará entre los cinco (5) días después de la ocurrencia del evento o según el RPO especificado en el documento de plan de Continuidad de negocio.

7.16. Cese de una ECD

Conforme a lo dispuesto en el artículo 34 de la ley 527 de 1999, modificado por el artículo 163 del decreto ley 019 de 2012 y conforme al Decreto 333 de 2014, las entidades de certificación digital abiertas deberán informar de la cesación de actividades a ONAC y a la Superintendencia de Industria y Comercio con una antelación mínima de 30 días.

La ECD - GSE informará a todos los suscriptores y/o responsables mediante dos avisos publicados en diarios o medios de amplia circulación nacional, con un intervalo de 15 días, sobre:

a. La terminación de la actividad o actividades y la fecha precisa de cesación.
b. Las consecuencias jurídicas de la cesación respecto a los servicios acreditados
c. La posibilidad de que un suscriptor obtenga el reembolso equivalente al valor del tiempo de vigencia restante sobre el servicio contratado.
d. La autorización emitida por la Superintendencia de Industria y Comercio para que la ECD pueda cesar el servicio, y si es el caso, el operador de la CRL responsable de la

publicación de los certificados emitidos por la ECD - GSE hasta cuando expire el último de ellos.

ECD GSE informará el nombre de la entidad que garantizará la continuidad del servicio para quienes hayan contratado, directamente o a través de terceros servicios de la ECD GSE, sin costos adicionales, de no aceptar la continuación del servicio a través del tercero el suscriptor y/o responsable podrá solicitar la revocación y el reembolso equivalente al valor del tiempo de vigencia restante del servicio de certificación digital, si lo solicitan dentro de los dos (2) meses siguientes a la segunda publicación en la página web y avisos.

8. CONTROLES TÉCNICOS DE SEGURIDAD

8.1 Generación e instalación del par de llaves

8.1.1 Generación del par de llaves

8.1.1.1 Generación del par de llaves de la ECD Raíz

La generación del par de llaves de la ECD Raíz, se realizó en las instalaciones del proveedor de servicios de plataforma con las más estrictas medidas de seguridad y bajo el protocolo de ceremonia de generación de llaves establecido para este tipo de eventos y en presencia de un delegado de ECD GSE. Para el almacenamiento de la llave privada se utilizó un dispositivo criptográfico homologado FIPS 140-2 nivel 3.

8.1.1.2 Generación del par de llaves de las subordinadas de ECD GSE

La generación del par de llaves de las subordinadas de ECD GSE, se realizó en las instalaciones del proveedor de servicios de ECD GSE bajo el protocolo de ceremonia de generación de llaves. Para el almacenamiento de la llave privada subordinada se utiliza un dispositivo criptográfico homologado FIPS 140-2 nivel 3.

8.1.1.3 Generación del par de llaves de los suscriptores o responsables de ECD GSE

La generación del par de llaves de los suscriptores de ECD GSE, se realiza en las instalaciones del proveedor de servicios de ECD GSE. Para el almacenamiento de la llave privada del suscriptor se utiliza un dispositivo criptográfico homologado FIPS 140-2 nivel 3.

8.1.2 Entrega de la llave privada a los suscriptores

La llave privada es entregada al suscriptor y/o responsable en su dispositivo criptográfico y no es posible la extracción de la misma. No existe por tanto ninguna copia de llave privada del suscriptor.

8.1.3 Entrega de la llave pública al emisor del certificado

La llave pública es enviada a la ECD GSE como parte de la petición de solicitud del certificado digital en formato PKCS#10.

8.1.4 Entrega de la llave pública de la ECD a terceros aceptantes

La llave pública de la ECD Raíz y de la ECD Subordinada está incluida en su certificado digital.

Los certificados de la ECD Raíz pueden ser consultados por los terceros de confianza en los repositorios listados en el numeral 4.1Repositorios, Certificados Raíz ECD GSE.

Los certificados de la ECD Subordinada pueden ser consultados por los terceros de confianza en los repositorios listados en el numeral 4.1 Repositorios, Certificados Subordinadas ECD GSE.
¡Tamaño de las llaves ¡¡Para RSA se tienen definidos los siguientes tamaños de las llaves:¡

- ECD Raíz de ECD GSE es de 4096 bits.
- Subordinadas de ECD GSE es de 4096 bits.
- Certificados emitidos por ECD GSE a usuarios finales es de 2048 bits.

Al intentar derivar la llave privada, a partir de la llave pública de 2048 bits contenida en los certificados de usuarios finales, el problema radica, en encontrar los factores primos de dos números grandes, ya que se tendrían 2^{2047} posibilidades por cada número. Se estima que descifrar una llave pública de 2048 bits requeriría un trabajo de procesamiento del orden de 3 x10^{20} MIPS-año*.

