



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia 27/11/2018

Versión 4

Documento	Políticas de Certificado para Servicios de Generación de Firmas Digitales
Versión	4
Grupo de Trabajo	Comité de Gerencia
Estado del documento	Final
Fecha de emisión	01-11-2016
Fecha de inicio de vigencia	27/11/2018
OID (Object Identifier)	1.3.6.1.4.1.31136.3.2
Ubicación de la Política	http://cps.gse.co
Elaboró	Gerente de Operaciones ECD
Revisó	Area de Calidad
Aprobó	Comité de Gerencia



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

CONTROL DE MODIFICACIONES

Versión	Fecha	Cambio/Modificación
1	01-11-2016	Documento inicial conforme al desarrollo del plan de acción de la auditoría de ONAC.
2	05-10-2017	Actualización de información referente a la sede de ECD GSE
3	03-04-2018	Actualización conforme a recomendaciones de la auditoría de ONAC.
4	27/11/2018	Se cambió de V3 a V4 26/11/2018 Actualización cargos, tarifas, rutas de acceso a la página web, cambio de título, inclusión de los límites de responsabilidad de la entidad de certificación abierta, vigencia de los servicios, Obligaciones de la ECD, de la RA, de la EE, del suscriptor, de los responsables, de los terceros de buena fe, de la entidad y obligaciones de otros participantes, además se actualizó la minuta de términos y condiciones y/o responsables y se listaron los documentos que se deben anexar para la solicitud del servicio.



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia 27/11/2018

Versión 4

1	INTRODUCCIÓN	5
1.1	Resumen	5
	DATOS DE LA ENTIDAD PRESTADORA DE SERVICIOS DE CERTIFICACIÓN DIGITAL:	5
	DATOS DE LA ENTIDAD PROVEEDORA DE SERVICIOS DE CERTIFICACIÓN DIGITAL (ENTIDAD SUBCONTRATADA):	5
	Página Web:	5
	Nombre: GESTIÓN DE SEGURIDAD ELECTRONICA S.A. – GSE S.A.	6
1.2	Definiciones y acrónimos	7
1.2.1	Definiciones	7
1.2.2	Acrónimos	10
2	REQUISITOS OPERACIONALES PARA EL SERVICIOS DE GENERACION DE FIRMAS DIGITALES	11
2.1	Servicios de Generación de Firmas Digitales	11
2.2	Funcionalidades del Servicios de Generación de Firmas Digitales	11
2.3	Tipos de firma y longevidad de la misma	12
2.4	Solicitud del servicio	12
2.4.1	Quién puede solicitar el servicio	13
2.4.2	Proceso de registro y responsabilidades	13
2.5	Tramitación de solicitud del servicio	13
2.5.1	Realización de las funciones de identificación y autenticación	13
2.5.2	Aprobación o rechazo de las solicitudes del servicio	13
2.5.3	Plazo para procesar las solicitudes del servicio	14
2.6	Activación del servicio	14
2.6.1	Actuaciones de la AC GSE durante la activación del servicio.	14
2.6.2	Notificación al solicitante por la AC ECD de la activación del servicio	14
2.7	Aceptación del servicio	14
2.7.1	Forma en la que se acepta el servicio	14
2.8	Uso del Servicios de Generación de Firmas Digitales	14
2.8.1	Uso del servicio por parte del responsable	14
2.9	Renovación del servicio sin cambio de credenciales	15
2.9.1	Circunstancias para la renovación del servicio sin cambio de credenciales.	15
2.9.2	Quién puede solicitar una renovación sin cambio de credenciales.	15
2.9.3	Trámites para la solicitud de renovación de certificados sin cambio de credenciales.	15
2.9.4	Notificación al titular de la renovación del servicio sin cambio de credenciales.	15
2.9.5	Forma en la que se acepta la renovación del servicio.	15
2.9.6	Notificación de la renovación por la ECD AC a otras entidades.	15
2.10	Renovación del servicio con cambio de llaves	15
2.10.1	Circunstancias para la renovación del servicio con cambio de credenciales.	17
2.10.2	Quién puede solicitar una renovación con cambio de llaves.	17
2.10.3	Trámites para la solicitud de renovación del servicio con cambio de llaves.	17
2.10.4	Notificación al responsable de la activación del servicio con cambio de llaves	17
2.10.5	Forma en la que se acepta la renovación del servicio.	17
2.10.6	Notificación de la renovación por la GSE a otras entidades	17
2.11	Modificación del servicio	17
2.12	Cancelación y suspensión del servicio	18



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia 27/11/2018

Versión 4

2.12.1	Circunstancias para la cancelación del servicio	18
2.12.2	Quién puede solicitar una cancelación	19
2.12.3	Procedimiento de solicitud de cancelación	21
2.12.4	Periodo de gracia de solicitud de cancelación	21
2.12.5	Plazo en el que la ECD debe resolver la solicitud de cancelación.....	21
2.12.6	Requisitos de verificación de las cancelaciones por los terceros de buena fe	22
2.12.7	Notificación de la cancelación del servicio	22
2.12.8	Requisitos especiales de cancelación de credenciales comprometidas.....	23
2.12.9	Circunstancias para la suspensión	23
2.12.9.1	Quién puede solicitar la suspensión	23
2.12.9.2	Procedimiento de solicitud de suspensión	23
2.12.9.3	Límites del periodo de suspensión.....	23
3	OTROS ASUNTOS LEGALES Y COMERCIALES	24
3.1	Tarifas	24
3.1.1	Tarifas de emisión o renovación del servicio	24
3.1.2	Tarifas de revocación o acceso a la información de estado.....	24
3.1.3	Tarifas de otros servicios	25
3.1.4	Política de reembolso	25
4	POLÍTICAS DEL SERVICIO DE GENERACION DE FIRMAS DIGITALES	30



