

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN V21

Código	Nombre	Versión	Clasificación de la información
POP-DT-58	Declaración de Prácticas de Certificación	21	Pública

Título del Documento	**Declaración de Prácticas de Certificación**
Versión	21
Grupo de Trabajo	Comité de Gerencia
Estado del documento	Final
Fecha de emisión	01/11/2016
Fecha de inicio de vigencia	28/10/2026
OID (Object Identifier) - IANA	1.3.6.1.4.1.31136.1.1.21
Ubicación de la DPC	https://gse.com.co/documentos/calidad/DPC/Declaracion_de_Practicas_de_Certificacion_V21.pdf
Elaboró	Project & Operations Manager
Revisó	Sistema Integrado de Gestión
Aprobó	Comité de Gerencia

Control de Cambios

Versión	Fecha	Cambio/Modificación
1	01-11-2016	Documento inicial
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 cambió 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 eliminó 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 cómo 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 Representante 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 incluyó el enlace para consultar en línea el Certificado de Existencia y Representación Legal para la ECD y la CA actual (Paynet SAS). 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 eliminó 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 actualizó 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 10. DESCRIPCIÓN 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 Prácticas 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 incluyó 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 actualizó el numeral 8.3.2 dando claridad del periodo de validez de las llaves raíz y subordinadas del algoritmo RSA y ECDSA • Se actualizan OID y links de consulta
12	27/10/2021	• Se modificó el numeral 6.5 de Validación de Identidad • Se actualizaron 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 eliminó el 4.1-10 dejando únicamente CEA. • 3.2. Petición, queja, reclamo y solicitudes: Se eliminó el término 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 incluyó un párrafo final sobre el consumo de confronta en los servicios. • 6.13.1 Descripción de contenido de los certificados: Se incluyó 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 modificó 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 modificó exoneración por límites de responsabilidad. • 11.9.6 Obligación de otros participantes: Se modificó el ítem r) eliminando el 4.1-10 dejando únicamente CEA. • 15. Se modificó el nombre del anexo sobre términos y condiciones. • 16. Se incluyó este ítem del anexo técnico de certificado de firma electrónica. • Se actualizaron 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 incluyó el código de calidad en el encabezado del documento.
14	23/09/2022	• 3.1 Resumen: Se incluyeron los capítulos del DURSCIT. • Se modificó la dirección de la ECD en los ítems 3.1, 3,2, 3.6.2 y 3.7.1. • Se modificó la dirección de Paynet SAS en los ítems 3.6.1 y 3.6.7.2. • Se modificó el numeral 3.6.4 cambiando responsable por tercero de buena fe • Se incluyó el numeral 3.6.4.1 Precauciones que deben observar los terceros • Se modificó el numeral 6.4.1 Realización de las funciones de identificación y autenticación • Se modificó el numeral 6.5.1 Método para demostrar la posesión de la llave privada dando claridad en caso de que los solicitantes generan el par de llaves en su propia infraestructura. • Se modificó el numeral 6.5.5 Criterios para la interoperabilidad • Se modificó el numeral 6.12.7 Frecuencia de actualización de las CRLs de acuerdo con el porcentaje de disponibilidad establecido en el nuevo CEA. • Se modificó el RFC 2560 por RFC 6960 en los numerales 6.12.10 Requisitos de comprobación de la revocación on-line, 6.14.1.4 Perfil OCSP y 6.14.1.5 Número de versión. • Se modificó el numeral 7.7. Sistema de almacenamiento haciendo claridad que los servidores están en ambientes cloud. • Se modificó el numeral 7.4. Exposición al agua aclarando que hace referencia a los datacenter de la PKI. • Se modificó el numeral 7.16. Cese de una ECD incluyendo un párrafo sobre el plan de seguridad de la cesación de actividades. • Se modificó el numeral 11.4 Límites de responsabilidad incluyendo la Responsabilidad por la veracidad de la información del Suscriptor, Responsabilidad por disponibilidad del servicio, Responsabilidad por la funcionalidad del servicio en la infraestructura del Suscriptor, Responsabilidad frente delitos informáticos. • Se modificó el numeral 11.9.1 Obligaciones de la ECD GSE incluyendo los ítems o) al y). • Se incluyeron los numerales 12.3 Notificación y comunicación, 12.5 Prevención y Resolución de disputas, 12.6 Ley aplicable y 12.7 Cumplimiento con la ley aplicable. • Se actualizaron 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.
15	10/05/2023	• Se modificó todo el orden del documento de acuerdo con los numerales del RFC 3647. • Se eliminó a Paynet SAS como la autoridad CA ya que se trasladó la PKI a la ECD de GSE. • Se modificó al Director de Operaciones por el Gerente de Operaciones • Se modificaron los datos de los datacenter principal y alterno quedando Hostdime y Claro.
16	24/10/2023	• Se modifica el numeral 1.1.6.2 Siglas: Se incluye la sigla RNEC • Se modifica el numeral 1.3.1.3 Se incluyen pseudónima y pseudoanónima, se amplían los sobrenombres. • Se modifica el numeral 1.3.2: Se actualiza la información de numeral. • Se modifica el numeral 1.3.2.3: Se incluye información de requisitos para la identificación y autenticación de la identidad de un Individuo • Se modifica el numeral 1.3.2.4 Se actualiza la información del numeral. • Se modifica el numeral 1.3.2.5 Se elimina la palabra recomendación • Se modifica el numeral 1.3.3.1 Se ajustan los requisitos de identificación y autenticación para generación de llaves de rutina. • Se modifica el numeral 1.4.1 Se incluye el ECD e información de bases de datos de plena confianza. • Se modifica el numeral 1.4.2.1 Se incluye la palabra información • Se modifica el numeral 1.4.3.2 Se incluye las palabras definido y autorizado • Se modifica el numeral 1.4.4.1 Se incluye la palabra informarlo y/o • Se modifica el numeral 1.4.7.2: Se incluye el término debidamente facultados y/o apoderados • Se modifica el numeral 1.4.7.3 Se actualiza los medios o mecanismos para recolectar información de la ECD • Se modifica el numeral 1.4.7.4 Se actualiza los medios para notificar al suscriptor • Se modifica el numeral 1.4.9.3 Se actualiza la información de solicitud de revocación en línea. • Se modifica el numeral 1.4.9.11 Se actualiza los medios para notificar al suscriptor • Se modifica el numeral 1.4.12.3 Se incluye la mesa de servicios para los casos de olvido de PIN • Se modifica el numeral 1.5.2.2 Se ajusta la información de las personas requeridas por rol. • Se modifica el numeral 1.5.7.2 Se incluye GSE • Se modifica el numeral 1.5.7.3 Se incluye GSE • Se modifica el numeral 1.7.1 Se actualiza la información de numeral. • Se modifica el numeral 1.9.3.4 Se actualiza información relacionando la TRD. • Se modifica el numeral 1.9.4.1 Se incluyen normas relacionadas al tratamiento de datos personales. • Se modifica el numeral 1.9.4.5 Se ajusta redacción del numeral • Se modifica el numeral 1.9.4.6 Se ajusta redacción del numeral • Se modifica el numeral 1.9.11.2 Se ajusta literal c • Se modifica el numeral 1.14 Se actualiza OID y ubicación de la Política de Certificado para Certificados Digitales
17	08/07/2024	• Se modifica el numeral 1.1 se actualiza indicativo de teléfono • Se modifica el numeral 1.1 elimina el fax • Se actualizan OID de todo el documento

		• Se actualiza la numeración y orden de acuerdo con el numeral 6 Esquema de un conjunto de disposiciones del RFC 3647 • Se actualiza el nombre del proceso TI por tecnología • Se modifica el numeral 3.2 Validación inicial de identidad (Se incluye método de verificación de información) • Se modifica el numeral 3.2 Se ajusta información de los mecanismos de verificación • Se modifica el numeral 4.1 Solicitud de certificado: se actualiza código de procedimiento • Se modifica el numeral 4.10.2 Se incluye información de disponibilidad del servicio y ajusta numeración relacionada • Se modifica el numeral 4.12 Se elimina texto de "almacenamiento de la llave privada a un responsable" ya que estaba repetido
18	01/10/2024	• Se ajusta el apartado 1.3 Participantes PKI, 1.3.1 Autoridad de Certificación (CA), suprimiendo "GSE Firma Electrónica Raíz". • Se modifica el numeral 3.1.1 Tipos de nombres, se elimina firma electrónica.
19	22/10/2025	1.**5.2 Contacto (Responsable de la ECD):**Se ajusta **Representante Legal** por **Presidente**. • 1.**5.3 Persona que determina la idoneidad de la DPC para la póliza:** Se ajusta **Gerente de Operaciones** por **Coordinador de Operaciones**. • 3.**2.4 Información de suscriptor no verificada:** Se ajusta redacción del apartado . •4.**1 Solicitud de certificado:** Se actualiza nombre del procedimiento • 4.**3.2 Mecanismos de notificación autorizados por los suscriptores:** Se ajusta la redacción del apartado . •4.12.**1 Política y prácticas en materia de custodia y recuperación de llaves / 6.1.1 Generación del par de llaves / 6.2.1 Estándares y controles para uso de módulos criptográficos / 6.2.4 Copia de respaldo de la llave privada / 6.2.5 Archivo de la llave privada:** Se incluye el cumplimiento de **FIPS 140-2 Nivel 3 o superior**. •5. **8 Cese de la CA o la RA:** Se actualiza información normativa
20	09/12/2025	**1.3.1 Autoridad de Certificación (CA).:** Se actualiza la información asociada a los Datacenter **5.8 Cese de la CA o la RA**. De acuerdo con lo definido en la Circular Externa No. 30-2021 se suprime la notificación a la Superintendencia de Industria y Comercio
21	28/10/2026	**1.1 Identificación de la compañía y del documento Apartado 1.1:** se suprime "S.A." del nombre de la compañía, quedando únicamente "Gestión de Seguridad Electrónica". **Apartado 1.2 – Nombre e identificación del documento:** se ajusta el último dígito del OID, correspondiente a la versión 21 del documento. **Apartado 1.3 – Participantes de la PKI:** se ajusta la imagen suprimiendo "S.A.". **1.2 Participantes, contactos y responsables** **Apartado 1.3.5 – Otros participantes:** se incluye el "Representante Legal Suplente". **Canal de atención:** se incluye "Felicitaciones" en el ítem de peticiones, quejas, reclamos y solicitudes (PQRS). **Apartado 1.5.2 – Contacto (Responsable de la ECD):** se reemplaza a Borja Carreras por María Ximena Flórez. **Apartado 1.5.3 – Persona que determina la idoneidad de la DPC para la póliza:** se reemplaza "Coordinador de Operaciones" por "Project & Operations Manager".

		1.3 Publicación y repositorio Apartado 2 – Responsabilidades de publicación y repositorio: se ajusta la clasificación de la información incluyendo "de uso interno". **1.4 Validación de identidad Apartado 3.2 – Validación inicial de identidad:** se realizan dos ajustes: El Registro Único Tributario (RUT) en formato actualizado de la DIAN pasa a solicitarse como "(Si aplica – Opcional)". Para los certificados de firma electrónica se incluye una verificación adicional de los datos registrados en la solicitud, mediante el envío de un código OTP al correo electrónico registrado. **1.5 Seguridad del personal Apartado 5.3.6 – Sanciones por actuaciones no autorizadas:** se incluye que, dentro del Reglamento Interno de Trabajo, dichas actuaciones se califican como falta grave. **1.6 Auditoría de cumplimiento Apartado 8 – Auditoría de cumplimiento y otras evaluaciones:** se ajusta el ítem completo, estableciendo que el cumplimiento de los controles que garantizan la seguridad en la emisión de certificados digitales se evaluará mediante una auditoría anual, ejecutada por una firma de auditoría externa y que cubre el período de enero a diciembre del año en curso. **1.7 Obligaciones del cliente y tarifas** **Apartado 9.11.5 – Obligaciones de la Entidad (Cliente):** se suprime el ítem 4. **Apartado de Tarifas:** se ajusta el cuadro de tarifas y se incluye el ítem 4, que precisa que las tarifas publicadas son precios base o de referencia y podrán ajustarse según las condiciones y acuerdos comerciales establecidos con cada cliente.

Tabla de Contenido

Tabla de Contenido

1. INTRODUCCIÓN.

1.1 Descripción General

1.2 Nombre e identificación del documento.

1.3 Participantes PKI.

- 1.3.1 Autoridad de Certificación (CA).
- 1.3.2 Autoridad de Registro (RA).
- 1.3.3 Suscriptores
- 1.3.4 Partes de confianza.
- 1.3.5 Otros participantes.

1.4 Uso del certificado.

- 1.4.1 Uso apropiado de los certificados
- 1.4.2 Uso prohibido de los certificados

1.5 Administración de políticas.

- **1.5.1 Organización que administra el documento.**
- **1.5.2 Contacto (Responsable de la ECD):**
- **1.5.3 Persona que determina la idoneidad de la DPC para la póliza.**
- **1.5.4 Procedimientos de aprobación de la DPC.**

1.6 Definiciones y acrónimos.

- Definiciones.
- Acrónimos.
- Estándares y Organismos de estandarización.