*MIPS-año: unidad utilizada para medir la capacidad de procesamiento de un computador funcionando durante un año. Equivale al número de millones de instrucciones que es capaz de procesar un computador por segundo durante un año.

Para ECDSA se tienen definidos los siguientes tamaños de las llaves:

- ECD Raíz de ECD GSE es de 384 bits.
- Subordinadas de ECD GSE es de 384 bits.
- Certificados emitidos por ECD GSE a usuarios finales es de 256 bits.

Para curva elíptica se elige un punto base G específico y publicado para utilizar con la curva E(q) y a continuación se escoge un número entero aleatorio k como llave privada. La llave publica correspondiente seria P=k*G y se da a conocer. El problema del logaritmo discreto dice que es un problema de complejidad exponencial obtener k a partir de P. Se estima que se requieren 2.4x10^{26} MIPS-año para derivar una llave publica de curva elíptica de 256 bits.

8.1.5 Parámetros de generación de la llave pública y verificación de la calidad

La llave pública de la ECD Raíz está codificada de acuerdo con el estándar RFC 5280 y PKCS#11. El algoritmo de firma utilizado en la generación de las llaves es el RSA o EC.

La llave pública de las subordinadas de ECD GSE está codificada de acuerdo con el estándar RFC 5280 y PKCS#11. El algoritmo de firma utilizado en la generación de las llaves es el RSA o EC.

La llave pública de los certificados de usuario final está codificada de acuerdo con el estándar RFC 5280 y PKCS#11. El algoritmo de firma utilizado en la generación de las llaves es el RSA o EC.

8.1.6 Usos permitidos de la llave (según el campo key usage de la X.509)

Los usos permitidos de la llave para cada tipo de certificado vienen establecidos por las Políticas de Certificado para certificados digitales y en las políticas definidas para cada tipo de certificado emitido por ECD GSE.

Todos los certificados digitales emitidos por ECD GSE contienen la extensión '*Key Usage'* definida por el estándar X.509 v3, la cual es calificada como crítica.

TIPO DE CERTIFICADO	KEY USAGE
Certificado de Firma	Digital Signature
Certificado de Autenticación	Non Repudiation

8.2 Protección de la llave privada y controles de ingeniería de los módulos criptográficos

8.2.1 Controles y estándares para los módulos criptográficos

Los módulos criptográficos utilizados en la creación de llaves utilizadas por ECD Raíz de Autoridad de Certificación ECD GSE cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

8.2.2 Control multipersona (n de m) de la llave privada

Las llaves privadas, de la ECD GSE Raíz y las llaves privadas de las subordinadas de ECD GSE, se encuentran bajo control multipersona. El método de activación de las llaves privadas es mediante la inicialización del software de ECD GSE por medio de una combinación de claves en poder de varias personas

8.2.3 Custodia de la llave privada

Las llaves privadas de ECD GSE se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad.

Los datos técnicos del dispositivo son los siguientes:

- **SafeNet Luna SA**

La llave privada de los certificados digitales de usuario final está bajo el exclusivo control y custodia del suscriptor o responsable. En ninguna circunstancia ECD GSE guarda copia de la llave privada del suscriptor o certificado administrado por el responsable ya que esta es generada por el mismo suscriptor o responsable y no es posible tener acceso a ella por ECD GSE.

8.2.4 Backup de la llave privada

Las llaves privadas de la ECD GSE se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (ver 8.2.3 Custodia de la llave privada**).**

Las copias de backup de las llaves privadas de la ECD GSE, están almacenadas en dispositivos externos protegidas criptográficamente por un control dual y solo son recuperables dentro de un dispositivo igual al que se generaron.

8.2.5 Archivo de la llave privada

Las llaves privadas de ECD GSE se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (ver 8.2.3 Custodia de la llave privada**).**

Las mismas se encuentran en una caja de backups criptográfica en un sitio distinto del lugar en donde se encuentren los HSM.

8.2.6 Transferencia de la llave privada desde el módulo criptográfico

Las llaves privadas de ECD GSE se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (Ver 8.2.3 Custodia de la llave privada).

El proceso de descarga de las llaves privadas se realiza según procedimiento del dispositivo criptográfico y se almacenan de forma segura protegidas por claves criptográficas.

8.2.7 Almacenamiento de las llaves privadas en un módulo criptográfico

Las llaves privadas de la ECD GSE son generadas y almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (Ver 8.2.3 Custodia de la llave privada).

Las llaves criptográficas pueden cargarse en un dispositivo criptográfico de igual prestación a partir de las copias de backup mediante un proceso que exige la participación de al menos dos operadores.