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia
27/11/2018

Versión
4

1 INTRODUCCIÓN

1.1 Resumen

Política de Servicios de Generación de Firmas Digitales Versión 1.0, en adelante **Política** es un documento elaborado por la Sociedad **Gestión de Seguridad Electrónica S.A. (en adelante GSE)** que, actuando como una Entidad de Certificación Digital, con certificado raíz valido desde el martes, 19 de enero de 2016 2:00:00 a. m. y hasta el jueves, 11 de enero de 2046 2:00:00 a.m. huella digital en SHA1 ecb1fc5784ee972751c15a7ab2eea15285273162, contiene las normas, procedimientos que la **Entidad de Certificación Digital (en adelante GSE)** como **Prestador de Servicios de Certificación digital (PSC)** aplica como lineamiento para prestar el servicio de generación de firmas digitales de acuerdo a lo establecido en la Ley 527 de 1999, el Decreto Ley 0019 de 2012, el Decreto 333 de 2014, el Decreto 1471 de 2014 y los reglamentos que los modifiquen o complementen, en el territorio de Colombia.

La Política está conforme con los siguientes lineamientos:

- i. Criterios Específicos de Acreditación para las Entidades de Certificación Digital CEA-4.1-10 Versión 01 (**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;

La actualización y/o modificación de la Política, se realizará a través del procedimiento establecido por GSE para los servicios de certificación digital a cargo del comité de seguridad, cualquier cambio o adecuación sobre el documento deberá ser revisado, analizado y aprobado por los integrantes del Comité de Seguridad, quienes velaran por la publicación de la nueva versión en el sitio Web de GSE, ajustada al contexto de GSE.

DATOS DE LA ENTIDAD PRESTADORA DE SERVICIOS DE CERTIFICACIÓN DIGITAL:

Número Identificación

Nombre: GESTION DE SEGURIDAD ELECTRONICA S.A. – GSE S.A.

Numero de Identificación Tributaria: 900.204.272 - 8

Registro Mercantil No: 01779392

Dirección: Carrera 82 No. 46 A 93 Local 1 Piso 1

Ciudad / País: Bogotá D.C., Colombia.

Teléfono: +57 (1) 5185158

Correo electrónico: info@gse.com.co

Página Web: www.gse.co

DATOS DE LA ENTIDAD PROVEEDORA DE SERVICIOS DE CERTIFICACIÓN DIGITAL (ENTIDAD SUBCONTRATADA):

Nombre: InDenova.

Dirección: Dels Traginers 14 2º B, Pol. Ind. Vara de Quart 46014

Domicilio: Valencia, España.

Teléfono: +34 (96) 381 99 47

Correo electrónico: info@indenova.com

Página Web:

DATOS DE LAS ENTIDADES DE REGISTRO

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

AC GSE tiene una Entidad de registro:

Nombre: GESTION DE SEGURIDAD ELECTRONICA S.A. – GSE S.A.

Dirección: Carrera 82 No. 46 A 93 Local 1 Piso 1

Domicilio: Bogotá D.C., Colombia.

Teléfono: +57 (1) 5185158

Correo electrónico: info@gse.com.co

Página Web: www.gse.co

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

1.2 Definiciones y acrónimos

1.2.1 Definiciones

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

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

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

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

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.

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

La 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.

Autoridades Intermedias: Son PSC Subordinados que bajo la jerarquía de un certificado raíz emiten certificados digitales a usuarios finales.

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.

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

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.

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



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

del momento que se realizó el estampado.

Autoridad de Estampado de Tiempo (TSA). Sigla en inglés de “Time Stamping Authority”: Entidad de certificación prestadora de servicios de archivo, registro, conservación custodia y anotación para los documentos electrónicos transferibles y mensajes de datos.

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

Suscriptor: persona natural o jurídica a la que se emite un certificado digital.

Tercero de buena fe: persona o entidad diferente del titular que decide aceptar y confiar en un certificado digital emitido por AC GSE.



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

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.

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 titular del certificado.

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

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

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

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

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

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

Módulo Criptográfico Hardware de Seguridad: módulo hardware utilizado para realizar funciones criptográficas y almacenar llaves en modo seguro.

PKCS#12: Estándar de sintaxis de intercambio de información personal. Define un formato de archivo usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica admitido.

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.

AC GSE: Es la Autoridad de Certificación de GSE, ente prestador de Servicios de Certificación digital.

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

AR GSEAR: Es la Autoridad de Registro de GSE, ente prestador del servicio de registro de la Autoridad de Certificación AC GSE en el proceso de solicitud e identificación de los solicitantes de un certificado digital.

AC TSA GSE: Corresponde al término utilizado por la Autoridad de Certificación AC GSE, en la prestación de su Servicios de Generación de Firmas Digitales, como Autoridad de Estampado Cronológico.

1.2.2 Acrónimos

- CA:** Certification Authority
- CPS:** Certification Practice Statement
- CRL:** Certificate Revocation List
- CSP:** Certification Service Provider



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

DNS: Domain Name System

FIPS: Federal Information Processing Standard

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

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

IEC: International Electrotechnical Commission

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

IP: Internet Protocol

ISO: International Organization for Standardization

OCSP: Online Certificate Status Protocol.