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.

2.1 Repositorios.
2.2 Publicación de información sobre certificación.
2.3 Plazo o frecuencia de la publicación.
2.4 Controles de acceso a los repositorios.
3. IDENTIFICACIÓN Y AUTENTICACIÓN.
3.1 Nombres.
3.1.1 Tipos de nombres.
Certificados raíz de la ECD GSE.
Curva Elíptica (ECDSA).
Certificados de las Subordinadas.
Curva Elíptica (ECDSA).
Certificados de suscriptor de ECD GSE (Matriz Perfil técnico de certificados).
Certificados de suscriptor de ECD GSE (Matriz Perfil técnico de certificados firma electrónica).
3.1.2 Necesidad de que los nombres tengan sentido.
3.1.3 Anonimato o seudonimato de los suscriptores.
3.1.4 Reglas de interpretación de las distintas formas del nombre.
3.1.5 Singularidad de los Nombres.
3.1.6 Reconocimiento, autenticación y rol de las marcas registradas.
3.2 Validación inicial de identidad.
3.2.1 Método para demostrar la posesión de la clave privada.
3.2.2 Autenticación de la identidad de la organización.
3.2.3 Autenticación de la identidad individual.
3.2.4 Información de suscriptor no verificada.
3.2.5 Validación de la autoridad.
3.2.6 Criterios de interoperabilidad.
3.3 Identificación y Autenticación para renovación de llaves.
3.3.1 Identificación y autenticación para la rutina de reúso llaves.
3.3.2 Identificación y autenticación para la rutina de reúso llaves tras la revocación.
3.4 Identificación y autenticación para la solicitud de revocación.
4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO.
4.1 Solicitud de certificado.
4.1.1 Quién puede solicitar un certificado.
4.1.2 Proceso de solicitud, registro y responsabilidad.
4.2 Procesamiento de solicitud de certificado.
4.2.1 Procedimiento para el procesamiento de la solicitud/ identificación y autentificación.
4.2.2 Criterios de aceptación o rechazo de la solicitud.
4.2.3 Plazo para procesar las solicitudes de certificado
4.3 Emisión del Certificado.
4.3.1 Acciones de la ECD GSE durante la emisión de certificados.
4.3.2 Mecanismos de notificación autorizados por los suscriptores.
4.4 Aceptación del Certificado.
4.4.1 Mecanismo de aceptación del certificado por parte del suscriptor.
4.4.2 Publicación del certificado por la CA
4.4.3 Notificación de la emisión de certificados por parte de la ECD GSE a otras entidades.
4.5 Uso de pares de llaves y certificados.

4.5.1 Responsabilidades del Suscriptor frente al uso de la llave privada y el certificado.
4.5.2 Responsabilidades del tercero de confianza relacionadas con el uso de la clave privada y el certificado del suscriptor.
4.6 Renovación del certificado
4.6.1 Circunstancias para la renovación de certificado.
4.6.2 Quién puede solicitar una renovación sin cambio de llaves.
4.6.3 Trámites para la solicitud de renovación de certificados.
4.6.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado sin cambio de llaves.
4.6.5 Forma en la que se acepta la renovación de un certificado.
4.6.6 Publicación del certificado renovado por la ECD.
4.6.7 Notificación de la emisión de un certificado renovado por la ECD a otras entidades.
4.7 Reúso de llave del certificado
4.7.1 Circunstancia para el reúso de llaves del certificado.
4.7.2 Quién puede solicitar la certificación de una nueva llave pública.
4.7.3 Procesamiento de las solicitudes de reúso de llave de certificados.
4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado.
4.7.5 Conducta que constituye la aceptación de un certificado con reúso de llave.
4.7.6 Publicación del certificado con reúso de llave por parte de la CA
4.7.7 Notificación de la emisión de certificados por parte de la CA a otras entidades
4.8 Modificación de Certificado.
4.8.1 Circunstancia para la modificación del certificado.
4.8.2 Quién puede solicitar la modificación del certificado.
4.8.3 Tramitación de solicitudes de modificación de certificados.
4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado
4.8.5 Conducta que constituye la aceptación de un certificado modificado.
4.8.6 Publicación del certificado modificado por la CA.
4.8.7 Notificación de la emisión de certificados por parte de la CA a otras entidades.
4.9 Revocación y Suspensión del Certificado.
4.9.1 Circunstancias para revocación.
4.9.2 Quién puede solicitar la revocación de un certificado
4.9.3 Procedimiento para solicitud de revocación de un certificado.
4.9.4 Periodo de gracia para solicitar revocación de un certificado.
4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación.
4.9.6 Requisito de comprobación de revocación para las partes confiantes.
4.9.7 Frecuencia de emisión de las CRLs.
4.9.8 Latencia máxima de las CRLs.
4.9.9 Disponibilidad de verificación en línea de revocación/estado
4.9.10 Requisitos de comprobación de revocación en línea.
4.9.11 Otras formas de anuncios de revocación disponibles.
4.9.12 Requisitos especiales de renovación de llaves comprometidas.
4.9.13 Circunstancias para la suspensión
4.9.14 Quién puede solicitar la suspensión
4.9.15 Procedimiento de solicitud de suspensión
4.9.16 Límites del periodo de suspensión
4.10 Servicios de Estado del Certificado.
4.10.1 Características operacionales

4.10.2 Disponibilidad servicio
4.10.3 Características opcionales.
4.11 Fin de la Suscripción.
4.12 Custodia y Recuperación de Llaves
4.12.1 Política y prácticas en materia de custodia y recuperación de llaves.
4.12.2 Política y prácticas de encapsulación y recuperación de llaves de sesión.
5. INSTALACIONES, GESTIÓN Y CONTROLES OPERATIVOS.
5.1 Controles de Seguridad Física.
5.1.1 Ubicación física de la construcción de la ECD.
5.1.2 Mecanismos de control de acceso físico.
5.1.3 Energía y aire acondicionado.
5.1.4 Exposición al agua.
5.1.5 Prevención y protección contra incendios.
5.1.6 Sistema de copia de respaldo - Almacenamiento de medios.
5.1.7 Eliminación de residuos
5.1.8 Copia de seguridad fuera de sitio.
5.2 Controles de Procedimiento.
5.2.1 Roles de confianza de la ECD.
5.2.2 Cantidad de personas requeridas en cada rol.
5.2.3 Identificación y autenticación de cada rol.
5.2.4 Roles que requieren segregación de funciones.
5.3 Controles de personal.
5.3.1 Requisitos sobre la cualificación, experiencia y requisitos de habilitación.
5.3.2 Procedimiento de verificación de antecedentes.
5.3.3 Requisitos de formación.
5.3.4 Requisitos y frecuencia de actualización de formación.
5.3.5 Frecuencia y secuencia de rotación de tareas.
5.3.6 Sanciones por actuaciones no autorizadas.
5.3.7 Controles para contratación de terceros.
5.3.8 Documentación proporcionada al personal.
5.4 Procedimientos de Registro de Auditoría.
5.4.1 Tipo de eventos registrados.
5.4.2 Frecuencia de procesamiento de Logs.
5.4.3 Periodo de retención de los registros de auditoría.
5.4.4 Protección de los registros de auditoría.
5.4.5 Procedimiento de copia de seguridad de los registros de auditoría.
5.4.6 Sistema de recolección de registro de auditoría (interna o externa)
5.4.7 Notificación a responsable de incidente de seguridad.
5.4.8 Análisis de vulnerabilidades.
5.5 Archivo de Registros.
5.5.1 Tipos de registros objeto de archivo.
5.5.2 Periodo de retención para archivo
5.5.3 Protección de archivo
5.5.4 Procedimientos de copia de respaldo de archivos
5.5.5 Requisitos para el sellado de tiempo de los registros.

5.5.6 Sistema de recolección de archivos (interna o externa).
5.5.7 Procedimientos para obtener y verificar información de archivo.
5.6 Cambio de Llaves.
5.7 Compromiso y Recuperación de Desastres.
5.7.1 Procedimientos de gestión de incidentes, eventos y compromisos
5.7.2 Procedimiento en caso de daño de los recursos informáticos, el software y/o los datos.
5.7.3 Procedimiento de recuperación frente al compromiso de la llave privada de la ECD.
5.7.4 Capacidad de recuperación en caso de desastre.
5.8 Cese de la CA o la RA.
6. CONTROLES TÉCNICOS DE SEGURIDAD.
6.1 Generación e Instalación de Pares de Llaves.
6.1.1 Generación del par de llaves
6.1.2 Entrega de la llave privada a los suscriptores.
6.1.3 Entrega de la llave pública al emisor del certificado.
6.1.4 Entrega de la llave pública de la CA a las partes confiantes.
6.1.5 Tamaño de las Llaves.
6.1.6 Parámetros de generación de la llave pública y control de calidad.
6.1.7 Fines de uso de la llave (según el campo de uso de la llave X.509 v3).
6.2 Protección de llave privada y controles de ingeniería de módulos criptográficos.
6.2.1 Estándares y controles para uso de módulos criptográficos.
6.2.2 Control multipersona (n de m) de la llave privada.
6.2.3 Custodia de la llave privada de la ECD.
6.2.4 Copia de respaldo de la llave privada.
6.2.5 Archivo de la llave privada.
6.2.6 Transferencia de llaves privadas hacia o desde un módulo criptográfico.
6.2.7 Almacenamiento de la llave privada en el módulo criptográfico.
6.2.8 Método de activación de la llave privada.
6.2.9 Método de desactivación de la llave privada.
6.2.10 Método para destruir la llave privada.
6.2.11 Clasificación del módulo criptográfico.
6.3 Otros Aspectos de la Gestión del Par de Llaves.
6.3.1 Archivo de la llave pública.
6.3.2 Periodos operativos de los certificados y periodo de uso del par de llaves.
6.4 Datos de Activación.
6.4.1 Generación e instalación de los datos de activación.
6.4.2 Protección de los datos de activación.
6.4.3 Otros aspectos de los datos de activación.
6.5 Controles de Seguridad Informática.
6.5.1 Requisitos técnicos específicos de seguridad informática.
6.5.2 Clasificación de la seguridad informática.
6.6 Controles de Técnicos del Ciclo de Vida.
6.6.1 Controles de desarrollo de sistemas.
6.6.2 Controles de gestión de seguridad.
6.6.3 Controles de seguridad del ciclo de vida.
6.7 Controles de Seguridad de Red.

6.8 Estampado Cronológico.
7. PERFILES DE CERTIFICADO, CRL Y OCSP.
7.1 Perfil del Certificado.
7.1.1 Números de versión.
7.1.2 Extensiones del certificado.
7.1.3 Identificadores de objetos algorítmicos.
7.1.4 Formas de nombres.
7.1.5 Restricciones de los nombres.
7.1.6 Identificador del objeto de la Política de Certificación.
7.1.7 Uso de la extensión Policy Constrains.
7.1.8 Sintaxis y semántica de los Policy Qualifiers
7.1.9 Tratamiento semántico para la extensión Certificate Policies.
7.2 Perfil de CRL.
7.2.1 Número(s) de versión
7.2.2 CRL y extensiones de entrada CRL
7.3 Perfil OCSP.
7.3.1 Número(s) de versión
7.3.2 Extensiones OCSP
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.
8.1 Frecuencia o Circunstancias de la Evaluación.
8.2 Identidad y cualificaciones del evaluador.
8.3 Relación del evaluador con la entidad evaluada.
8.4 Temas objeto de evaluación.
8.5 Acciones tomadas como resultado de la deficiencia.
8.6 Comunicación de Resultados.
9. OTROS ASUNTOS COMERCIALES Y LEGALES.
9.1 Honorarios.
9.1.1 Tasas de emisión o renovación de certificados
9.1.2 Tasas de acceso a certificados
9.1.4 Tasas por otros servicios
9.1.5 Política de reembolso
9.2 Responsabilidad Financiera.
9.2.1 Seguro o garantía de cobertura para suscriptores, responsables y terceros de buena fe.
9.2.2 Otros bienes.
9.2.3 Cobertura de seguro o garantía para entidades finales
9.3 Confidencialidad de la Información Comercial.
9.3.1 Alcance de la información confidencial.
9.3.2 Información no confidencial.
9.3.3 Deber de proteger la información confidencial.
9.4 Privacidad de la Información Personal.
9.4.1 Plan de Privacidad - Política de Tratamiento de Datos Personales.
9.4.2 Información tratada como privada.
9.4.3 Información que no se considera privada.
9.4.4 Responsabilidad de proteger la información privada.
9.4.5 Aviso y consentimiento para utilizar información privada.