8.2.8 Método de activación de la llave privada

Las llaves privadas, de la ECD GSE Raíz y de las ECD Subordinadas, se encuentran bajo control multipersona. El método de activación de la llave privada es mediante la inicialización del software de la ECD GSE por medio de una combinación de claves en poder de varios operadores.

Se requiere un control multipersona para la activación de la llave privada de la ECD. Se necesitan al menos 2 personas para la activación de las llaves.

8.2.9 Método de desactivación de la llave privada

La desactivación de la llave privada se realiza mediante desactivación del software o el apagado del servidor ECD. Se activa nuevamente mediante el uso de control multipersona, siguiendo los procedimientos marcados por el fabricante del módulo criptográfico.

8.2.10 Método para destruir la llave privada

El método utilizado en caso de requerirse la destrucción de la llave privada es mediante el borrado de las llaves almacenadas en los dispositivos criptográficos tal y como se describe en el manual del fabricante del dispositivo y la destrucción física de las tarjetas de acceso en poder de los operadores en el caso en el que se requiera.

8.2.11 Características técnicas de los módulos criptográficos utilizados

Los dispositivos criptográficos utilizados por ECD GSE se ajustan a lo indicado en el Anexo F: Dispositivos Criptográficos, del CEA.

8.2.12 Evaluación del módulo criptográfico

El dispositivo criptográfico es monitoreado mediante el software propio del mismo para prever posibles fallas.

8.2.13 Evaluación del sistema de cifrado

ECD GSE acoge las recomendaciones para el uso de algoritmos criptográficos y longitudes de clave que sean publicados por el NIST (Instituto Nacional de Estándares y Tecnología por sus siglas en ingles) y por el ONAC, si se materializa alguna circunstancia en donde los algoritmos utilizados para firma y cifrado por ECD GSE sea vean comprometidos a todos los niveles, ECD GSE tomará inmediatamente las medidas y recomendaciones impartidas por esta entidad o por ONAC para mantener la seguridad de la firma durante el restante de su ciclo de vida.

8.3 Otros aspectos de la gestión del par de llaves

8.3.1 Archivo de la llave pública

ECD GSE mantendrá controles para el archivo de su propia llave pública.

8.3.2 Periodos operativos de los certificados y periodo de uso del par de llaves

El periodo de uso del par de llaves está determinado por la siguiente vigencia de cada certificado:

ALGORITMO RSA:

El periodo de validez del certificado digital de RSA y el par de llaves de la raíz es de treinta (30) años.

El periodo de validez del certificado digital de RSA y el par de llaves de la subordinada es de diez (10) años.

ALGORITMO ECDSA:

El periodo de validez del certificado digital de ECDSA y el par de llaves de la Raíz es de veinticinco (25) años.

El periodo de validez del certificado digital de ECDSA y el par de llaves de la subordinada es de diez (10) años.

8.4 Datos de activación

8.4.1 Generación e instalación de los datos de activación

Para el funcionamiento de la ECD GSE se crean contraseñas para los operadores del dispositivo criptográfico y que servirán junto con un PIN para la activación de las llaves privadas.

Los datos de activación de la llave privada se encuentran divididos en contraseñas custodiadas por un sistema multipersona donde 4 personas comparten el código de acceso de dichas tarjetas.

8.4.2 Protección de los datos de activación

El conocimiento de los datos de activación es personal e intransferible. Cada uno de los intervinientes es responsable por su custodia y debe manejarlo como información confidencial.

8.4.3 Otros aspectos de los datos de activación

La clave de activación es confidencial, personal e intransferible y por tanto se deben tener en cuenta las normas de seguridad para su custodia y uso.

8.5 Controles de seguridad informática

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Control de accesos a los dispositivos.
- Cierre de vulnerabilidades de los sistemas.
- Hardenización de los sistemas según buenas prácticas.
- Configuración de red a nivel de seguridad (DMZ, Red Interna, Red administrativa, entre otros)
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Plan de continuidad de servicios
- Configuración antivirus.
- Requerimientos de tráfico de red.

8.5.1 Requisitos técnicos de seguridad específicos

ECD GSE cuenta con una infraestructura tecnológica debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar una alta disponibilidad y confianza en los servicios ofrecidos a sus suscriptores, entidades y terceros de confianza.

La información relacionada con Seguridad de la Información es considerada como confidencial y por tanto solo puede ser suministrada a aquellos entes de control que requieran de su conocimiento.

8.5.2 Evaluación de la seguridad informática

El sistema de gestión de la seguridad de la Información del proveedor Paynet SAS evalúa los procesos relacionados con la infraestructura tecnológica con el fin de identificar posibles debilidades y definir los planes de mejoramiento continuo con el apoyo de las auditorias periódicas.