OID: Object identifier (Identificador de objeto único)

PIN: Personal Identification Number

PUK: Personal Unlocking Key

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

PKI: Public Key Infrastructure (Infraestructura de Llave Pública)

PKIX: Public Key Infrastructure (X.509)

RA: Registration Authority

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

URL: Uniform Resource Locator

2 REQUISITOS OPERACIONALES PARA EL SERVICIOS DE GENERACION DE FIRMAS DIGITALES

2.1 Servicios de Generación de Firmas Digitales

Consiste en una plataforma de firma electrónica y digital, accesible mediante certificado digital o usuario y contraseña, que permite a sus Usuarios la firma electrónica y digital de un documento y su envío a un tercero usuario o no del servicio, el intercambio confidencial de documentos y archivos entre los mismos, la creación de circuitos de firma electrónica/digital de documentos y archivos, y su almacenamiento y gestión, ofreciéndose igualmente el servicio de timestamping o “sellado de tiempo”, que acredita la fecha y hora oficial del documento electrónico.

Por su funcionalidad y características técnicas, la solución se ajusta a la normativa internacional de firma electrónica/digital, lo que garantiza la plena validez jurídica de los documentos firmados por este procedimiento, su “integridad” y el “no repudio” por parte de los firmantes.

La robustez de la tecnología del servicio se basa en la utilización de sistemas de criptografía de clave asimétrica y certificados digitales

2.2 Funcionalidades del Servicios de Generación de Firmas Digitales

Este servicio permite a los usuarios realizar, las siguientes acciones:

- Firmar electrónicamente/digitalmente documentos o archivos y enviarlos a la dirección de correo electrónico de terceros.
- Iniciar circuitos de firma electrónica/digital de documentos, asociando al mismo, como firmantes, a



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

- otros usuarios de la aplicación o a terceros no usuarios.
- Descarga y visualización de los documentos o archivos asociados a una tarea de firma, tanto los originales como copias firmadas, si las hubiera.
- Creación y gestión de contactos entre los usuarios de la aplicación o terceros ajenos a la misma.
- Control estadístico de uso.

2.3 Tipos de firma y longevidad de la misma

El servicio integra los estándares internacionales relacionados con los conceptos de generación y validación de firma electrónica/digital, ofreciendo, como mínimo, los formatos de firma siguientes:

- **Formato XAdES**, XML Advanced Electronic Signatures, según especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2.

El archivo de firma es un XML que facilita que los documentos puedan tener cualquier formato. La modalidad de firma corresponde a la que genera un único fichero que contiene el documento original, codificado en base64, y las firmas, encontrándose al mismo nivel XML lo firmado y la firma.

- **Formato PAdES**, PDF Advanced Electronic Signatures, según especificación técnica ETSI TS 102 778-3, versión 1.1.2. En este formato la firma está incluida en el estándar ISO PDF y sólo se pueden firmar documentos PDF.

En ambos formatos el Servicio incorpora a las firmas electrónicas/digitales información adicional para garantizar la validez de una firma a largo plazo o su conservación en el tiempo una vez que haya vencido el periodo de validez del certificado digital, permitiendo elegir al Usuario indistintamente entre los formatos de firma longeva:

- **XAdES-XL**, incorpora a la firma los datos de revocación de los certificados digitales para permitir la verificación en el futuro, incluso si las fuentes originales no estuvieran ya disponibles y la firma.
- **PAdES-LTV**, permite prorrogar por tiempo indefinido la validez de las firmas en formato PDF.

Asimismo, ambos formatos incluyen sellado de tiempo o timestamping, consistente en la asignación por medios electrónicos de una fecha y una hora oficial a un documento electrónico, que asegure la exactitud e integridad de la marca de tiempo.

2.4 Solicitud del servicio

Cualquier persona que requiera la prestación del Servicios de Generación de Firmas Digitales, debe realizar el procedimiento indicado en el portal de GSE adjuntando la documentación requerida para autenticar la información suministrada. Una vez completada y confirmada la información por parte del responsable, GSE validará la información suministrada de conformidad con el cumplimiento de los requisitos exigidos para el servicio.

Los usuarios que solicitan nuestros productos y servicios, aceptan los términos de uso y condiciones del servicio especificadas en la presente Política.

El solicitante debe aportar los documentos necesarios y GSE surte los procedimientos establecidos para la obtención del Servicios de Generación de Firmas Digitales.

GSE S.A., se reserva el derecho de solicitar documentos adicionales, 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 GSE S.A. a través de otros medios.



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

El solicitante acepta que GSE S.A. tiene el derecho discrecional de rechazar una solicitud del Servicios de Generación de Firmas Digitales cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial, buen nombre de GSES.A. o idoneidad legal o moral de todo el sistema de certificación, notificando la no aprobación sin necesidad de indicar las causas.

Los documentos que se deben anexar para la solicitud del servicio son:

- Formulario diligenciado de solicitud del certificado
- Términos y condiciones.
- Fotocopia de documento de identidad del Suscriptor.
- Documento de Existencia y Representación Legal de la Empresa. Vigente.
- Registro Único Tributario – RUT.

2.4.1 Quién puede solicitar el servicio

Toda persona natural o jurídica legalmente facultada y debidamente identificada puede tramitar la solicitud del Servicios de Generación de Firmas Digitales.