9.4.6 Divulgación en virtud de un procedimiento judicial o administrativo.
9.4.7 Otras circunstancias de divulgación de información.
9.5 Derechos de Propiedad Intelectual.
9.6 Representaciones y Garantías.
9.6.1 Declaraciones y garantías de la CA
9.6.2 Declaraciones y garantías de la RA
9.6.3 Declaraciones y garantías del suscriptor
9.6.4 Declaraciones y garantías de la parte confiante
9.6.5 Declaraciones y garantías de otros participantes
9.7 Renuncias de Garantías.
9.8 Limitaciones de Responsabilidad.
9.9 Indemnizaciones.
9.10 Duración y Terminación.
9.10.1 Duración.
9.10.2 Terminación.
9.10.3 Efecto de terminación, notificación y comunicación.
9.10.4 Procedimiento de Cambio en la DPC y PC.
9.11 Notificaciones y comunicaciones individuales a los participantes.
9.11.1 Obligaciones de la ECD GSE.
9.11.2 Obligaciones de la RA.
9.11.3 Obligaciones (Deberes y Derechos) del Suscriptor y/o Responsable.
9.11.4 Obligaciones de los Terceros de buena fe.
9.11.5 Obligaciones de la Entidad (Cliente).
9.11.6 Obligaciones de otros participantes de la ECD.
9.12 Enmiendas.
9.12.1 Procedimiento para enmienda.
9.12.2 Mecanismo y plazo de notificación.
9.12.3 Circunstancias en las que debe modificarse un OID.
9.12.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado.
9.12.5 Forma en la que se acepta la modificación de un certificado.
9.12.6 Publicación del certificado modificado por la ECD.
9.12.7 Notificación de la emisión de un certificado por la ECD a otras entidades.
9.13 Disposiciones sobre resolución de disputas.
9.14 Legislación aplicable.
9.15 Cumplimiento de la legislación aplicable.
9.16 Disposiciones varias.
9.16.1 Acuerdo completo
9.16.2 Cesión
9.16.3 Divisibilidad
9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)
9.16.5 Fuerza mayor
9.17 Otras Disposiciones.
DESCRIPCIÓN DE PRODUCTOS Y SERVICIOS
TARIFAS.
Tarifas de emisión o renovación de certificados.

Tarifas de acceso a los certificados.
Tarifas de revocación o acceso a la información de estado.
Tarifas de otros servicios.
Política de devoluciones.
IMPARCIALIDAD Y NO DISCRIMINACIÓN
POLÍTICAS DE CERTIFICACIÓN.
ANEXO 1 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS DIGITALES.
ANEXO 2 DPC MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES.
ANEXO 3 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS FIRMA ELECTRÓNICA.

1. INTRODUCCIÓN.

1.1 Descripción General

La Declaración de Prácticas de Certificación (DPC)- Global Certification Authority Root GSE (en adelante DPC) es un documento elaborado por **Gestión de Seguridad Electrónica (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 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.

La DPC está conforme con los siguientes lineamientos:

1. 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;
2. 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.
3. ETSI EN 319 411-1 V1.2.0 (2017-08).
4. 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

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.

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

DATOS DE GESTIÓN DE SEGURIDAD ELECTRÓNICA:

Razón Social:	GESTIÓN DE SEGURIDAD ELECTRÓNICA
Sigla:	GSE
Número de Identificación Tributaria:	900.204.272 – 8
Registro Mercantil No: **Certificado de Existencia y Representante Legal:**	01779392 de 28 de febrero de 2008 https://gse.com.co/documentos/marco-regulatorio/Certificado-de-Existencia-y-Representante-Legal-GSE.pdf
Estado del registro mercantil:	Activo
Dirección social y correspondencia:	Calle 77 No. 7 – 44 Oficina 701
Ciudad / País:	Bogotá D.C., Colombia
Teléfono:	+57 (601) 4050082
Correo electrónico:	info@gse.com.co

Página Web:	www.gse.com.co

1.2 Nombre e identificación del documento.

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:

JERARQUÍA OID	DESCRIPCIÓN	NOMBRE
1	Formato ISO	No varía
3	Organización	No varía
6	Público	No varía
1	Internet	No varía
4.1 (31136)	Identificación de la organización	No varía, 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
21	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: **1.3.6.1.4.1.31136.1.1.21**

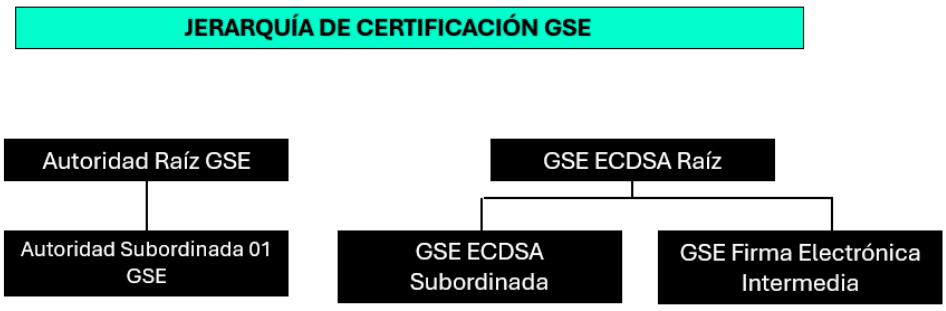
1.3 Participantes PKI.

1.3.1 Autoridad de Certificación (CA).

Es aquella persona jurídica, acreditada conforme a la ley 527 de 1999 y el Decreto 333 de 2014, facultada por el Gobierno colombiano o el Organismo Nacional de Acreditación en Colombia para prestar servicios de certificación digital de acuerdo con lo establecido en la Ley 527 de 1999, el Decreto Ley 0019 de 2012, el Decreto 333 de 2014, el Decreto 1471 de 2014 y los reglamentos que los modifiquen o complementen, es el origen de la jerarquía de certificación digital que le permite prestar los servicios relativos a las comunicaciones basadas en infraestructuras de clave pública.

Jerarquía de las CA.

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



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

1. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.
    a. Repositorios de la PKI.

- **Certificados Raíz ECD GSE**

https://certs2.gse.com.co/CA_ROOT.crt

https://certs2.gse.com.co/CA_ECROOT.crt

- **Lista de Certificados Revocados Raíz ECD GSE (CRL)**

https://crl2.gse.com.co/CA_ROOT.crl

https://crl2.gse.com.co/CA_ECROOT.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**

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.

1.3.2 Autoridad de Registro (RA).

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

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

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

1.3.3 Suscriptores

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

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

1.3.4 Partes de confianza.

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

publicados en esta DPC.

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

Precauciones que deben observar los terceros:

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

Solicitante.

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

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

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

1.3.5 Otros participantes.

Comité de Gerencia.

El comité de Gerencia es un organismo interno de ECD GSE, conformado por el representante legal suplente 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.

Proveedores de servicios.

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

Entidades de Certificación Digital Recíprocas.

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

Actualmente ECD GSE no cuenta con acuerdos vigentes de reciprocidad.

Peticiones, Quejas, Reclamos, Solicitudes y Felicitaciones.

Las peticiones, quejas, reclamos, solicitudes y felicitaciones sobre los servicios prestados por ECD GSE o entidades subcontratadas, explicaciones sobre esta 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 (601) 4050082

Correo electrónico: pqrs@gse.com.co

Dirección: Calle 77 No. 7 – 44 Oficina 701

Página Web: www.gse.com.co

Responsable: Servicio al Cliente

Una vez presentado el caso, este es transmitido con la información concerniente al proceso del Servicio al Cliente según procedimiento interno establecido para la investigación y gestión de estas. Del mismo modo, se determina qué área es responsable de tomar acciones correctivas o de mejora, 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 PQRSF y su comunicación final al suscriptor, responsable o parte interesada.

1.4 Uso del certificado.

1.4.1 Uso apropiado de los certificados

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 íntegro, 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.

La 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 y/o responsable, sin perjuicio de las acciones penales o civiles a las que haya lugar por parte de la ECD GSE.

1.4.2 Uso prohibido de los certificados

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

1.5 Administración de políticas.

1.5.1 Organización que administra el documento.

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

1.5.2 Contacto (Responsable de la ECD):

Nombre: María Ximena Flórez Artunduaga

Cargo: Representante Legal Suplente

Dirección: Calle 77 # 7-44 Oficina 701

Domicilio: Bogotá D.C., Colombia.

Teléfono: +57 (601) 4050082

Correo electrónico: info@gse.com.co

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

Área encargada: Project & Operations Manager

Dirección: Calle 77 # 7-44 Oficina 701

Domicilio: Bogotá D.C., Colombia.

Teléfono: +57 (601) 4050082

Correo electrónico: info@gse.com.co

1.5.4 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

1.6 Definiciones y acrónimos.

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 esté firmada digitalmente.

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

Criterios Específicos de Acreditación (CEA): Requisitos que deben ser cumplidos para obtener la Acreditación como Entidad de Certificación Digital - ECD, ante el Organismo Nacional de Acreditación de Colombia – ONAC; es decir para prestar servicios de certificación digital de acuerdo con lo establecido en la Ley 527 de 1999, el Decreto Ley 019 de 2012, los capítulos 47 y 48 del

título 2 de la parte 2 del libro 2 del Decreto Único del Sector Comercio, Industria y Turismo – DURSCIT y los reglamentos que los modifiquen o complementen.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Pseudónimo: Oculta con un nombre falso el suyo verdadero.

Pseudoanónimo: Utiliza un nombre falso de manera intencional

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

Solicitante: Toda persona natural o jurídica que solicita la expedición o renovación de un Certificado digital.

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

Tercero de buena fe: Persona o entidad diferente del suscriptor y/o responsable que decide aceptar y confiar en un certificado digital emitido por ECD GSE.

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

Acrónimos.

CA: Certification Authority

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

RNEC: Registraduría Nacional del Estado Civil

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

URL: Uniform Resource Locator

VA: Autoridad de validación (Validation Authority)

Estándares y Organismos de estandarización.

CEN: Comité Europeo de Normalización

CWA: CEN Workshop Agreement

ETSI: European Telecommunications Standard Inst

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

2. RESPONSABILIDADES DE PUBLICACIÓN Y REPOSITORIO.

2.1 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)**

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**

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 de Uso Interno.

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.

2.2 Publicación de información sobre 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.

2.3 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 auditoría 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 Auditoría 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 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.

2.4 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.

3. IDENTIFICACIÓN Y AUTENTICACIÓN.

3.1 Nombres.

3.1.1 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.

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

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

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

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

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

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

3.1.2 Necesidad de que los nombres tengan sentido.

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.

3.1.3 Anonimato o seudonimato de los suscriptores.

No se podrán utilizar alias, sobrenombres, apodos, diminutivos, y/o semejantes 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.

3.1.4 Reglas de interpretación de las distintas formas del 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).

3.1.5 Singularidad de los Nombres.

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

3.1.6 Reconocimiento, autenticación y rol de las marcas registradas.

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

3.2 Validación inicial de identidad.

La ECD GSE recibirá solicitudes para certificar la identificación inequívoca de la identidad del suscriptor (persona natural o jurídica) la veracidad y autenticidad de la información a través de cualquier sistema de identificación propio, o si pertenece a un tercero siempre y cuando subsista un contrato, convenio, acuerdo, alianza, y/o cualquier medio de relación contractual y/o comercial, directa y/o indirectamente, entre otras, con las que se realiza la verificación de la información de manera análoga a la validación presencial consumiendo alguno(s) de los servicios ampliamente usados de acuerdo con el servicio de certificado digital solicitado, para tal fin enumerados a continuación:

- Archivo Nacional de Identificación - Registraduría Nacional del Estado Civil.
- Muisca -Modelo Único de Ingresos, Servicio y Control Automatizado – y/o bases de datos de la DIAN (Dirección de impuestos y Aduanas Nacionales).
- Confronta.
- Registro Único Empresarial y Social y/o bases de datos de las Cámaras de Comercio (Para Persona Jurídica).
- Migración Colombia (para extranjeros).
- Bases de datos que disponga la Registraduría Nacional del Estado Civil que permitan la identificación inequívoca del solicitante. De acuerdo con la normativa vigente expedida por la Entidad.
- Selfie contra documento de identificación (cédulas de ciudadanía de hologramas, digital física y de extranjería)

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 mismo, 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) y correo electrónico son revisados y/o validados en conjunto con el formulario de solicitud, la información y/o documentación suministrada para cada tipo de certificado digital.

El documento Registro Único Tributario – RUT se solicitará en el formato actualizado de DIAN que incluye código QR (si aplica; opcional)

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 sí los mecanismos de verificación que apliquen para confirmar la veracidad y autenticidad de la información, como podrían ser:

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

- Muisca - Modelo Único de Ingresos, Servicio y Control Automatizado – y/o bases de datos de la DIAN (Dirección de impuestos y Aduanas Nacionales).
- Registro Único Empresarial y Social y/o bases de datos de las Cámaras de Comercio (Para Persona Jurídica).
- Migración Colombia (para extranjeros).

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, si la solicitud de certificado digital de persona natural se realiza directa y/o indirectamente desde las plataformas de la Registraduría Nacional del Estado Civil – RNEC previa verificación por parte de dicha entidad y sus funciones descritas en el Decreto 1010 de 2000:

(...)

ARTÍCULO 2°. Objeto. Es objeto de la Registraduría Nacional del Estado Civil - , registrar la vida civil e identificar a los colombianos y organizar los procesos electorales y los mecanismos de participación ciudadana, en orden a apoyar la administración de justicia y el fortalecimiento democrático del país.