La seguridad de los equipos se soporta con un análisis de riesgos inicial de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.
Este análisis se realiza periódicamente de manera que se identifiquen posibles vulnerabilidades de los sistemas.

8.5.3 Acciones en caso de un evento o incidente de seguridad de la información

El sistema de gestión de la seguridad de la Información implementado por ECD GSE tiene establecido un procedimiento de gestión de incidentes tanto para la CA como para la RA

que especifica las acciones a ejecutar, componentes o recursos a utilizar y como debe reaccionar el personal en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación digital de ECD GSE.

a. **Detección y reporte del incidente:** Los incidentes de seguridad deberán ser reportados a través del correo seguridad.informacion@gse.com.co, el cual es administrado por el Oficial de Seguridad de la Información de la ECD GSE
   Los incidentes podrán ser detectados a través de sistemas de monitorización, sistemas de detección de intrusos, registros del sistema, aviso por parte del personal o por parte de suscriptores y/o responsables.
b. **Análisis y evaluación del incidente:** Una vez detectado el incidente se determina el procedimiento de respuesta y se contacta con las personas responsables para evaluar y documentar las acciones a tomar según la gravedad de la incidencia. Se efectúa una investigación para determinar cuál fue el alcance del incidente, es decir averiguar hasta donde llego el ataque y la máxima información posible de la incidencia.
c. **Control de daños ocasionados por incidente:** Reaccionar rápidamente para contener la incidencia y evitar que se propague tomando medidas como bloquear accesos al sistema.
d. **Investigación y recopilación de evidencias:** Revisar registros de auditoría para realizar un seguimiento de lo ocurrido.
e. **Recuperación y medidas contra incidencia:** Restaurar el sistema a su correcto funcionamiento y documentar el procedimiento y formas de evitar que vuelva a presentarse la incidencia.
f. **Análisis posterior de la incidencia para la mejorar del procedimiento:** Realizar un análisis de todo lo ocurrido, detectar la causa de la incidencia, corregir la causa para el futuro, analizar la respuesta y corregir errores en la respuesta.

8.6 Controles técnicos del ciclo de vida

8.6.1 Controles de desarrollo de sistemas

ECD GSE cumple con los procedimientos de control de cambios establecidos para los nuevos desarrollos y actualizaciones de software.

8.6.2 Controles de gestión de seguridad

ECD GSE mantiene un control sobre los inventarios de los activos utilizados en su proceso de certificación. Existe una clasificación de estos de conformidad con su nivel de riesgo.

ECD GSE monitorea de manera periódica su capacidad técnica con el fin de garantizar una infraestructura de alta disponibilidad.

8.6.3 Controles de seguridad del ciclo de vida

ECD GSE cuenta con los debidos controles de seguridad a lo largo de todo el ciclo de vida de los sistemas que tengan algún impacto en la seguridad de los certificados digitales emitidos.

8.7 Controles de seguridad de la red

ECD GSE cuenta con una infraestructura de red debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar una alta disponibilidad y confianza en los servicios ofrecidos a sus suscriptores, entidades y terceros de buena fe.

La información relacionada con Seguridad de la Información es considerada como confidencial y por tanto solo puede ser suministrada a aquellos entes de control que requieran de su conocimiento.

8.8 Estampado cronológico

ECD GSE cuenta con el servicio de estampado cronológico, que se describe en las correspondientes Políticas de Certificado para Servicio Estampado Cronológico, publicada en el portal http://www.gse.com.co.

9. AUDITORIA DE CONFORMIDAD Y OTROS CONTROLES

9.1 Frecuencia o circunstancias de los controles

El cumplimiento de los controles que garanticen la seguridad en la emisión de certificados digitales se evaluará por medio de una auditoría anual realizada por una firma de auditoría externa.

9.2 Identidad/cualificación del auditor

De conformidad con el Decreto 333 de 2014 y específicamente en el **Artículo 14. Auditorias.** Las entidades de certificación deberán cumplir con la auditoria de tercera parte en los términos previstos en los Criterios Específicos de Acreditación establecidos por ONAC.

Requisitos de aseguramiento: Empresa de auditoría legalmente constituida en Colombia en cuyo objeto social esté incluido: servicios de auditoría de sistemas, seguridad de la información e infraestructura de llave pública PKI. Las competencias del grupo auditor deberán demostrarse respecto a los criterios específicos de acreditación, los requisitos de la norma internacional ISO/IEC 27001 en cuanto a seguridad de la información, en relación con el servicio ISO 9001 o ISO/IEC 20000-1, en caso de que el auditor no tenga competencia en PKI, debe estar en compañía de un experto técnico conocedor de la gestión relacionada a infraestructura de llave pública PKI. El personal auditor debe tener tarjeta profesional vigente en Ingeniería.