2.4.2 Proceso de registro y responsabilidades

La AR GSE previamente cumplidos los requisitos de autenticación y verificación de los datos del solicitante, aprobará y firmará digitalmente la solicitud de activación del servicio. Toda la información relacionada quedará registrada en el sistema de la AR GSE.

2.5 Tramitación de solicitud del servicio

2.5.1 Realización de las funciones de identificación y autenticación

Las funciones de autenticación y verificación de la identidad del solicitante son realizadas por la AR GSE, encargada de autorizar la activación del servicio, quien comprueba si la información suministrada es auténtica y si la documentación anexa cumple con los requisitos definidos para el servicio de acuerdo con esta Política.

2.5.2 Aprobación o rechazo de las solicitudes del servicio

Si una vez verificada la identidad del solicitante, la información suministrada cumple con los requisitos establecidos por esta Política, 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 activa el Servicios de Generación de Firmas Digitales. La Autoridad de Certificación AC GSE no asume ninguna responsabilidad por las consecuencias que puedan derivarse de la no aprobación del Servicios de Generación de Firmas Digitales y así lo acepta y reconoce el solicitante al que le haya sido negada la expedición del respectivo servicio.

Igualmente, la AC GSE se reserva el derecho de no activar el Servicios de Generación de Firmas Digitales a pesar que la identificación del solicitante o la información suministrada por este haya sido plenamente autenticada, cuando la activación del Servicios de Generación de Firmas Digitales en particular por razones de orden legal o de conveniencia comercial, buen nombre o reputación de AC GSE pueda poner en peligro



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

el sistema de certificación digital.

2.5.3 Plazo para procesar las solicitudes del servicio

El plazo para la aprobación de una solicitud por parte de la AR GSE, es de tres (3) días hábiles desde el momento de recibir la documentación e información completa. El tiempo para la activación del servicio es de cinco (5) días hábiles una vez recibida la documentación completa.

2.6 Activación del servicio

2.6.1 Actuaciones de la AC GSE durante la activación del servicio.

El paso final del proceso de activación del Servicios de Generación de Firmas Digitales es la entrega de las credenciales de acceso por parte de la AC GSE y su entrega de manera segura al responsable.

El proceso de activación del Servicios de Generación de Firmas Digitales vincula de una manera segura la información de registro y las credenciales entregadas.

2.6.2 Notificación al solicitante por la AC ECD de la activación del servicio

Mediante correo electrónico se informa al responsable la activación del Servicios de Generación de Firmas Digitales y por consiguiente el solicitante acepta y reconoce que una vez reciba el citado correo electrónico, se entenderá entregado el Servicios de Generación de Firmas Digitales. Se entenderá que se ha recibido el correo electrónico donde se notifica la activación, cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección de correo electrónico que consta en el formulario de solicitud.

2.7 Aceptación del servicio

2.7.1 Forma en la que se acepta el servicio

No se requiere confirmación de parte del responsable como aceptación del servicio recibido. Se considera que el Servicios de Generación de Firmas Digitales es aceptado por el responsable desde el momento que solicita su expedición, por ello, si la información contenida en la comunicación de activación del servicio no corresponde al estado actual de la misma o no fue suministrada correctamente, se debe solicitar su cancelación por parte del responsable y éste así lo acepta, según procedimiento descrito en el apartado Procedimiento de solicitud de cancelación.

2.8 Uso del Servicios de Generación de Firmas Digitales.

2.8.1 Uso del servicio por parte del responsable

El responsable del servicio emitido por AC GSE acepta las condiciones de uso establecidas en esta Política por el solo hecho de haber solicitado la activación del servicio y solo podrá emplearlos para los usos explícitamente mencionados y autorizados en la presente Política. Por consiguiente, los servicios de archivo, registro, conservación custodia y anotación para los documentos electrónicos transferibles y mensajes de datos, no deberán ser usado en otras actividades que estén por fuera de los usos mencionados. Una vez pérdida la vigencia el servicio, el responsable está obligado a no seguir usando las credenciales asociadas al mismo. Con base en lo anterior, desde ya acepta y reconoce el responsable, que en tal sentido será el único responsable por cualquier perjuicio pérdida o daño que cause a terceros por el uso del servicio una vez

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

expirada la vigencia. AC GSE no asume ningún tipo de responsabilidad por los usos no autorizados.

2.9 Renovación del servicio sin cambio de credenciales

Para la Autoridad de Certificación AC GSE, un requerimiento de renovación del servicio sin cambio de credenciales es un requerimiento normal y por consiguiente implica solo procesar nuevamente la solicitud con la información que cambio, el suscriptor lo reconoce y acepta.

2.9.1 Circunstancias para la renovación del servicio sin cambio de credenciales.

El servicio puede ser renovado a solicitud del responsable por próxima pérdida de vigencia de conformidad con las causales mencionadas en esta Política o cuando así lo requiera el responsable.

2.9.2 Quién puede solicitar una renovación sin cambio de credenciales.

Para el Servicios de Generación de Firmas Digitales el responsable puede solicitar la renovación sin cambio de credenciales.

2.9.3 Trámites para la solicitud de renovación de certificados sin cambio de credenciales.

El procedimiento para renovación del Servicios de Generación de Firmas Digitales sin cambio de credenciales es igual al procedimiento de solicitud del servicio. El responsable tiene que ingresar al portal Web e iniciar el proceso de solicitud de renovación del servicio de la misma forma que lo hizo cuando solicitó el servicio por primera vez. Igualmente, AC GSE atenderá los requerimientos de renovación cuando sea solicitado por el responsable a través del diligenciamiento y envío del formulario. Su información será nuevamente validada con el fin de actualizar datos o completarla si se requiere.