(...)

ARTÍCULO 5°. Funciones. Son funciones de la Registraduría Nacional del Estado Civil, las siguientes:

19. Expedir y elaborar las cédulas de ciudadanía de los colombianos, en óptimas condiciones de seguridad, presentación y calidad y adoptar un sistema único de identificación a las solicitudes de primera vez, duplicados y rectificaciones.

20. Atender todo lo relativo al manejo de la información, las bases de datos, el Archivo Nacional de Identificación y los documentos necesarios para el proceso técnico de la identificación de los ciudadanos, así como informar y expedir las certificaciones de los trámites a los que hubiere lugar.

24. Atender las solicitudes de expedición de la cédula de ciudadanía en los consulados de Colombia en el exterior para que quienes estén habilitados puedan ejercer sus derechos políticos como ciudadanos colombianos y brindar información acerca de su trámite.

Eso quiere decir que si la solicitud del certificado digital para un solicitante (ciudadano) es realizada desde la RNEC como fuente de información principal de Colombia, se asegura que el solicitante tuvo una validación previa de su identidad y datos de domicilio para realizar el trámite de expedición de la cédula de ciudadanía, la ECD GSE recibirá la información de dicha fuente, se asegura la veracidad y autenticidad realizando la identificación inequívoca del suscriptor, la ECD GSE mantendrá los registros de la solicitud asegurando el proceso de Ciclo de Vida de la Certificación Digital.

Para el caso de los certificados de firma electrónica se realiza adicionalmente 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.

3.2.1 Método para demostrar la posesión de la clave 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.

En virtud de lo establecido por ONAC en el CEA 3.0-07, para el caso en que el par de llaves son generadas por el solicitante en su propia infraestructura, por ejemplo, para la utilización del certificado en plataformas desatendidas, el solicitante debe aceptar y cumplir con los requerimientos expuestos en el documento Anexo 1 de Términos y Condiciones numeral 6 literal m), si estas fueron generadas por software y mediante dispositivos que cumplen con el Anexo F del CEA, si fueron generadas por hardware.

3.2.2 Autenticación de la identidad de la organización.

Para asegurar la identidad de una persona jurídica, la RA GSE exige la entrega de la información de la persona jurídica y/o 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.

3.2.3 Autenticación de la identidad individual.

Para asegurar la identidad de una persona natural, la RA GSE, exige el registro de la información que demuestre la identidad del solicitante y/o presentación del documento de identidad del solicitante digital y verifica su existencia y correspondencia contra bases de datos propias y/o de terceros, sean oficiales y/o privadas a través de contratos, convenios, acuerdos, alianzas, y/o cualquier tipo de relación contractual y/o comercial, ya sean directas y/o indirectas. 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.

3.2.4 Información de suscriptor no verificada.

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

Para el caso específico de los datos de domicilio, la RA presume la veracidad de la información suministrada por el solicitante en aplicación del principio de buena fe de acuerdo con nuestra Constitución Política, razón por la cual no se hace necesario un proceso de validación adicional.

3.2.5 Validación de la autoridad.

GSE utiliza un método de comunicación fiable con el Solicitante o su representante.

La autoridad de los Solicitantes para solicitar Certificados en nombre de una organización se verifica durante la validación de la identidad del Solicitante.

GSE puede permitir que los Solicitantes especifiquen por escrito las personas que pueden solicitar Certificados en su nombre. Cuando se haya realizado dicha especificación, GSE no aceptará solicitudes de certificados que estén fuera de esta especificación pero, previa solicitud por escrito, proporcionará a la empresa Solicitante una lista de sus solicitantes de certificados autorizados.

3.2.6 Criterios de interoperabilidad.

ECD GSE únicamente emitirá certificados digitales a ECD Subordinadas, donde la toma de decisión de emitir o activar el servicio de certificación digital sea de la ECD GSE a través de la recomendación con base en la revisión de la solicitud de la RA de GSE.

3.3 Identificación y Autenticación para renovación de llaves.

3.3.1 Identificación y autenticación para la rutina de reúso llaves.

La ECD GSE no considera el proceso de reúso de las llaves pública y privada del certificado para la renovación de certificados digitales.

En caso de ser solicitada la renovación de un certificado emitido, debe cumplir el proceso de solicitud de emisión de la misma manera que un nuevo certificado, el cual será generado a partir de un nuevo par de llaves.

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. Lo anterior, a través de cualquier sistema de identificación siempre que subsista contrato, convenio, acuerdo, alianza, y/o cualquier tipo de relación contractual y/o comercial directa y/o indirectamente, entre otras, con la Registraduría Nacional del Estado Civil, confronta, Bases de Datos de burós de crédito o fuentes de datos del gobierno. 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.

3.3.2 Identificación y autenticación para la rutina de reúso llaves tras la revocación.

GSE no considera el proceso de reúso de las llaves pública y privada del certificado para la renovación de certificados digitales, cuando haya sido solicitada su revocación.

En caso de ser solicitada la revocación de un certificado emitido y luego se pretende solicitar de nuevo el certificado con los mismos datos del revocado, debe cumplir el proceso de solicitud de emisión de la misma manera que un nuevo certificado, el cual será generado a partir de un nuevo par de llaves.

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).

3.4 Identificación y autenticación para la solicitud 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 del certificado. De acuerdo con lo establecido en el procedimiento de revocaciones.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO.

4.1 Solicitud de certificado.

Cualquier persona que requiera la prestación del servicio de certificación digital, lo podrá hacer utilizando los canales, medios o mecanismos dispuestos por ECD GSE, en los que se obtendrá la información necesaria para gestionar la solicitud del servicio de certificación digital requerido. Una vez aceptados los términos y condiciones y radicada la solicitud la información es enviada a la Autoridad de Registro quien se encargará de revisar la solicitud para asegurar la identificación inequívoca de la identidad del suscriptor (Persona Natural o Jurídica), la veracidad y autenticidad de la información que permita dar una recomendación para la toma de decisión dando cumplimiento a los requisitos exigidos en las Políticas de Certificación.

El solicitante aporta la información y/o los documentos necesarios según aplique entregándolos escaneados o en original electrónico, preservando la legibilidad para el uso de la información. También la información puede ser obtenida a través de bases de datos de plena confianza, conforme a las ya nombradas en numerales precedentes con lo cual se surten los procedimientos establecidos por la ECD GSE, para la obtención del certificado digital.

La ECD GSE, se reserva el derecho de solicitar información y/o 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 la ECD GSE a través de otros medios o mecanismos dispuestos. La información y/o documentación suministrada será revisada de acuerdo con los Criterios y Métodos de Evaluación de Solicitudes establecidos por GSE.

El solicitante acepta que la 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, idoneidad legal o moral de todo el sistema de certificación digital, notificando al solicitante la no aprobación.

Para la solicitud de certificado de firma electrónica se tiene establecido el **PROCEDIMIENTO DE ADQUISICIÓN FIRMA ELECTRÓNICA**.

4.1.1 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.

4.1.2 Proceso de solicitud, registro y responsabilidad.

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.

4.2 Procesamiento de solicitud de certificado.

4.2.1 Procedimiento para el procesamiento de la solicitud/ identificación y autentificación.

Las funciones de autenticación y verificación de la identidad del solicitante son realizadas por la RA de GSE, encargada de dar la recomendación para la decisión sobre la certificación digital con base en la revisión de la solicitud, quien comprueba si la

información suministrada es auténtica y cumple con los requisitos definidos para cada tipo de certificado de acuerdo con esta DPC.

La información y/o documentación que la RA de GSE deberá revisar para dar la recomendación para la toma de decisión para la correcta emisión de cada tipo de certificado se define en las Políticas de Certificado para Certificado Digitales.

4.2.2 Criterios de aceptación o rechazo de la solicitud.

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 realizó la validación de identidad, pasados quince (15) días sin que se subsane la novedad, la RA de la ECD GSE tendrá como alternativa realizar el rechazo de la solicitud y se notificará al solicitante para que tramite una nueva solicitud.

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

4.2.3 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 información y/o documentación solicitada y el solicitante haya aprobado la validación inicial de la 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.

4.3 Emisión del Certificado.

4.3.1 Acciones 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.

4.3.2 Mecanismos de notificación autorizados por los suscriptores.

Mediante correo electrónico u otro medio previamente definido y autorizado para tal fin, se notificará al suscriptor la emisión de su certificado digital. El suscriptor acepta y reconoce que, una vez recibida dicha notificación, el certificado se entenderá como emitido. La notificación se considerará recibida en el momento en que no se presente novedad en la entrega, es decir, cuando el sistema confirme que la comunicación fue enviada de manera satisfactoria al canal autorizado. En el caso en que el suscriptor solicitó que la emisión del certificado digital sea en un dispositivo criptográfico, se entenderá como entregado una vez se tenga el registro de envío: carta de entrega y/o la guía de envío al operador logístico o mensajería y/o confirme en la notificación de emisión que ha recibido el dispositivo criptográfico
La publicación de un certificado en el repositorio de certificados constituye la prueba y una notificación pública de su emisión.

4.4 Aceptación del Certificado.

4.4.1 Mecanismo de aceptación del certificado por parte del suscriptor.

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 informarlo y/o solicitar su revocación.

4.4.2 Publicación del certificado por la CA

GSE publica todos los certificados de CA raíz y subordinadas en su repositorio y dispone de un mecanismo para la consulta de los certificados de entidad final por parte del suscriptor como responsable del certificado digital. En la página web: Consultas en línea

4.4.3 Notificación de la emisión de certificados por parte de la ECD GSE a otras entidades.

Véase el apartado 4.4.2. anterior.

4.5 Uso de pares de llaves y certificados.

4.5.1 Responsabilidades del Suscriptor frente al uso de la llave privada y el certificado.

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.

4.5.2 Responsabilidades del tercero de confianza relacionadas con el uso de la clave privada y el certificado del suscriptor.

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 la lista de revocación de certificados, 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

4.6 Renovación del certificado

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

4.6.1 Circunstancias para la renovación de certificado.

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

4.6.2 Quién puede solicitar una renovación sin cambio de llaves.

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

4.6.3 Trámites para la solicitud de renovación de certificados.

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

4.6.4 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.

4.6.5 Forma en la que se acepta la renovación de un certificado.

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

4.6.6 Publicación del certificado renovado por la ECD.

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

4.6.7 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.

4.7 Reúso de llave del certificado

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

En conclusión, GSE trata todas las solicitudes de reemisión y/o renovación de certificados como solicitudes de emisión de un nuevo certificado, teniendo en cuenta que no hace en ningún caso reúso de llaves.

4.7.1 Circunstancia para el reúso de llaves del certificado.

Se puede generar un nuevo certificado digital a solicitud del suscriptor y/o responsable por finalización de vigencia o revocación del certificado actual de conformidad con las causales mencionadas en esta DPC o cuando así lo requiera el suscriptor.

No procede. Véase el apartado 4.7

4.7.2 Quién puede solicitar la certificación de una nueva llave pública.

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 responsables o designados debidamente facultados o apoderados.

No procede. Véase el apartado 4.7

4.7.3 Procesamiento de las solicitudes de reúso de llave de certificados.

El procedimiento para renovación de certificados digitales es igual al procedimiento de solicitud de un certificado nuevo. El suscriptor debe acceder por los medios o mecanismos para tal fin para radicar la solicitud a la ECD GSE e iniciar el proceso de solicitud de un nuevo certificado digital de la misma forma que lo hizo cuando radicó la solicitud del certificado digital por primera vez. Su solicitud será nuevamente validada con el fin de actualizar datos si se requiere.

No procede. Véase el apartado 4.7

4.7.4 Notificación al suscriptor de la emisión de un nuevo certificado.

Mediante correo electrónico u otro medio para tal fin se notifica al suscriptor la emisión de su certificado digital y por consiguiente el suscriptor acepta y reconoce que una vez reciba dicha notificación, se entenderá la aceptación de los términos y condiciones de la ECD GSE que ha sido emitido el certificado. En el caso en que el suscriptor solicitó que la emisión del certificado digital sea en un dispositivo criptográfico, se entenderá como entregado una vez se tenga el registro de envío: carta de entrega y/o la guía de envío al operador logístico o mensajería y/o confirme en la notificación de emisión que ha recibido el dispositivo criptográfico

No procede. Véase el apartado 4.7

4.7.5 Conducta que constituye la aceptación de un certificado con reúso de llave.

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 este así lo acepta.

No procede. Véase el apartado 4.7

4.7.6 Publicación del certificado con reúso de llave por parte de la CA

No aplica por cuanto ECD GSE no realiza reúso de llaves de certificados.

No procede. Véase el apartado 4.7

4.7.7 Notificación de la emisión de certificados por parte de la CA a otras entidades

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

No procede. Véase el apartado 4.7

4.8 Modificación de Certificado.

Los certificados digitales emitidos por ECD GSE no pueden 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.