9.3 Relación entre el auditor y la entidad auditada

La única relación establecida entre el auditor y la entidad auditada es la de auditor y auditado. La firma de auditoría ejerce su absoluta independencia en el cumplimiento de sus actividades de auditoría y no existe conflicto de intereses pues la relación es netamente de tipo contractual.

9.4 Aspectos cubiertos por los controles

Los aspectos cubiertos por el control de auditoría enmarcan el alcance acreditado por ONAC para la ECD, de conformidad con lo establecido en el numeral REQUISITOS DEL SISTEMA DE GESTIÓN – Auditoria de Tercera Parte del documento de CEA establecidos por ONAC el entregable es el informe de conformidad, no se permite con salvedad o razonabilidad.

9.5 Acciones que tomar como resultado de la detección de deficiencias

Las deficiencias detectadas durante el proceso de auditoría deben ser subsanadas a través de acciones correctivas o de mejora, procedimientos e implementación de los controles requeridos para atender los hallazgos.

9.6 Comunicación de resultados

Una vez terminada la auditoría, la firma auditora debe presentar el informe de auditoría a ECD GSE y, de requerirse, ECD GSE debe establecer unas acciones correctivas y de mejora. El informe final deber ser remitido a ONAC.

10. DESCRIPCION DE PRODUCTOS Y SERVICIOS

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.

TIPO DE CERTIFICADO	OBJETO
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	Certificado exclusivo para facturación electrónica atendiendo a la necesidad de las personas naturales que buscan la seguridad del certificado para la emisión de facturas electrónicas. 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 facturacion gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad.
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 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 facturacion gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad.
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 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.
Generación de Firmas Electrónicas Certificadas	Certificado exclusivo para la generación de firmas electrónicas certificadas.

TIPO DE CERTIFICADO	OBJETO
Servicio de Correo electrónico certificado	El servicio de correo electrónico certificado 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.
Servicio de estampado Cronológico (TSA)	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.
Servicio de Archivo y Conservación de Documentos Electrónicos Transferibles y Mensaje de Datos	Servicio consiste en un espacio de almacenamiento seguro y encriptado al cual accede con credenciales o con un certificado digital. La documentación que se almacene en esta plataforma tendrá valor probatorio siempre y cuando este firmada digitalmente.

Nota: Para la verificación del proceso de generación de cada servicio remitirse a los procedimientos correspondientes.

11. OTROS ASUNTOS LEGALES Y COMERCIALES

11.1 Tarifas

11.1.1 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

Detalle del producto	Tiempo de entrega	Vigencia	Precio sin IVA	IVA	Total
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 están calculados sobre vigencia de uno y dos años. 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 el caso de certificado de firma electrónica no tiene costo porque está incluido en los paquetes para la generación de firmas electrónicas certificadas.

11.1.2 Tarifas de acceso a los certificados

El acceso a la consulta del estado de los certificados emitidos es libre y gratuito y por tanto no aplica una tarifa.

11.1.3 Tarifas de revocación o acceso a la información de estado

La solicitud de revocación de un certificado no tiene costo. El acceso a la información de estado de los certificados emitidos es libre y gratuito y por tanto no aplica una tarifa.

11.1.4 Tarifas de otros servicios

Una vez se ofrezcan otros servicios por parte de GSE, se encuentran publicadas en las PC de los servicios en la página web de GSE.

11.1.5 Política de devoluciones

Se debe tener en cuenta la Política de Devoluciones publicada en la página web de GSE (https://gse.com.co/Nosotros/politicas)

11.2 Garantías

La ECD GSE dispondrá en todo momento de un seguro de responsabilidad civil de acuerdo con lo indicado en el decreto 333 de 2014 con un cubrimiento de 7500 salarios mínimos mensuales legales por evento.

La ECD GSE actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los certificados, de los suscriptores/responsables y de los terceros que confíen en los certificados.

Las responsabilidades de la ECD GSE incluyen las establecidas por la presente DPC, así como las que resulten de aplicación como consecuencia de la Normativa Colombiana e Internacional.

ECD GSE será responsable del daño causado ante el Suscriptor, Entidad o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de toda la información contenida en el certificado en la fecha de su emisión.
- La garantía de que, en el momento de la entrega del certificado, obra en poder del Suscriptor, la llave privada correspondiente a la llave pública dada o identificada en el certificado.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente.

11.3 Imparcialidad y No Discriminación

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/politicas.

11.4 Límites de responsabilidad

ECD GSE no será responsable en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales, terrorismo, huelgas o cualquier otro caso de Fuerza Mayor.
- Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente DPC y sus Anexos.
- Por el uso indebido o fraudulento de los certificados o CRL's emitidos por la Autoridad de Certificación.
- Por el uso de la información contenida en el Certificado o en la CRL.
- Por el incumplimiento de las obligaciones establecidas para el Suscriptor, Entidades, Responsables o Terceros que confían en la normativa vigente, la presente DPC y sus Anexos.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Por la no recuperación de documentos cifrados con la clave pública del Suscriptor o Entidad.
- Fraude en la documentación presentada por el solicitante.