2.9.4 Notificación al titular de la renovación del servicio sin cambio de credenciales.

Mediante correo electrónico se informa al responsable la activación del Servicios de Generación de Firmas Digitales y por consiguiente el suscriptor acepta y reconoce que una vez reciba el citado correo electrónico se entenderá entregado el servicio. Se entenderá que se ha recibido el correo electrónico donde se notifica la activación del servicio cuando dicho correo ingrese en el sistema de información designado por el responsable, esto es en la dirección correo electrónico que consta en el formulario de solicitud.

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

2.9.5 Forma en la que se acepta la renovación del servicio.

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

2.9.6 Notificación de la renovación por la ECD AC a otras entidades

No existen entidades externas a las que se requiera ser notificada la activación del servicio.

2.10 Renovación del servicio con cambio de llaves

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

Para la Autoridad de Certificación AC GSE, un requerimiento de renovación del servicio con cambio de credenciales es un requerimiento normal y por consiguiente procesar nuevamente la solicitud con la información que cambio, el suscriptor lo reconoce y acepta.



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

2.10.1 Circunstancias para la renovación del servicio con cambio de credenciales.

El servicio puede ser renovado a solicitud del responsable por próxima pérdida de vigencia de conformidad con las causales mencionadas en esta Política o cuando así lo requiera el responsable.

2.10.2 Quién puede solicitar una renovación con cambio de llaves.

Para el Servicios de Generación de Firmas Digitales el responsable puede solicitar la renovación con cambio de credenciales.

2.10.3 Trámites para la solicitud de renovación del servicio con cambio de llaves.

El procedimiento para renovación del Servicios de Generación de Firmas Digitales con cambio de llaves es igual al procedimiento de solicitud del servicio. El responsable tiene que ingresar al portal Web e iniciar el proceso de solicitud de renovación del servicio de la misma forma que lo hizo cuando solicitó el servicio por primera vez. Igualmente, AC GSE atenderá los requerimientos de renovación cuando sea solicitado por el responsable a través del diligenciamiento y envío del formulario. Su información será nuevamente validada con el fin de actualizar datos o completarla si se requiere.

2.10.4 Notificación al responsable de la activación del servicio con cambio de llaves

Mediante correo electrónico se informa al responsable la activación del Servicios de Generación de Firmas Digitales con cambio de llaves y por consiguiente el suscriptor acepta y reconoce que una vez reciba el citado correo electrónico se entenderá entregado el servicio. Se entenderá que se ha recibido el correo electrónico donde se notifica la activación del servicio cuando dicho correo ingrese en el sistema de información designado por el responsable, esto es en la dirección correo electrónico que consta en el formulario de solicitud.

2.10.5 Forma en la que se acepta la renovación del servicio.

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

2.10.6 Notificación de la renovación por la GSE a otras entidades

No existen entidades externas a las que se requiera ser notificada la activación del servicio

2.11 Modificación del servicio

El Servicios de Generación de Firmas Digitales, activado por la Autoridad de Certificación AC GSE, puede ser modificados las siguientes características:

- Por cambio de credenciales.
- Por cambio en el número de gigas solicitadas.

El responsable debe solicitar la modificación del servicio. En este evento y por una única vez se modificará el servicio y se informará al responsable, el sin costo de esta modificación adicional de la emisión será asumido completamente por el responsable conforme a las tarifas informadas por GSE., por el tiempo faltante para el

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

vencimiento original, cobrando solamente el valor del dispositivo criptográfico si a ello hubiere lugar.

2.12 Cancelación y suspensión del servicio

2.12.1 Circunstancias para la cancelación del servicio.

El responsable puede voluntariamente solicitar la cancelación del servicio en cualquier instante, pero está obligado a solicitar la cancelación del servicio bajo las siguientes situaciones:

- a. Por pérdida o inutilización de las credenciales (usuario y contraseña)
- b. Las credenciales han sido expuestas o corre peligro de que se le dé un uso indebido.
- c. Cambios en las circunstancias por la cuales GSE autorizo el servicio.



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

Si el responsable no solicita la cancelación del servicio 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 servicio.

El responsable reconoce y acepta que el Servicios de Generación de Firmas Digitales deben ser cancelación cuando GSE conoce o tiene indicios o confirmación de ocurrencia de alguna de las siguientes circunstancias:

- d. A petición del responsable o un tercero en su nombre y representación.
- e. Por cambio del responsable.
- f. Por muerte del responsable.
- g. Por liquidación en el caso de las personas jurídicas (entidad) que adquirieron el servicio.
- h. Por la confirmación o evidencia de que alguna información es falsa.
- i. Por el cese de actividades de la entidad de certificación.
- j. Por orden judicial o de entidad administrativa competente.
- k. Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
- l. Por incapacidad sobrevenida del responsable o entidad.
- m. Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
- n. Por la terminación del documento términos y condiciones, de conformidad con las causales establecidas en el contrato.
- o. Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la confiabilidad del certificado digital.
- p. Por el manejo indebido por parte del responsable del servicio.
- q. Por el incumplimiento del suscriptor o de la persona jurídica que representa o a la que está vinculado a través del documento de términos y condiciones o responsable del servicio.
- r. 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.
- s. En cualquier momento que se evidencie falsedad en los datos suministrados por el solicitante, suscriptor o responsable.
- t. Por incumplimiento por parte de la GSE, el suscriptor o responsable de las obligaciones establecidas en la Política.
- u. Por incumplimiento en el pago de los valores por los servicios de certificación, acordados entre el solicitante y GSE.