4.8.1 Circunstancia para la modificación del certificado.

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

4.8.2 Quién puede solicitar la modificación del certificado.

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

4.8.3 Tramitación de solicitudes de modificación de certificados.

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

4.8.4 Notificación al suscriptor de la emisión de un nuevo certificado

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

4.8.5 Conducta que constituye la aceptación de un certificado modificado.

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

4.8.6 Publicación del certificado modificado por la CA.

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

4.8.7 Notificación de la emisión de certificados por parte de la CA a otras entidades.

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

4.9 Revocación y Suspensión del Certificado.

4.9.1 Circunstancias para revocación.

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:

1. Por pérdida o inutilización de la clave privada o certificado digital.
2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.
3. Cambios en las circunstancias por la cuales ECD GSE autorizó la emisión del certificado digital.
4. 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:

1. A petición del suscriptor, responsable o un tercero en su nombre y representación.
1. Por muerte del suscriptor o responsable.
2. Por la confirmación o evidencia de que alguna información o hecho contenido en el certificado digital es falso.
3. 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.
4. Por orden judicial o de entidad administrativa competente.
5. Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
6. Por incapacidad sobrevenida del suscriptor o responsable.
7. Por liquidación de la persona jurídica representada que consta en el certificado digital.
8. Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
9. Por pérdida o inutilización del dispositivo criptográfico que haya sido entregado por ECD GSE.
10. Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato.
11. 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.
12. Por el manejo indebido por parte del suscriptor del certificado digital.
13. 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.
14. 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.
15. En cualquier momento que se evidencie falsedad en los datos suministrados por el solicitante, suscriptor o responsable.
16. Por incumplimiento por parte de la ECD GSE, el suscriptor o responsable de las obligaciones establecidas en la DPC.
17. 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.

4.9.2 Quién puede solicitar la revocación de un certificado

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 Tecnología de la CA como máximo ente de control que tiene atribuida la administración de la seguridad de la infraestructura tecnológica de la 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 revocación de un certificado.

4.9.3 Procedimiento para solicitud de revocación de un certificado.

El suscriptor y/o responsable, un tercero de buena fe o cualquier persona 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 , 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 y envía la solicitud de revocación de su certificado digital; una vez la solicitud termine, se realizará la revocación de su certificado digital y al correo electrónico registrado se le enviará la notificación de revocación.

Otros medios dispuestos para realizar la revocación del certificado digital por parte del suscriptor y/o responsable y/o tercero de buena fe podrán ser a través de la(s) herramienta(s) y/o aplicación(es) desde donde se radicó la solicitud para la emisión del certificado digital de terceros autorizados.

- 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 digital firmada o correo electrónico con los datos del suscriptor y causal de revocación, Formulario de Revocación Servicio de Certificación Digital.

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, opción Revocaciones y Certificados raíz y subordinado

La ECD por medio del área de Tecnología 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.

4.9.4 Periodo de gracia para solicitar revocación de un certificado.

Previa revisión de una solicitud de revocación la ECD GSE procederá en forma inmediata con la revocación solicitada, dentro de los horarios de oficina de este. 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 la ECD GSE no podrá reactivarlo.

El procedimiento utilizado por la ECD GSE para verificar una solicitud de revocación formulada por una persona determinada, es revisar 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 la ECD GSE, toda vez que reconoce y acepta que el control, custodia y confidencialidad de la llave privada es responsabilidad exclusiva de este.

4.9.5 Tiempo dentro del cual la CA debe procesar la solicitud de revocación.

La solicitud de revocación de un certificado digital debe ser atendida con la máxima prioridad, 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, la ECD GSE como prestador de servicios de certificación y responsable de la CA, 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 la 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.* La ECD GSE no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante el suscriptor y/o responsables del certificado o terceros de confianza a excepción de lo establecido por las disposiciones de la presente DPC.

4.9.6 Requisito de comprobación de revocación para las partes confiantes.

Es responsabilidad del suscriptor y/o responsable de un certificado digital y este 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 y/o responsable al tercero de buena fe que, para realizar dicha consulta, dispone de la lista de certificados revocados CRL, publicada de manera periódica por la ECD GSE.

Las partes confiantes deben confirmar la validez de cada certificado de la cadena de certificación, comprobando la CRL o el respondedor OCSP correspondiente antes de confiar en un certificado emitido por la CA de la ECD GSE.

4.9.7 Frecuencia de emisión 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 7×24×365, 99.8% uptime por año.

4.9.8 Latencia máxima de las CRLs.

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

4.9.9 Disponibilidad de verificación en línea de revocación/estado

La 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 las respuestas generadas por el servicio, tal es el caso de OPENSSL.

4.9.10 Requisitos de comprobación de revocación en línea.

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.

4.9.11 Otras formas de anuncios de revocación disponibles.

Dentro de las 24 horas siguientes a la revocación de un certificado, la ECD GSE informa al suscriptor y/o responsable mediante correo electrónico u otro medio para tal fin se notifica la revocación de su certificado digital y por consiguiente el solicitante acepta y reconoce que una vez reciba la notificación se entenderá que su solicitud fue atendida. Se entenderá que se ha recibido la información donde se notifica la revocación de un certificado cuando dicha notificación ingrese en el sistema de información designado por el solicitante.

La publicación de un certificado revocado en la CRL constituye la prueba y una notificación pública de su revocación.

La 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 la ECD GSE.

4.9.12 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 este 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.

En caso de que la llave privada del suscriptor se vea comprometida, el suscriptor deberá notificar inmediatamente a la ECD GSE el evento de compromiso de la llave privada. La ECD GSE revocará el certificado en cuestión y el mismo se visualizará en la siguiente CRL que se publique en la siguiente actualización para informar a las partes usuarias de que el certificado ya no es de confianza.
El suscriptor es responsable de investigar las circunstancias de dicho compromiso.

4.9.13 Circunstancias para la suspensión

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

4.9.14 Quién puede solicitar la suspensión

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

4.9.15 Procedimiento de solicitud de suspensión

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

4.9.16 Límites del periodo de suspensión

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

4.10 Servicios de Estado del Certificado.

4.10.1 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 vía CRL.

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

Las entradas de revocación de una CRL o respuesta OCSP no se eliminan hasta después de la fecha de caducidad del certificado revocado.

4.10.2 Disponibilidad servicio

La GSE ECD opera y mantiene su capacidad CRL y OCSP con recursos suficientes para proporcionar un tiempo de respuesta de diez segundos o menos en condiciones normales de funcionamiento.
Los servicios de estado de certificados están disponibles 24 horas al día, 7 días a la semana, a menos que no estén disponibles temporalmente debido a tareas de mantenimiento pero siempre garantizando una disponibilidad de consulta en línea 7×24×365, 99.8% uptime por año

Número de versión.

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

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).

Disponibilidad CRL.

Conforme a lo indicado en el numeral 4.9.9 Disponibilidad de verificación en línea de revocación/estado

Perfil OCSP.

El servicio OCSP cumple con lo estipulado en el RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

Número de versión.

Cumple con la OCSP Versión 1 del RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

Extensiones OCSP.

No aplica

Disponibilidad servicio OCSP

Conforme a lo indicado en el numeral 4.9.9 Disponibilidad de verificación en línea de revocación/estado

4.10.3 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.

4.11 Fin de la Suscripción.

La 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.

4.12 Custodia y Recuperación de Llaves

4.12.1 Política y prácticas en materia de custodia y recuperación de llaves.

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

Los dispositivos criptográficos en hardware utilizados por la 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 o superior 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 vigente 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.

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 este así lo acepta y reconoce.

4.12.2 Política y prácticas de encapsulación y recuperación de llaves 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 proteger el acceso al PIN, por lo que si se presenta olvido del PIN se radicará un caso en la mesa de servicios de la ECD – GSE para verificar la solicitud y de ser necesario por el suscriptor podrá radicar la solicitud de revocación del certificado digital por los canales dispuestos para tal fin y gestionará la solicitud de un nuevo certificado digital.

5. INSTALACIONES, GESTIÓN Y CONTROLES OPERATIVOS.

5.1 Controles de Seguridad Física.

La infraestructura de CA de la ECD GSE se encuentra en instalaciones seguras y se gestiona desde ellas. Existen y se siguen procedimientos de seguridad detallados que prohíben el acceso y la entrada no autorizados a las áreas de las instalaciones en las que residen los sistemas de CA.

5.1.1 Ubicación física de la construcción de la ECD.

La ECD GSE dispone de medidas de seguridad para el control de acceso al edificio donde se encuentra su infraestructura, los servicios de certificación digital 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.

La ECD GSE garantiza que los servidores de la PKI se encuentran en operación continua 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:

1. Ingresan únicamente personas autorizadas.
2. Los equipos de comunicación crítica están debidamente protegidos en racks.
3. No posee ventanas hacia el exterior del edificio.
4. Se monitorea a través de un circuito cerrado de televisión las 24 horas, con cámaras tanto al interior como al exterior del centro de cómputo.
5. Cuenta con control de acceso físico.
6. Sistemas de protección y prevención de incendios: detectores de humo, sistema de extinción de incendios.

7. Cuenta con personal capacitado para actuar ante eventos catastróficos.
8. Cuenta con un sistema detector de intrusos físicos.
9. El cableado está debidamente protegido contra daños, intentos de sabotaje o interceptación por medio de canaletas

5.1.2 Mecanismos de control de 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.

5.1.3 Energía 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.

5.1.4 Exposición al agua.

Los datacenter donde se encuentran alojados los servicios de PKI cuentan con aislamientos de posibles fuentes de agua y cuentan con sensores de detección de inundaciones conectados al sistema general de alarma.

5.1.5 Prevención y protección contra 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.

5.1.6 Sistema de copia de respaldo - Almacenamiento de medios.

Se cuenta con procedimientos de toma de backups, restauración y pruebas para las bases de datos para los servicios acreditados.

Los servidores misionales se encuentran en ambientes cloud, sin embargo, a los servidores onpremises se les realizan los backups y se almacenan en un servidor NAS local con su respectiva contingencia.

5.1.7 Eliminación de residuos

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.

5.1.8 Copia de seguridad fuera de sitio.

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.

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.

5.2 Controles de Procedimiento.

5.2.1 Roles de confianza de la ECD.

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

- **Agentes de la RA:** Personas responsables de las operaciones diarias tales como lo 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.

5.2.2 Cantidad de personas requeridas en cada rol.

Para cada uno de los roles mencionados la ECD garantizará los colaboradores para realizar las tareas que afectan a la gestión de claves criptográficas de la propia ECD.

5.2.3 Identificación y autenticación de 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 o certificados digitales.

5.2.4 Roles que requieren segregación de funciones.

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

5.3 Controles de personal.

5.3.1 Requisitos sobre la cualificación, experiencia y requisitos de habilitación.

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 y los procedimientos de servicios de certificación digital. El candidato a un cargo debe tener la formación, experiencia, conocimientos y habilidades definidas en el documento Perfil y Funciones de cargo.

5.3.2 Procedimiento de verificación 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.

5.3.3 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.

5.3.4 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.

5.3.5 Frecuencia y secuencia de rotación de tareas.

No existe rotación de tareas en los cargos mencionados.

5.3.6 Sanciones por actuaciones no autorizadas.

Dentro del Reglamento Interno de Trabajo es calificada como falta grave ejecutar acciones no autorizadas y las personas serán sancionadas de conformidad con reconvención y/o proceso disciplinario.

5.3.7 Controles para 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.

5.3.8 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.

5.4 Procedimientos de Registro de Auditoría.

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

5.4.1 Tipo 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

5.4.2 Frecuencia de procesamiento de Logs.

Los registros de auditoría 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.

5.4.3 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, puede proceder a destruirlos, no obstante, si los registros se están utilizando en procesos judiciales su retención serán por tiempo indefinido.

5.4.4 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.

5.4.5 Procedimiento de copia de seguridad de los registros de auditoría.

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

5.4.6 Sistema de recolección de registro 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

5.4.7 Notificación a responsable de incidente de seguridad.

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.

5.4.8 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

5.5 Archivo de Registros.

El registro de archivo y registro de eventos es ejecutado por el NOC SOC de la ECD GSE.

5.5.1 Tipos de registros objeto de archivo.

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

5.5.2 Periodo de retención para archivo

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

5.5.3 Protección de archivo

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

5.5.4 Procedimientos de copia de respaldo de archivos

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.

5.5.5 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.

5.5.6 Sistema de recolección de archivos (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.

5.5.7 Procedimientos para obtener y verificar información de archivo.

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 auditorías ante incidentes de seguridad.

5.6 Cambio de Llaves.

Cambio de llave 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.

Cambio de llaves de la Subordinada de ECD GSE.

El procedimiento de cambio de llaves de una subordinada de la 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.

5.7 Compromiso y Recuperación de Desastres.

5.7.1 Procedimientos de gestión de incidentes, eventos y compromisos

La ECD GSE tiene establecido y probado un **Procedimiento de incidentes, eventos y compromisos de Seguridad de la Información** 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.

5.7.2 Procedimiento en caso de daño de los recursos informáticos, el software y/o los datos.

Ante una sospecha de alteración de los recursos hardware, software, o datos se detendrá el funcionamiento de la ECD GSE 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.