11.5 Responsabilidades financieras y legales

11.5.1 Otros bienes

ECD GSE cuenta con la capacidad económica y financiera suficiente para prestar los servicios autorizados y responder por sus deberes como entidad de certificación. ECD

GSE como prestador de servicios de certificación responderá por los perjuicios que se causen a los suscriptores, entidades o terceros de buena fe derivados de errores y omisiones, de mala fe de los administradores, representantes legales o empleados de ECD GSE en el desarrollo de las actividades para las cuales cuenta con autorización y para ello cuenta con un seguro de responsabilidad civil de conformidad con el del Artículo 9°. Garantías, del Decreto 333 de 2014. ECD GSE no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante suscriptor y/o responsable de certificados o terceros de confianza a excepción de lo establecido por las disposiciones de la presente DPC.

11.5.2 Seguro o garantía de cobertura para suscriptores, responsables y terceros de buena fe

En cumplimiento del Artículo 9°. Garantías, del Decreto 333 de 2014, ECD GSE ha adquirido un seguro expedido por una entidad aseguradora autorizada para operar en Colombia, que cubre todos los perjuicios contractuales y extracontractuales de los suscriptores, responsables y terceros de buena fe exenta de culpa derivados de errores y omisiones, o de actos de mala fe de los administradores, representantes legales o empleados de ECD GSE en el desarrollo de las actividades para las cuales cuenta con autorización.

11.6 Confidencialidad de la información

11.6.1 Responsabilidad de proteger la información confidencial

ECD GSE se compromete a proteger todos los datos a los que tenga acceso como consecuencia de su actividad como ECD.

Toda información no pública es considerada confidencial y por tanto de acceso restringida, excepto en aquellos supuestos previstos legalmente como lo son tribunales u órganos administrativos competentes o impuesta por una ley, no se difunde información confidencial sin el consentimiento expreso por escrito del suscriptor o la entidad que le haya otorgado el carácter de confidencialidad.

No obstante, se reserva el derecho a revelar a los empleados y consultores, externos o internos, los datos confidenciales necesarios para realizar sus actividades como ECD obligando a todo el personal a suscribir un acuerdo de confidencialidad en el marco de las obligaciones contractuales contraídas con ECD GSE.

11.6.2 Información confidencial

La siguiente información es considerada confidencial:

a. Llave privada de la Autoridad de Certificación y/o ECD
b. Llave privada del suscriptor o entidad
c. Información suministrada por el suscriptor o entidad y que no sea necesaria para validar la confianza del suscriptor o entidad
d. Información acerca del solicitante, suscriptor y/o responsable obtenida en fuentes diferentes (por ejemplo, de un reclamante o de los reguladores)
e. Registros de las transacciones
f. Registros de auditoría
g. Políticas de seguridad
h. Plan de Continuidad de Negocio
i. Toda aquella información que sea calificada como "Confidencial" en los documentos entregados por ECD GSE

11.6.3 Información no confidencial

Toda información no confidencial es considerada pública y por tanto de libre acceso para terceros:

a. La contenida en la presente Declaración de Prácticas de Certificación y sus anexos.
b. La contenida en el repositorio sobre el estado de los certificados.
c. La lista de certificados revocados.
d. Toda aquella información que sea calificada como "PÚBLICA" en los documentos entregados por ECD GSE.

11.6.4 Deber de proteger la información confidencial

ECD GSE mantiene medidas de seguridad para proteger toda la información confidencial suministrada a ECD GSE directamente o a través de los canales establecidos para ello desde su recibo hasta su almacenamiento y custodia, donde reposarán por 10 años. ECD GSE cuenta con un Sistema Integrado de Gestión que incluye un Sistema de Seguridad de la Información. Esto nos permite asegurar que la información de nuestros suscriptores no será comprometida, ni divulgada a terceras personas salvo que medie solicitud formal de una autoridad competente que así la requiera.

11.7 Protección de la información personal

11.7.1 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.

11.7.2 Información tratada como privada

La información personal suministrada por el suscriptor o responsable y que es requerida para la aprobación del certificado digital es considerada información de carácter privado.

11.7.3 Información no calificada como privada

Son aquellos datos personales que las normas y la Constitución han determinado expresamente como públicos para cuya recolección y tratamiento no es necesaria la autorización del titular de la información.