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

2.12.2 Quién puede solicitar una cancelación

El 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 cancelación del servicio*** de esta Política.

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

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

Política.

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

El comité de Seguridad como máximo ente de control que tiene atribuida la administración de la seguridad de la infraestructura tecnológica de GSE, está en capacidad de solicitar la revocación del servicio si tuviera el conocimiento o sospecha del compromiso de las credenciales del servicio o cualquier otro hecho que tienda al uso indebido del servicio por parte del responsable o de la GSE.

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

2.12.3 Procedimiento de solicitud de cancelación

Las personas interesadas en solicitar la cancelación del servicio cuyas causas están especificadas en esta Política lo pueden hacer bajo los siguientes procedimientos:

- *En las oficinas de GSE.*
En horario de atención al público se reciben las solicitudes escritas de cancelación del Servicios de Generación de Firmas Digitales firmadas por los suscriptores y/ responsables.
- *Servicio de cancelación telefónica.*
A través de la línea de atención telefónica permanente los responsables pueden solicitar la cancelación del servicio conforme a las causales de cancelación mencionadas en el apartado Circunstancias para la cancelación del servicio de esta Política.
- *Servicio de cancelación vía correo electrónico*
Por medio de nuestro correo electrónico documentos@gse.com.co, responsables pueden solicitar la cancelación del servicio conforme a las causales de cancelación mencionadas en el apartado Circunstancias para la cancelación del servicio de esta Política.

2.12.4 Periodo de gracia de solicitud de cancelación

Previo validación de la autenticidad de una solicitud de cancelación, GSE procederá en forma inmediata con la cancelación solicitada, dentro de los horarios de oficina de éste. Si se trató de una falsa alarma, el responsable debe notificar a la GSE para que proceda a reactivar el servicio si este fue revocado.

El procedimiento utilizado por GSE para verificar la autenticidad de una solicitud de revocación formulada por una persona determinada, es verificar la solicitud y validarla directamente con el suscriptor o responsable realizando el contacto con él mismo y confrontando los datos suministrados en la solicitud original.

Una vez solicitada la cancelación el servicio, si se evidencia que dicho servicio es utilizado el responsable releva de toda responsabilidad legal a GSE, toda vez que reconoce y acepta que el control, custodia y confidencialidad de las credenciales es responsabilidad exclusiva de este.

2.12.5 Plazo en el que la ECD debe resolver la solicitud de cancelación

La solicitud de cancelación del servicio debe ser atendida con la máxima urgencia, sin que la cancelación tome más de tres (3) días hábiles una vez validada la solicitud.

Una vez cumplidas las formalidades previstas para la cancelación y si por alguna razón, no se hace efectiva la cancelación del servicio en los términos establecidos por esta Política, GSE como prestador de servicios de certificación responderá por los perjuicios que se causen a los suscriptores o terceros de buena fe derivados de errores y omisiones, de mala fe de los administradores, representantes legales o empleados de 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 20142*. GSE no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros de confianza a excepción de lo establecido por las disposiciones de la presente Política.

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

2.12.6 Requisitos de verificación de las cancelaciones por los terceros de buena fe

Es responsabilidad del responsable del servicio y éste así lo acepta y reconoce, informar a los terceros de buena fe de la necesidad de comprobar la validez de las estampas cronológicas sobre los que esté haciendo uso en un momento dado.

2.12.7 Notificación de la cancelación del servicio

Dentro de las 24 horas siguientes a la cancelación del servicio de archivo, registro, conservación custodia y anotación para los documentos electrónicos transferibles y mensajes de datos, GSE informa al suscriptor o responsable, mediante correo electrónico, la cancelación del servicio y por consiguiente el solicitante acepta y reconoce que una vez reciba el citado correo electrónico se entenderá que su solicitud fue atendida. Se entenderá que se ha recibido el correo electrónico donde se notifica la cancelación del servicio cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección correo electrónico que consta en el formulario de solicitud.

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

2.12.8 Requisitos especiales de cancelación de credenciales comprometidas

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

2.12.9 Circunstancias para la suspensión

El servicio puede ser suspendido a solicitud del responsable por pérdida de las credenciales o cuando así lo requiera el responsable.

2.12.9.1 Quién puede solicitar la suspensión

Para el Servicios de Generación de Firmas Digitales, el responsable puede solicitar la suspensión.

2.12.9.2 Procedimiento de solicitud de suspensión

Las personas interesadas en solicitar la suspensión del servicio lo pueden hacer bajo los siguientes procedimientos:

- *En las oficinas de GSE.*
En horario de atención al público se reciben las solicitudes escritas de suspensión del Servicios de Generación de Firmas Digitales, firmadas por los suscriptores y/ responsables.
- *Servicio de suspensión telefónica.*
A través de la línea de atención telefónica permanente los suscriptores y responsables pueden solicitar la suspensión.
- *Servicio de suspensión vía correo electrónico*
Por medio de nuestro correo electrónico documentos@gse.com.co, los suscriptores y responsables pueden solicitar la suspensión del servicio.