5.7.3 Procedimiento de recuperación frente al compromiso de la llave privada de la ECD.

La ECD GSE tiene establecido y probado un Plan de Continuidad de Negocio que define las acciones a seguir en caso de producirse una vulnerabilidad de la llave privada de la raíz de la 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/o responsables se deben emitir nuevos certificados, adicionalmente, este plan se ejecutará bajo los siguientes escenarios:

1. Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
2. Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.
3. Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.
4. Cuando se presente cualquier otro evento o incidente de seguridad de la información.

En caso de compromiso de la ECD GSE:

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

5.7.4 Capacidad de recuperación en caso de desastre.

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, 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.

5.8 Cese de la CA o la RA.

Procedimiento en caso de cese de la CA y la RA

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, la Circular Externa No. 30-2021 y conforme al Decreto 333 de 2014 y el DURSCIT artículo 2.2.2.48.3.8, las entidades de certificación digital abiertas deberán informar de la cesación de actividades a ONAC 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:

- La terminación de la actividad o actividades y la fecha precisa de cesación.
- Las consecuencias jurídicas de la cesación respecto a los servicios acreditados
- La posibilidad de que un suscriptor obtenga el reembolso equivalente al valor del tiempo de vigencia restante sobre el servicio contratado.
- 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.

La 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.

La ECD GSE cuenta con un plan de seguridad en caso de cese de actividades el cual contempla los lineamientos y actividades para la ejecución de este.

6. CONTROLES TÉCNICOS DE SEGURIDAD.

6.1 Generación e Instalación de Pares de Llaves.

6.1.1 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 la ECD. Para el almacenamiento de la llave privada se utilizó un dispositivo criptográfico homologado FIPS 140-2 nivel 3 o superior.

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 o superior.

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 o superior.

6.1.2 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 esta. No existe por tanto ninguna copia de llave privada del suscriptor.

6.1.3 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.

6.1.4 Entrega de la llave pública de la CA a las partes confiantes.

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 2.1 Repositorios, 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 2.1 Repositorios, Certificados Subordinadas ECD GSE.

6.1.5 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 22047 posibilidades por cada

número. Se estima que descifrar una llave pública de 2048 bits requeriría un trabajo de procesamiento del orden de 3 ×1020 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 pública correspondiente sería P=k*G y se da a conocer. El problema del algoritmo discreto dice que es un problema de complejidad exponencial obtener k a partir de P. Se estima que se requieren 2.4×1026 MIPS-año para derivar una llave pública de curva elíptica de 256 bits.

6.1.6 Parámetros de generación de la llave pública y control de 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.

6.1.7 Fines de uso de la llave (según el campo de uso de la llave X.509 v3).

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

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

6.2.1 Estándares y controles para uso de 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.

6.2.2 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

6.2.3 Custodia de la llave privada de la ECD.

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.

6.2.4 Copia de respaldo 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 6.2.3 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.

6.2.5 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 6.2.3 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.

6.2.6 Transferencia de llaves privadas hacia o desde un 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 6.2.3 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.

6.2.7 Almacenamiento de la llave privada en el 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 6.2.3 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.

6.2.8 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 GSE. Se necesitan al menos 2 personas para la activación de las llaves.

6.2.9 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.

6.2.10 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.

6.2.11 Clasificación del módulo criptográfico.

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

Evaluación del módulo criptográfico.

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

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 inglés) y por el ONAC, si se materializa alguna circunstancia

en donde los algoritmos utilizados para firma y cifrado por ECD GSE se 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.

6.3 Otros Aspectos de la Gestión del Par de Llaves.

6.3.1 Archivo de la llave pública.

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

6.3.2 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.

6.4 Datos de Activación.

6.4.1 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.

6.4.2 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.

6.4.3 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.

6.5 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 (Red Interna, Red administrativa, entre otros)
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red configurados en el firewall.

6.5.1 Requisitos técnicos específicos de seguridad informática.

ECD GSE cuenta con una infraestructura tecnológica debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar la disponibilidad que se establecen en el CEA 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.

6.5.2 Clasificación de la seguridad informática.

La seguridad de los equipos de usuario final se gestiona desde ECD GSE y se soporta con un análisis de riesgos de tal forma que las medidas de seguridad implantadas sean respuestas a la probabilidad e impacto producido por un grupo de amenazas definidas que puedan aprovechar las brechas de seguridad.

Adicionalmente, se realizan pruebas de seguridad (ethical hacking) periódicas, de manera que se identifiquen posibles vulnerabilidades de los sistemas y que coadyuven con el cierre de estas.

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, eventos y compromisos que especifica las acciones a ejecutar, componentes o recursos a utilizar y cómo 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.

1. **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.

1. **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 dónde llegó el ataque y la máxima información posible de la incidencia.
2. **Control de daños ocasionados por incidente:** Reaccionar rápidamente para contener la incidencia y evitar que se propague tomando medidas como bloquear accesos al sistema.
3. **Investigación y recopilación de evidencias:** Revisar registros de auditoría para realizar un seguimiento de lo ocurrido.
4. **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.
5. **Análisis posterior de la incidencia para la mejora 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.

6.6 Controles de Técnicos del Ciclo de Vida.

6.6.1 Controles de desarrollo de sistemas.

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

6.6.2 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 con la disponibilidad mínima que se solicita en el CEA.

6.6.3 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.

6.7 Controles de Seguridad de Red.

ECD GSE cuenta con una infraestructura de red debidamente monitoreada y equipada con elementos de seguridad requeridos para garantizar la 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.

6.8 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.co

7. PERFILES DE CERTIFICADO, CRL Y OCSP.

7.1 Perfil del Certificado.

Los certificados cumplen con el estándar X.509 vigente 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 esta, contendrá como mínimo lo siguiente:

1. Nombre, dirección y domicilio del suscriptor.
2. Una Identificación única del suscriptor nombrado en el certificado.
3. El nombre y el lugar donde realiza actividades la CA
4. Llave pública del certificado.
5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
6. El número de serie (único) del certificado.
7. Fecha de emisión y expiración del certificado.

Adicional se incluye el Código de acreditación asignado por el ONAC conforme a la extensión de certificado definido en el numeral 4.2 del RFC 5280 identificado en el campo: Nombre alternativo del sujeto

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.
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 subniveles 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 subniveles que se admiten en la ruta del certificado. No existe restricción para ECD GSE, por tanto, es cero.

7.1.1 Números de versión.

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

7.1.2 Extensiones del certificado.

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

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”.

Extensión de política de certificados.

La extensión de “certificatepolicies” del X.509 vigente 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.

Nombre alternativo del sujeto.

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

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 subniveles en la ruta del certificado. Es un campo crítico.

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

7.1.3 Identificadores de objetos algorítmicos.

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

7.1.4 Formas de nombres.

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

7.1.5 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”.

7.1.6 Identificador del 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.

7.1.7 Uso de la extensión Policy Constrains.

No se estipula.

7.1.8 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 está publicada la DPC.

7.1.9 Tratamiento semántico para la extensión Certificate Policies.

No se estipula.

7.2 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.

7.2.1 Número(s) de versión

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:

7.2.2 CRL y extensiones de entrada 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).

7.3 Perfil OCSP.

El servicio OCSP cumple con lo estipulado en el RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

7.3.1 Número(s) de versión

Cumple con la OCSP Versión 1 del RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP" y RFC6019 "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments".

7.3.2 Extensiones OCSP

Las singleExtensions de una respuesta OCSP NO CONTIENEN la extensión de entrada CRL reasonCode (OID 2.5.29.21).

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES.

8.1 Frecuencia o Circunstancias de la Evaluación.

El cumplimiento de los controles que garanticen la seguridad en la emisión de certificados digitales se evaluará a través de auditoría, esta se realizará una vez por cada año calendario, considerando el período comprendido entre enero y diciembre del año en curso, ejecutada por una firma de auditoría externa.

8.2 Identidad y cualificaciones del evaluador.

De conformidad con el Decreto 333 de 2014 y específicamente en el **Artículo 14. Auditorías.** Las entidades de certificación deberán cumplir con la auditoría 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.

8.3 Relación del evaluador con la entidad evaluada.

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.

8.4 Temas objeto de evaluación.

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 – Auditoría de Tercera Parte del documento de CEA establecidos por ONAC el entregable es el informe de conformidad, no se permite con salvedad o razonabilidad.

8.5 Acciones tomadas como resultado de la deficiencia.

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.

8.6 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 debe ser remitido a ONAC.

9. OTROS ASUNTOS COMERCIALES Y LEGALES.

9.1 Honorarios.

No Aplica.

9.1.1 Tasas de emisión o renovación de certificados

GSE cobra tasas por la emisión y renovación de certificados. GSE podrá modificar sus tarifas de conformidad con el contrato de cliente aplicable. Ver tabla de tarifas en el numeral 9.17

9.1.2 Tasas de acceso a certificados

Si no se especifica en los correspondientes acuerdos legales o CP de un tercero asociado, GSE podrá cobrar una tarifa razonable por el acceso a sus bases de datos de certificados.

GSE no cobra tasas por revocación de certificados ni por comprobar el estado de validez de un certificado emitido utilizando una CRL. GSE puede cobrar una tasa por proporcionar información sobre el estado de los certificados a través de OCSP

9.1.4 Tasas por otros servicios

Sin estipulación.

9.1.5 Política de reembolso

Según lo establecido en el correspondiente acuerdo de cliente con GSE.

9.2 Responsabilidad Financiera.

9.2.1 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.

9.2.2 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.

9.2.3 Cobertura de seguro o garantía para entidades finales

Sin estipulación.

9.3 Confidencialidad de la Información Comercial.

9.3.1 Alcance de 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.

Información confidencial.

La siguiente información es considerada confidencial:

1. Llave privada de la Autoridad de Certificación y/o ECD
2. Llave privada del suscriptor o entidad
3. Información suministrada por el suscriptor o entidad y que no sea necesaria para validar la confianza del suscriptor o entidad
4. Información acerca del solicitante, suscriptor y/o responsable obtenida en fuentes diferentes (por ejemplo, de un reclamante o de los reguladores)
5. Registros de las transacciones
6. Registros de auditoría
7. Políticas de seguridad
8. Plan de Continuidad de Negocio
9. Toda aquella información que sea calificada como "Confidencial" en los documentos entregados por ECD GSE

9.3.2 Información no confidencial.

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

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

9.3.3 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 de acuerdo con lo definido en la TRD. 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.

9.4 Privacidad de la Información Personal.

9.4.1 Plan de Privacidad - 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, decreto 1377 de 2013, y demás normas que la adicionen, modifiquen, complementen, sustituyan, la cual podrá ser consultada en nuestra página web https://gse.com.co/marco-regulatorio/ en la sección Política de Tratamiento de Datos Personales, al igual se puede consultar la autorización para el tratamiento de los datos personales.

9.4.2 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.

9.4.3 Información que no se considera 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.

9.4.4 Responsabilidad de proteger la información privada.

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 recolectados 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

9.4.5 Aviso y consentimiento para utilizar información privada.

Los datos de carácter personal no podrán ser comunicados a terceros, sin la debida notificación y consentimiento de su titular, de conformidad con la normativa aplicable en materia de protección de datos personales.

9.4.6 Divulgación en virtud de un procedimiento judicial o administrativo.

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 normativa de protección de datos personales vigente.

9.4.7 Otras circunstancias de divulgación 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".

- **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:

1. El proveedor de la infraestructura debe contar con las buenas prácticas de las siguientes Normas:
    a. ISO 27001
    b. ISO 9001
2. Pruebas de penetración y escaneo de vulnerabilidades en la red, realizada por una empresa especializada en Ethical Hacking.

9.5 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.

9.6 Representaciones y 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.

9.6.1 Declaraciones y garantías de la CA

Salvo que se indique expresamente en la presente DPC o en un acuerdo independiente con un Suscriptor, GSE no hace ninguna declaración relativa a sus productos o servicios. GSE declara, en la medida especificada en esta DPC, que: GSE cumple, en todos los aspectos materiales, con la PC, la presente DPC y todas las leyes aplicables, GSE publica y actualiza regularmente la CRL y la base de datos para generar respuestas OCSP.

9.6.2 Declaraciones y garantías de la RA

La RA declara que:

1. Los servicios de emisión y gestión de certificados de la RA se ajustan a la PC de GSE y a esta DPC,
2. La información proporcionada por la RA no contiene ninguna información falsa o engañosa,
3. Las traducciones realizadas por la RA son una traducción exacta de la información original, y
4. Todos los certificados solicitados por la RA cumplen con los requisitos de esta DPC.

El acuerdo de GSE con la RA puede contener declaraciones adicionales.

Los Acuerdos del Suscriptor pueden incluir declaraciones y garantías adicionales.

9.6.3 Declaraciones y garantías del suscriptor

Antes de que se le expida y reciba un Certificado, el suscriptor será el único responsable de cualquier declaración falsa que realice a terceros y de todas las transacciones en las que se utilice la llave Privada del Suscriptor, independientemente de que dicho uso haya sido autorizado o no. Los suscriptores están obligados a notificar a GSE si se produce un cambio que pueda afectar al estado del Certificado o la solicitud.