11.7.4 Responsabilidad de la protección de los datos de carácter personal

ECD GSE es responsable y cuenta con los adecuados recursos tecnológicos, para ayudar a garantizar la adecuada custodia y conservación de los datos de carácter personal colectados por los canales usados por la compañía, dando cumplimiento a la Ley 527 de 1999 “Artículo 32. Deberes de las entidades de certificación. Las entidades de certificación tendrán, entre otros, los siguientes deberes: Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor, responsable y entidad”.

GSE ECD hace uso de mecanismos tecnológicos como el directorio activo donde se instrumentaliza la política de control de acceso y un repositorio centralizado donde se encuentra la información protegida por un firewall que previene intrusiones dentro de la red para los equipos de la oficina, y por certificados digitales para el acceso a los servidores de producción de la ECD

11.7.5 Notificación y consentimiento para usar datos de carácter personal

Los datos de carácter personal no podrán ser comunicados a terceros, sin la debida notificación y consentimiento de su dueño, de conformidad con la ley de protección de datos.

11.7.6 Revelación en el marco de un proceso administrativo o judicial

Los datos de carácter personal podrán ser comunicados cuando se requieran por parte de una de las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial sin la debida notificación y consentimiento de su dueño, de conformidad con la ley de protección de datos.

11.7.7 Otras circunstancias de revelación de información

ECD GSE tiene como política de privacidad lo estrictamente establecido en el derecho la ley de protección de datos: “La información privada, será aquella que por versar sobre

información personal o no, y que por encontrase en un ámbito privado, solo puede ser obtenida u ofrecida a los terceros autorizados por el Suscriptor o responsable o por la ley".

11.7.8 Sistema de seguridad para proteger la información

Respecto al sistema que alberga la información suministrada por el suscriptor o responsable del servicio de certificación se realizan las siguientes validaciones:

a. El proveedor de la infraestructura debe contar con las buenas prácticas de las siguientes Normas:

   i. ISO 27001
   ii. ISO 9001

b. Pruebas de penetración y escaneo de vulnerabilidades en la red, realizada por una empresa especializada en Ethical Hacking.

11.8 Derechos de propiedad intelectual

En Colombia la protección de los derechos de autor incluye todos los trabajos literarios, artísticos o científicos que puedan ser reproducidos o divulgados a través de cualquier medio. En consecuencia, ECD GSE se reserva todos los derechos relacionados con la propiedad intelectual y prohíbe sin su autorización expresa la reproducción, divulgación, comunicación pública y transformación de la información, técnicas, modelos, políticas internas, procesos, procedimientos o cualquiera de los elementos contenidos en la presente DPC, de acuerdo con la normatividad nacional e internacional relacionada con propiedad intelectual.

11.9 Obligaciones

11.9.1 Obligaciones de la ECD GSE

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

a) Respetar lo dispuesto en la normatividad vigente, en esta DPC y en las Políticas de Certificación PC.
b) Publicar esta DPC y cada una de las Políticas de Certificación en la página Web de GSE.
c) Informar a ONAC sobre las modificaciones de la DPC y de las Políticas de Certificación.
d) Mantener la DPC con su última versión publicada 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 Certificación y a los estándares definidos en la presente DPC.

g) Generar certificados consistentes con la información suministrada por el solicitante o suscriptor.
h) Conservar la información sobre los certificados digitales 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 digitales emitidos en un repositorio de acceso libre.
k) No mantener copia de la llave privada del solicitante o suscriptor.
l) Revocar los certificados digitales según lo dispuesto en la Política de revocación de certificados digitales.
m) Actualizar y publicar la lista de certificados digitales 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.

11.9.2 Obligaciones de la RA

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

a) Conocer y dar cumplimiento a lo dispuesto en la presente DPC y en las Políticas de Certificación 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 para la emisión del certificado digital, 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.

11.9.3 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 presente DPC como es:

a) Usar su certificado digital o certificado de firma electrónica según los términos de esta 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/o firmado en el documento términos y condiciones.
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 las PC establecidos en la presente DPC para cada uno de los tipos de certificado.
m) Solicitar como suscriptor y/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 presente 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 el estado de un certificado digital revocado para lo cual se 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 que pueda considerar engañosa o no autorizada, conforme a lo dispuesto por esta 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 esta DPC, indicando la versión.
u) 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.

11.9.4 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.
c) Verificar el estado de los certificados digitales 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.

11.9.5 Obligaciones de la Entidad (Cliente)

Conforme lo establecido en las PC relacionadas en este documento, en el caso de los certificados donde se acredite la vinculación del suscriptor y/o responsable con la misma, será obligación de la Entidad:

a) Solicitar a la RA de la ECD GSE la suspensión/revocación del certificado digital 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 relacionadas en esta 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.