2.12.9.3 Límites del periodo de suspensión

GSE dispondrá de un término de quince (15) días hábiles como periodo de tiempo máximo en la cual podrá estar el Servicios de Generación de Firmas Digitales, en estado suspendido, una vez superado el periodo el servicio será cancelado.

2.13 Límites de Responsabilidad de la Entidad de Certificación Abierta.

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

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor.
- Por el uso de los servicios siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente DPC y sus Anexos.



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia

27/11/2018

Versión

4

- Por el uso indebido o fraudulento de los servicios emitidos por la Autoridad de Certificación.
- Por el uso de la información contenida en el servicio.
- 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.
- Fraude en la documentación presentada por el solicitante.

2.14 Vigencia de los servicios.

El servicio de Generación de Firmas Digitales emitido por ECD GSE tiene una vigencia máxima de un (1) año.

3 OTROS ASUNTOS LEGALES Y COMERCIALES

3.1 Tarifas

3.1.1 Tarifas de emisión o renovación del servicio

PLATAFORMA			
Descripción	Valor Unitario	IVA	Valor Total
Paquete Personal, vigencia un (1) año.	\$ 300.000	\$ 57.000	\$ 357.000
Paquete Business, vigencia un (1) año.	\$ 750.000	\$ 142.500	\$ 892.500

*Están calculados sobre vigencia de un año. Las cifras aquí indicadas para cada tipo de servicio podrán variar según acuerdos comerciales especiales a los que se pueda llegar con los responsables, entidades o solicitantes, en desarrollo de campañas promocionales adelantadas por GSE.

3.1.2 Tarifas de revocación o acceso a la información de estado

La solicitud de revocación del servicio no tiene costo.

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

3.13 Tarifas de otros servicios

Una vez se ofrezcan otros servicios por parte de GSE, se publicarán en el portal web de GSE.

3.14 Política de reembolso

Una vez solicitado un certificado, esta solicitud se convierte en un documento de términos y condiciones, sobre el cual puede solicitarse reembolso por las siguientes circunstancias:

- **Insatisfacción del cliente:** Percepción del cliente sobre el grado en que se han cumplido sus requisitos, para lo cual GSE designara a la persona que evaluara la solicitud y pertinencia del reembolso de acuerdo a los lineamientos de protección del consumidor impartidos por la Superintendencia de Industria y Comercio.
- **Pago por un valor mayor al establecido:** Devolución de una cantidad de dinero cancelada en exceso por los servicios prestados por la GSE.

Para todos los casos el suscriptor y/o responsable debe ejecutar el procedimiento de Peticiones, Quejas, Reclamos, Solicitudes, Denuncias, Felicitaciones y Apelaciones.

4 OBLIGACIONES

4.1 Obligaciones de la ECD GSE

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

1. Respetar lo dispuesto en la normatividad vigente, la DPC y en las Políticas de Certificado.
2. Publicar la DPC y cada una de las Políticas de Certificado en la página Web de GSE.
3. Informar a ONAC sobre las modificaciones de la DPC y de las Políticas de Certificado.
4. Mantener la DPC y Políticas de Certificado con su última versión publicadas en la página Web de GSE.
5. Emitir el servicio conforme a las Políticas de Certificado y a los estándares definidos en la DPC.
6. Generar el servicio consistente con la información suministrada por el solicitante o suscriptor.
7. Conservar la información sobre los servicios emitidos de conformidad con la normatividad vigente.
8. No mantener copia de las credenciales de los servicios entregados al solicitante o suscriptor.
9. Revocar los servicios según lo dispuesto en las Políticas de Certificado.
10. Notificar al Solicitante, Suscriptor o Entidad la revocación del servicio digital dentro de las 24 horas siguientes de conformidad con las Política de Certificado.

4.2 Obligaciones de la RA

Las RA son las entidades delegadas por la ECD GSE para realizar la labor de identificación y registro, por lo

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

tanto, la RA está obligada en los términos definidos en la Declaración de Prácticas de Certificación a:

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

4.3 Obligaciones de EE

Las EE son las entidades delegadas por la ECD GSE para realizar la labor de enrolamiento de solicitantes, por lo tanto, la EE está obligada en los términos definidos en la DPC a:

1. Conocer y dar cumplimiento a lo dispuesto en la DPC y en las Políticas de Certificado para servicio de Archivo Confiable de Datos.
2. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
3. Archivar y custodiar la documentación suministrada por el solicitante o suscriptor, durante el tiempo establecido por la legislación vigente.
4. Respetar lo dispuesto en los contratos firmados entre ECD GSE y el suscriptor o responsable.

4.4 Obligaciones del suscriptor

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

1. Usar el servicio contratado según los términos de la DPC.
2. Verificar dentro del día siguiente hábil que la información del servicio contratado es correcta. En caso de encontrar inconsistencias, notificar a la ECD.
3. Abstenerse de: prestar, ceder, escribir, publicar la contraseña de uso su servicio y tomar todas las medidas necesarias, razonables y oportunas para evitar que éste sea utilizado por terceras personas.
4. Suministrar toda la información requerida en el Formulario de Solicitud de Certificados digitales o servicios para facilitar su oportuna y plena identificación.
5. Solicitar la revocación del servicio ante el cambio de nombre y/o apellidos.
6. Solicitar la revocación del Servicio cuando el Suscriptor haya variado su nacionalidad.
7. Cumplir con lo aceptado y firmado en el documento términos y condiciones o responsable de certificados digitales.