Los suscriptores se comprometen a cumplir los compromisos y garantías de esta DPC y a los siguientes puntos:

1. En caso de generar peticiones en formato PKCS#10, deben generar de forma segura sus llaves Privadas y proteger sus llaves Privadas de cualquier compromiso,

2. Facilitar información precisa y completa cuando se comunique con GSE,

3. Confirmar la exactitud de los datos del certificado antes de utilizarlo,

4. Inmediatamente si aplica:

(i) solicitar la revocación de un Certificado, dejar de utilizarlo y su llave Privada asociada, y notificar a GSE si se produce o se sospecha que se ha producido un uso indebido o se ha puesto en peligro la llave Privada asociada a la clave pública incluida en el certificado, y

(ii) solicitar la revocación del Certificado, y dejar de utilizarlo, si cualquier información en el Certificado es o se convierte en incorrecta o inexacta,

5. Garantizar que las personas que utilicen certificados en nombre de una organización hayan recibido la formación de seguridad adecuada y relativa al Certificado,

6. Utilizar el certificado únicamente para fines autorizados y legales, de conformidad con la finalidad del certificado, la presente DPC, cualquier PC aplicable y el acuerdo de suscriptor correspondiente.

7. Utilizar el certificado únicamente para fines autorizados y legales, de conformidad con la finalidad del certificado, la presente DPC, cualquier PC aplicable y el correspondiente acuerdo de suscriptor, incluida la instalación de certificados únicamente en servidores autorizados con el consentimiento del suscriptor, y

8. Dejar de utilizar inmediatamente el certificado y la llave privada relacionada tras la expiración del certificado.

Los acuerdos de suscripción pueden incluir declaraciones y garantías adicionales.

9.6.4 Declaraciones y garantías de la parte confiante

Cada Parte confiante declara que, antes de confiar en un Certificado emitido por GSE:

1. Obtuvo conocimientos suficientes sobre el uso de Certificados digitales y PKI,

2. Ha estudiado las limitaciones aplicables al uso de Certificados y acepta las limitaciones de responsabilidad de GSE relacionadas con el uso de Certificados,

3. Ha leído, comprende y acepta el Acuerdo de Parte Confiante de GSE y la presente DPC,

4. Ha verificado tanto los certificados de suscriptor emitidos por GSE como los certificados de la cadena de certificación utilizando la CRL u OCSP correspondiente,

5. No utilizará un certificado emitido por GSE si el certificado ha caducado o ha sido revocado, y

6. Adoptará todas las medidas razonables para minimizar el riesgo asociado a la confianza en una firma digital, incluida la confianza únicamente en un certificado emitido por GSE después de considerar:

a) la legislación aplicable y los requisitos legales para la identificación de las partes, la protección de la confidencialidad o privacidad de la información, y la aplicabilidad de la transacción;

b) el uso previsto del Certificado tal y como se enumera en el certificado o en esta DPC,

c) los datos enumerados en el Certificado

d) el valor económico de la transacción o comunicación

e) la pérdida o el daño potencial que causaría una identificación errónea o una pérdida de confidencialidad o privacidad de la información en la solicitud, transacción o comunicación,

f) la trayectoria anterior de la Parte que Confía en el suscriptor,

g) los conocimientos comerciales de la parte que confía, incluida la experiencia con métodos comerciales informáticos, y

h) cualquier otro indicio de fiabilidad o falta de fiabilidad en relación con el suscriptor y/o la aplicación, comunicación o transacción.

Toda confianza no autorizada en un Certificado es por cuenta y riesgo de la parte confiante.

Los Acuerdos de Parte Confiante pueden incluir declaraciones y garantías adicionales.

9.6.5 Declaraciones y garantías de otros participantes

No Aplica

9.7 Renuncias de Garantías.

No Aplica

9.8 Limitaciones de Responsabilidad.

Responsabilidad por la veracidad de la información del Suscriptor.

El Suscriptor asume todos los riesgos por perjuicios que pudieran derivarse de conductas como otorgar información falsa, suplantar la identidad de terceros, validar documentos o información incompleta o desactualizada.

Responsabilidad por disponibilidad del servicio.

El Suscriptor se compromete a obrar diligentemente para reducir al mínimo las posibilidades de fallas o interrupciones que puedan llegar a presentar al interior de su organización. Las fallas ocasionadas por la incapacidad o insuficiencia de los equipos del Suscriptor, o por su falta de conocimientos frente al uso del servicio, no serán en ningún caso imputables a ECD GSE y no se podrá exigir de su parte el saneamiento de ningún perjuicio.

Responsabilidad por la funcionalidad del servicio en la infraestructura del Suscriptor.

El Suscriptor será el único responsable de la provisión y el pago de los costos necesarios para asegurar la compatibilidad del servicio (certificado de firma digital), frente a sus equipos, incluyendo todo el hardware, software, componentes eléctricos y otros componentes físicos o lógicos requeridos para acceder y usar el mismo, incluyendo de forma enunciativa pero no limitativa servicios de telecomunicaciones, acceso y conexión a Internet, enlaces, navegadores, u otros programas, equipos y servicios requeridos para acceder y usar el servicio.

Responsabilidad frente delitos informáticos.

En el evento en que el Suscriptor sea víctima de alguna de las conductas tipificadas como delito, por la Ley 1273 de 2009 (Ley de delitos Informáticos), en sus sistemas de información, en sus aplicaciones e infraestructura tecnológica, en la ejecución de transacciones electrónicas o en el acceso y uso del servicio, ataques de phishing, suplantaciones de identidad, por negligencia en el manejo y confidencialidad del certificado digital, este será el único responsable y saneará los perjuicios a que haya lugar, toda vez que es su obligación adoptar las medidas de seguridad, políticas, campañas culturales, instrumentos legales y demás mecanismos para salvaguardar la confidencialidad y el buen uso de su certificado digital.

Exenciones de responsabilidad de las garantías.

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.

9.9 Indemnizaciones.

No Aplica.

9.10 Duración y Terminación.

9.10.1 Duración.

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.

9.10.2 Terminación.

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.

9.10.3 Efecto de terminación, notificación y comunicación.

ECD GSE notifica los cambios en la presente declaración de prácticas de certificación publicando en la página web la nueva versión una vez sea autorizada por el comité de Gerencia y en la misma se registrará el control de cambios respectivo.

9.10.4 Procedimiento de Cambio en la DPC y PC.

Cambios que afectan la DPC y PC.

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

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

Circunstancias bajo las cuales la OID debe cambiarse.

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

1. La autorización de una nueva jerarquía de certificación, evento en el cual los OID deberán ser definidos de acuerdo con la estructura.
2. 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.

9.11 Notificaciones y comunicaciones individuales a los participantes.

9.11.1 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:

1. Respetar lo dispuesto en la normatividad vigente, en esta DPC y en las Políticas de Certificación PC.
2. Publicar esta DPC y cada una de las Políticas de Certificación en la página Web de GSE.
3. Informar a ONAC sobre las modificaciones de la DPC y de las Políticas de Certificación.
4. Mantener la DPC con su última versión publicada en la página Web de GSE.
5. Proteger y custodiar de manera segura y responsable su llave privada.
6. Emitir certificados conforme a las Políticas de Certificación y a los estándares definidos en la presente DPC.
7. Generar certificados consistentes con la información suministrada por el solicitante o suscriptor.
8. Conservar la información sobre los certificados digitales emitidos de conformidad con la normatividad vigente.
9. Emitir certificados cuyo contenido mínimo esté de conformidad con la normativa vigente para los diferentes tipos de certificados.
10. Publicar el estado de los certificados digitales emitidos en un repositorio de acceso libre.
11. No mantener copia de la llave privada del solicitante o suscriptor.
12. Revocar los certificados digitales según lo dispuesto en la Política de revocación de certificados digitales.
13. Actualizar y publicar la lista de certificados digitales revocados CRL con los últimos certificados revocados.
14. Notificar al Solicitante, Suscriptor o Entidad la revocación del certificado digital dentro de las 24 horas siguientes a la revocación del certificado de conformidad con la política de revocación de certificados digitales.
15. Informar a los suscriptores la proximidad del vencimiento de su certificado digital.
16. Disponer de personal calificado, con el conocimiento y experiencia necesaria para la prestación del servicio de certificación ofrecido por la ECD GSE.
17. Proporcionar al solicitante en la página web de la ECD GSE la siguiente información de manera gratuita y acceso libre cumpliendo con los parámetros y características de la normatividad vigente sin inducir al error:
    - La Declaración de Prácticas de certificación sus Anexos, las Políticas de Certificado y todas las actualizaciones de los documentos mencionados.
    - Obligaciones del suscriptor y la forma en que han de custodiarse los datos.
    - Procedimiento para solicitar la emisión de certificado.
    - El procedimiento de revocación de su certificado.
    - Las condiciones y límites del uso del certificado
18. Comprobar por sí o por medio de una persona diferente que actúe en nombre y por cuenta suya, la identidad y cualesquiera otras circunstancias de los solicitantes o de datos de los certificados, que sean relevantes para los fines propios del procedimiento de verificación previo a su expedición.
19. Informar al ONAC, de manera inmediata, la ocurrencia de cualquier evento que comprometa o pueda comprometer la prestación del servicio.
20. Informar oportunamente la modificación o actualización de servicios incluidos en el alcance de la acreditación, en los términos que establezcan los procedimientos, reglas y requisitos del servicio de acreditación de ONAC
21. Actualizar la información de contacto cada vez que haya cambio o modificación en los datos suministrados.
22. Capacitar y advertir a sus usuarios sobre las medidas de seguridad que deben observar y sobre la logística que se requiere para la utilización de los mecanismos de la prestación del servicio.
23. Garantizar la protección, integridad, confidencialidad y seguridad de la información suministrada por el suscriptor conservando la documentación que respalda los certificados emitidos.
24. Garantizar las condiciones de integridad, disponibilidad, confidencialidad y seguridad, de acuerdo con los estándares técnicos nacionales e internacionales vigentes y con los criterios específicos de acreditación que para el efecto establezca el ONAC.

25. Disponer en la página web de la ECD GSE los servicios que se encuentran acreditados.

9.11.2 Obligaciones de la RA.

La RA de la ECD GSE 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:

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

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

El Suscriptor 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:

1. Usar su certificado digital o certificado de firma electrónica según los términos de esta DPC.
2. Verificar dentro del día siguiente hábil que la información del certificado digital es correcta. En caso de encontrar inconsistencias, notificar a la ECD.
3. Abstenerse de: prestar, ceder, escribir, publicar la contraseña de uso de su certificado digital y tomar todas las medidas necesarias, razonables y oportunas para evitar que este sea utilizado por terceras personas.
4. No transferir, compartir ni prestar el dispositivo criptográfico a terceras personas.
5. Suministrar toda la información requerida en el formulario de solicitud o utilizando los canales, medios o mecanismos dispuestos por GSE para la solicitud de certificados digitales para facilitar su oportuna y plena identificación.
6. Solicitar la revocación del certificado digital ante el cambio de nombre y/o apellidos.
7. Solicitar la revocación del certificado digital cuando el Suscriptor haya variado su nacionalidad.
8. Cumplir con lo aceptado y/o firmado en el documento términos y condiciones.
9. Proporcionar con exactitud y veracidad la información requerida.
10. Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del certificado.
11. Custodiar y proteger de manera responsable su llave privada.
12. Dar uso al certificado de conformidad con las PC establecidos en la presente DPC para cada uno de los tipos de certificado.
13. 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.
14. No hacer uso de la llave privada ni del certificado digital una vez cumplida su vigencia o se encuentre revocado.
15. Informar a los terceros de confianza de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado.
16. Informar al tercero de buena fe el estado de un certificado digital revocado para lo cual se dispone de la lista de certificados revocados CRL, publicada de manera periódica por ECD GSE.
17. No utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para la ECD.

18. No realizar ninguna declaración relacionada con su certificación digital en la ECD GSE que pueda considerar engañosa o no autorizada, conforme a lo dispuesto por esta DPC y PC.
19. Una vez caducado o revocado el servicio de certificación digital el suscriptor debe inmediatamente dejar de utilizarla en todo el material publicitario que contenga alguna referencia al servicio.
20. El suscriptor al hacer referencia al servicio de certificación digital prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, debe informar que cumple con los requisitos especificados en las PC de esta DPC, indicando la versión.
21. El suscriptor podrá utilizar las marcas de conformidad y la información relacionada con el servicio de certificación digital prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, desde que cumpla lo requerido en el literal anterior.

Por otro lado, tiene los siguientes derechos:

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

9.11.4 Obligaciones de los Terceros de buena fe.

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

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

9.11.5 Obligaciones de la Entidad (Cliente).

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:

1. Solicitar a la RA de la ECD GSE la suspensión/revocación del certificado digital cuando cese o se modifique dicha vinculación.
2. Todas aquellas obligaciones vinculadas al responsable del servicio de certificación digital.
3. La entidad al hacer referencia al servicio de certificación digital prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, debe informar que cumple con los requisitos especificados en la DPC.