11.9.6 Obligaciones de otros participantes de la ECD

El Comité de Gerencia y el 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 los cambios a realizar sobre los servicios de certificación, por decisiones de tipo normativo o por solicitudes de suscriptores o responsables.
c) Aprobar la notificación de cualquier cambio a los suscriptores y/o 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 se realice.
e) Informar los planes de acción a ONAC sobre todo cambio que tenga impacto en la infraestructura PKI y que afecte los servicios de certificación digital, de acuerdo con el RAC-3.0-01.
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 digital 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 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 por que las condiciones de acreditación otorgadas 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.
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, en los numerales que correspondan.
s) El Sistema Integrado de Gestión ejecutará planes de acción correctivos y acciones de mejora para responder ante cualquier riesgo que comprometa la imparcialidad de la ECD, ya sea que se derive de las acciones de cualquier persona, organismo, organización, actividades, sus relaciones o las relaciones de su personal o de sí misma, para lo cual utiliza la norma ISO 31000 para la identificación de riesgos que comprometa la imparcialidad y no discriminación de la ECD, entregando a el Comité de Gerencia el mecanismo que elimina o minimiza tal riesgo, de manera continua.

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 que 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 esta 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.

12. Términos y condiciones de la DPC y PC

12.1 Inicio de vigencia de la DPC y PC

La DPC y PC entran en vigor desde el momento en que se publican en la página web de ECD GSE, a partir de ese momento la versión anterior del documento queda derogada y la nueva versión reemplaza íntegramente la versión anterior.

ECD GSE conserva en el repositorio las anteriores versiones de la DPC y PC.

i. Efectos de terminación e inicio de vigencia de la DPC y PC

Para los certificados digitales que hayan sido emitidos bajo una versión antigua de la DPC o PC aplica la nueva versión de la DPC o PC en todo lo que no se oponga a las declaraciones de la versión anterior.

ii. Cambios que afectan la DPC y PC

Todo cambio que afecte la DPC y PC de la ECD GSE seguirá el siguiente procedimiento:

a. El comité de Gerencia aprobará los cambios que considere pertinentes sobre la DPC y las PC.
b. La DPC y PC actualizada es publicada en la página web de la ECD GSE una vez sea autorizada por el comité de Gerencia.

iii. Circunstancias bajo las cuales la OID debe cambiarse

En los siguientes casos la ECD GSE realizará ajustes a la identificación de OID:

a. La autorización de una nueva jerarquía de certificación, evento en el cual los OID deberán ser definidos de acuerdo con la estructura.
b. En caso de que los cambios de la DPC y PC que afecten la aceptabilidad de los servicios de certificación digital se proceden a realizar el ajuste de OID.
Este tipo de modificaciones se comunicará a los usuarios de los certificados correspondientes a la PC o DPC.

13. Políticas de Certificación

La interrelación entre esta DPC y la Políticas de certificación de los distintos certificados es fundamental. Y ello, en la medida en que:

- **La DPC** es el conjunto de prácticas adoptadas por ECD GSE para la prestación de los servicios acreditados por ONAC y contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los certificados, además sobre la relación de confianza entre Solicitante, Suscriptor, Responsable, Entidad, Tercero de buena fe y la ECD.

- **Políticas de certificación** constituye el conjunto de reglas que definen las características de los distintos certificados ECD GSE y la aplicabilidad de estos certificados para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

En definitiva, la política define "**qué**" requerimientos son necesarios para la emisión de los distintos certificados ECD GSE mientras que la DPC nos dice "**cómo**" se cumplen los requerimientos de seguridad impuestos por la política.

Por este motivo, se relacionan las siguientes Políticas de Certificados:

- Políticas de Certificado para Certificados Digitales

OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.4.12
Ubicación de la DPC	https://gse.com.co/documentos/calidad/politicas/Politicas_de_Certificado_para_Certificados_Digitales_V12.pdf

- Políticas de Certificado para Servicio de Estampado Cronológico

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.2.11
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_Certificado_para_Servicio_de_Estampado_Cronologico_V11.pdf

- Políticas de Certificado para Servicio de Archivo y Conservación de Documentos Electrónicos Transferibles y Mensajes de Datos.

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.3.11
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_Certificado_para_Servicio_de_Archivo_Confiable_de_Datos_V11.pdf

- Políticas de Certificado para Servicio de Correo Electrónico Certificado

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.5.11
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politica_Certificado_para_Servicio_de_Correo_Electronico_Certificado_V11.pdf

- Políticas de Generación de Firmas Electrónicas Certificadas

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.6.3
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_Generacion_de_Firmas_Electronicas_Certificadas_V3.pdf

14. ANEXO 1 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS DIGITALES

15. ANEXO 2 DPC MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TERMINOS Y CONDICIONES

16. ANEXO 3 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS FIRMA ELECTRÓNICA