9.11.6 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:

1. Revisar la consistencia de la DPC con la normatividad vigente.
2. Aprobar y decidir los cambios a realizar sobre los servicios de certificación, por decisiones de tipo normativo o por solicitudes de suscriptores o responsables.
3. Aprobar la notificación de cualquier cambio a los suscriptores y/o responsables analizando su impacto legal, técnico o comercial.
4. Revisar y tomar acciones sobre cualquier comentario realizado por suscriptores o responsables cuando un cambio en el servicio de certificación se realice.
5. 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 vigente.
6. Autorizar los cambios o modificaciones requeridas sobre la DPC.
7. Autorizar la publicación de la DPC en la página Web de la ECD GSE.

8. Aprobar los cambios o modificaciones a las Políticas de Seguridad de la ECD GSE.
9. Asegurar la integridad y disponibilidad de la información publicada en la página Web de la ECD GSE.
10. Asegurar la existencia de controles sobre la infraestructura tecnológica de la ECD GSE.
11. Solicitar la revocación de un certificado digital si tuviera el conocimiento o sospecha del compromiso de la llave privada del suscriptor, entidad o cualquier otro hecho que tienda al uso indebido de llave privada del suscriptor, entidad o de la propia ECD.
12. Conocer y tomar acciones pertinentes cuando se presenten incidentes de seguridad.
13. Realizar con una frecuencia máxima anual, una revisión de la DPC para verificar que las longitudes de las llaves y periodos de los certificados que se estén empleando son adecuados.
14. Revisar, aprobar y autorizar cambios sobre los servicios de certificación acreditados por el organismo competente.
15. Revisar, aprobar y autorizar la propiedad y el uso de símbolos, certificados y cualquier otro mecanismo que requiera ECD GSE para indicar que el servicio de certificación digital está acreditado.
16. Velar por que las condiciones de acreditación otorgadas por el organismo competente se mantengan.
17. Velar por el uso adecuado en documentos o en cualquier otra publicidad que los símbolos, los certificados, y cualquier otro mecanismo que indique que ECD GSE cuenta con un servicio de certificación acreditado y cumple con lo dispuesto en las Reglas de Acreditación de ONAC.
18. Velar por mantener informados a sus proveedores críticos y ECD recíproca, en caso de existir, de la obligación de cumplimiento de los requisitos del CEA, en los numerales que correspondan.
19. El 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 como buena práctica para la identificación de riesgos que comprometa la imparcialidad y no discriminación de la ECD, entregando al Comité de Gerencia el mecanismo que elimina o minimiza tal riesgo, de manera continua.
20. Velar que todo el personal y los comités de la ECD (sean internos o externos), que puedan tener influencia en las actividades de certificación actúen con imparcialidad y no discriminación, especialmente aquellas que surjan por presiones comerciales, financieras u otras que comprometan su imparcialidad.
21. Documentar y demostrar el compromiso de imparcialidad y no discriminación.
22. Velar que el personal administrativo, de gestión, técnico de la PKI, de la ECD asociado a las actividades de consultoría, mantenga completa independencia y autonomía respecto al personal del proceso de revisión y toma de decisión sobre la certificación de esta ECD.
23. Velar por mantener informados a sus proveedores críticos como la ECD recíproca y datacenter que cumplen con los requisitos de acreditación para ECD como soporte para su contratación y del cumplimiento de los requisitos solicitados tanto administrativos como técnicos.

9.12 Enmiendas.

Los certificados digitales emitidos por ECD GSE no pueden 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.

9.12.1 Procedimiento para enmienda.

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

9.12.2 Mecanismo y plazo de notificación.

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

9.12.3 Circunstancias en las que debe modificarse un OID.

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

9.12.4 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.

9.12.5 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.

9.12.6 Publicación del certificado modificado por la ECD.

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

9.12.7 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.

9.13 Disposiciones sobre resolución de disputas.

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

1. La prestación de los servicios de certificación digital descritos en esta DPC.
2. Durante la ejecución de los servicios contratados.
3. 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 quedarán 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.

De acuerdo con lo enunciado en el Anexo 2 - Términos y Condiciones de la DPC.

9.14 Legislación aplicable.

El funcionamiento y las operaciones realizadas por la ECD GSE, así como la presente Declaración de Prácticas de Certificación y las Políticas de Certificación aplicables a cada tipo de certificado están sujetas a la normativa que les sea aplicable y en especial a:

1. Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
2. Decreto 333 de 2014, por el cual se reglamenta el artículo 160 del Decreto-ley 019 de 2012 respecto a las características y requerimientos de las entidades de certificación, y lo relacionado con los certificados digitales.
3. 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.

9.15 Cumplimiento de la legislación aplicable.

La ECD GSE manifiesta el cumplimiento de la ley 527 de 1999 y de sus decretos asociados, adicionalmente que la Declaración de Prácticas de Certificación sea satisfactoria de acuerdo con los requisitos establecidos por el Organismo Nacional de Acreditación de Colombia.

9.16 Disposiciones varias.

9.16.1 Acuerdo completo

La ECD GSE obliga contractualmente a cada RA a cumplir con esta DPC y las directrices aplicables del sector. Asimismo, la ECD GSE exige que cada parte que utilice sus productos y servicios celebre un acuerdo en el que se definan las condiciones asociadas al producto o servicio. Si un acuerdo contiene disposiciones que difieren de la presente DPC, prevalecerá la presente DPC. Los terceros no podrán basarse en dicho acuerdo ni emprender acciones para exigir su cumplimiento, si dicho acuerdo es contrario a la presente DPC.

9.16.2 Cesión

Las entidades que operen en virtud de esta DPC no podrán ceder sus derechos u obligaciones sin el consentimiento previo por escrito de la ECD GSE.

9.16.3 Divisibilidad

Si alguna disposición de la presente DPC es declarada inválida o inaplicable por un juzgado o tribunal competente, el resto de la DPC seguirá siendo válida y aplicable.

9.16.4 Ejecución (honorarios de abogados y renuncia de derechos)

La ECD GSE puede solicitar indemnización y honorarios de abogados a cualquiera de las partes por daños, pérdidas y gastos relacionados con la conducta de dicha parte.

El hecho de que la ECD GSE no haga cumplir una disposición de esta DPC no implica que renuncie a su derecho de hacer cumplir la misma disposición más adelante o a su derecho de hacer cumplir cualquier otra disposición de esta DPC.

Para ser efectivas, las renuncias deberán constar por escrito y estar firmadas por la ECD GSE.

9.16.5 Fuerza mayor

La ECD GSE no será responsable de ningún retraso o incumplimiento de una obligación en virtud de la presente DPC en la medida en que el retraso o incumplimiento se deba a un hecho ajeno al control razonable de la ECD GSE.

El funcionamiento de Internet escapa al control razonable de la ECD GSE.

En la medida en que lo permita la legislación aplicable, los Contratos de Suscriptor y los Contratos de Parte Confiante incluirán una cláusula de fuerza mayor que proteja a la ECD GSE.

9.17 Otras Disposiciones.

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:

1. Por cambios normativos en la legislación para ECD.
2. Por solicitud del ONAC.
3. Por solicitud de la Superintendencia de Industria y Comercio de Colombia - SIC.
4. Cambios tecnológicos que afecten los servicios de certificación digital.
5. Por solicitud de suscriptores o responsables, previa aprobación del comité de Gerencia.

Para lo cual el Suscriptor o responsable deberá enviar comunicación dirigida al comité de Gerencia de la ECD GSE sobre el cambio solicitado, la aceptación o rechazo estará bajo la discreción del Comité de Gerencia.

Procedimiento para los Cambios.

Cambios que no requieren notificación.

1. 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.
2. Cuando los cambios impliquen correcciones tipográficas o de edición en el contenido de los servicios prestados.

Cambios que requieren notificación

1. 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.
2. Cuando los cambios impliquen actualización de datos de contacto con la ECD GSE.

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:

1. 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.

2. 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 y/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 al 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.

DESCRIPCIÓN DE PRODUCTOS Y SERVICIOS

TIPO DE CERTIFICADO DIGITAL	OBJETO
Pertenencia a Empresa	Garantiza la identidad de la persona natural titular del certificado, así como su vinculación a una determinada entidad jurídica en virtud del cargo que ocupa en la misma. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual.
Representación Empresa	Es emitido a favor de una persona natural representante de una determinada entidad jurídica. El titular del certificado se identifica no únicamente como persona física perteneciente a una empresa, sino que añade su cualificación como representante legal de la misma.
Función Pública	Garantiza la identidad de la persona natural titular del certificado, así como su vinculación a una Administración Pública en virtud del rango como funcionario público. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual.
Profesional Titulado	Garantiza la identidad de la persona natural titular del certificado, así como su condición de profesional titulado. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual en el ámbito de su profesión.
Persona Natural	Garantiza únicamente la identidad de la Persona natural.
Factura Electrónica 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 facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad.
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 facturación gratuita de la DIAN y la plataforma RADIAN, en cumplimiento de los anexos técnicos emitidos por dicha entidad.
Persona Jurídica	Realización de trámites empresariales por parte de una aplicación ejecutándose en una máquina en procesos de firma automáticos y desatendidos en nombre de una persona Jurídica de derecho público o privado que requieran garantizar la autenticidad y la integridad de los datos enviados o almacenados digitalmente 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.
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 esté firmada digitalmente.

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

TARIFAS.

Tarifas de emisión o renovación de certificados.

Detalle del producto	Tiempo de entrega	Vigencia	Precio sin IVA	IVA	Total
Certificado Persona Natural	Normal	1	$ 231.092	$ 43.908	$ 275.000
Certificado Persona Natural	Normal	2	$ 376.471	$ 71.529	$ 448.000
Certificado Perteneciente a empresa	Normal	1	$ 231.092	$ 43.908	$ 275.000
Certificado Perteneciente a empresa	Normal	2	$ 376.471	$ 71.529	$ 448.000
Certificado Profesional Titulado	Normal	1	$ 231.092	$ 43.908	$ 275.000
Certificado Profesional Titulado	Normal	2	$ 376.471	$ 71.529	$ 448.000
Certificado Representante Empresa	Normal	1	$ 231.092	$ 43.908	$ 275.000
Certificado Representante Empresa	Normal	2	$ 376.471	$ 71.529	$ 448.000
Certificado Función Pública	Normal	1	$ 231.092	$ 43.908	$ 275.000
Certificado Función Pública	Normal	2	$ 376.471	$ 71.529	$ 448.000
Certificado Persona Jurídica	Normal	1	$ 720.168	$ 136.832	$ 857.000
Certificado Persona Jurídica	Normal	2	$ 1.343.697	$ 255.303	$ 1.599.000
Facturación Electrónica	Normal	1	$ 279.832	53.168	$ 333.000
Facturación Electrónica	Normal	2	$ 376.471	$ 71.529	$ 448.000

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.

- La ECD GSE pone a disposición la emisión de certificados digitales con vigencia en días o meses sin superar los 24 meses, los precios de venta de estos certificados serán acordados con el cliente previa negociación.
- Para la emisión de certificados digitales con algoritmo de curva elíptica aplicarán los mismos precios definidos en la tabla de tarifas.
- Las tarifas anteriormente mencionadas corresponden a precios base o de referencia y podrán ajustarse de acuerdo con las condiciones y los acuerdos comerciales establecidos con cada cliente.

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.

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.

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.

Política de devoluciones.

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

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, financieras u otras comprometan su imparcialidad.
- GSE puede declinar la aceptación de una solicitud o el mantenimiento de un contrato para la certificación cuando existen razones fundamentadas y demostradas, por ejemplo, la participación del solicitante y/o suscriptor en actividades ilegales, o temas similares relacionados con el suscriptor.
- 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.

POLÍTICAS DE CERTIFICACIÓN.

La interrelación entre esta DPC y las 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 la 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 la 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	1.3.6.1.4.1.31136.1.4.19
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_certificado_para_certificados_digitales_V19.pdf

- Políticas de Certificado para Servicio de Estampado Cronológico:

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.2.16
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_Certificado_para_Servicio_de_Estampado_Cronologico_V16.pdf

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

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.3.15
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_Certificado_para_Servicio_de_Archivo_Confiable_de_Datos_V15.pdf

- Políticas de Certificado para Servicio de Correo Electrónico Certificado:

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.5.16
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politica_Certificado_para_Servicio_de_Correo_Electronico_Certificado_V16.pdf

- Políticas de Generación de Firmas Electrónicas Certificadas:

OID (Object Identifier) – IANA	1.3.6.1.4.1.31136.1.6.7
Ubicación de la PC	https://gse.com.co/documentos/calidad/politicas/Politica_de_Generacion_de_Firmas_Electronicas_Certificadas_V7.pdf

ANEXO 1 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS DIGITALES.

ANEXO 2 DPC MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES.

ANEXO 3 DPC MATRIZ PERFIL TÉCNICO CERTIFICADOS FIRMA ELECTRÓNICA.