Políticas de Certificado para Servicios de generación de firmas digitales

Fecha de vigencia	27/11/2018
Versión	4

8. Proporcionar con exactitud y veracidad la información requerida.
9. Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del servicio.
10. Custodiar y proteger de manera responsable su llave privada.
11. Dar uso al servicio de conformidad con las PC establecidas en la DPC para cada uno de los tipos de certificado y servicios.
12. Solicitar como suscriptor o responsable de manera inmediata la revocación de su servicio cuando tenga conocimiento que existe una causal definida en numeral Circunstancias para la revocación de un certificado de la DPC.
13. No hacer uso de la llave privada ni del servicio digital una vez cumplida su vigencia o se encuentre revocado.

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

4.4.1 Obligaciones de los responsables

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

1. Usar su servicio según los términos de la DPC.
2. Verificar dentro del día siguiente hábil que la información del servicio es correcta, en caso de encontrar inconsistencias notificar a la ECD.
3. Abstenerse de: prestar, ceder, escribir, publicar la contraseña de uso su servicio y tomar todas las medidas necesarias, razonables y oportunas para evitar que éste sea utilizado por terceras personas.
4. Suministrar toda la información requerida en el Formulario de Solicitud de Certificados digitales o servicios para facilitar su oportuna y plena identificación.
5. Cumplir con lo aceptado y firmado en el documento términos y condiciones o responsable de certificados digitales.
6. Proporcionar con exactitud y veracidad la información requerida.
7. Informar durante la vigencia del servicio cualquier cambio en los datos suministrados inicialmente

para la emisión del certificado.

8. Custodiar y proteger de manera responsable su llave privada.
9. Dar uso al certificado de conformidad con las Políticas de Certificado establecidos en la DPC....
10. Solicitar como suscriptor o responsable de manera inmediata la revocación de su servicio cuando tenga conocimiento que existe una causal definida en numeral Circunstancias para la revocación de un certificado de la DPC.
11. No hacer uso de la llave privada ni del servicio una vez cumplida su vigencia o se encuentre revocado.
12. No realizar ninguna declaración relacionada con su servicio en la ECD GSE pueda considerar engañosa o no autorizada, conforme a lo dispuesto por la DPC y PC.
13. Una vez caducado o revocado el el responsable debe inmediatamente dejar de utilizarlo en todo el material publicitario que contenga alguna referencia al servicio que se le presta a la entidad.
14. El responsable del servicio deberá garantizar que la entidad cumple con lo dispuesto en el numeral Obligaciones de la Entidad.

4.5 Obligaciones de los Terceros de buena fe

Los Terceros de buena fe en su calidad de parte que confía en los servicios 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 servicios antes de realizar operaciones con certificados digitales.
4. Conocer y aceptar las condiciones sobre garantías, usos y responsabilidades al realizar operaciones con los servicios contratados.

4.6 Obligaciones de la Entidad.

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

1. Solicitar a la RA GSE la suspensión/revocación del servicio cuando cese o se modifique dicha vinculación.
2. Todas aquellas obligaciones vinculadas al responsable del servicio.
3. La entidad al hacer referencia al servicio prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, debe informar que cumple con los requisitos especificados en las PC de la DPC.
4. La entidad podrá utilizar las marcas de conformidad y la información relacionada con el servicio prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, desde que cumpla lo requerido en el literal anterior.

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

4.7 Obligaciones de otros participantes.

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

1. Revisar la consistencia de la PC con la normatividad vigente.
2. Aprobar y decidir sobre los cambios a realizar sobre los servicios, por decisiones de tipo normativo o por solicitudes de suscriptores o responsables.
3. Aprobar la notificación de cualquier cambio a los suscriptores y/ 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 se realice.
5. Informar los planes de acción a el ONAC y SIC sobre todo cambio que tenga impacto sobre la infraestructura PKI y que afecte los servicios, de acuerdo con el R-AC-01.
6. Autorizar los cambios o modificaciones requeridas sobre la PC.
7. Autorizar la publicación de la PC 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 servicio 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 PC para verificar que las longitudes de las llaves y periodos de los servicios que se estén empleando son adecuados.
14. Revisar, aprobar y autorizar cambios sobre los servicios de certificación digital acreditados por el organismo competente.
15. Revisar, aprobar y autorizar la propiedad y el uso de símbolos, servicios y cualquier otro mecanismo que requiera ECD GSE para indicar que el servicio de certificación digital está acreditado.
16. Velar que las condiciones de acreditación otorgado por el organismo competente se mantengan.
17. Velar por el uso adecuado en documentos o en cualquier otra publicidad que los símbolos, y cualquier otro mecanismo que indique que ECD GSE cuenta con un servicio de certificación acreditado y cumple con lo dispuesto en las Reglas de Acreditación de ONAC R-AC-01 y R-AC-1.4-03.
18. Velar por mantener informados a sus proveedores críticos y ECD recíproca en caso de existir, de la obligación de cumplimiento de los requisitos del CEA-4.1-10, en los numerales que correspondan.
19. El Equipo Sistema Integrado de Gestión ejecutara planes de acción preventivos y correctivos para responder ante cualquier riesgo que comprometa la imparcialidad de la ECD, ya sea que se derive

	Políticas de Certificado para Servicios de generación de firmas digitales	Fecha de vigencia	27/11/2018
		Versión	4

de las acciones de cualquier persona, organismo, organización, actividades, sus relaciones o las relaciones de su personal o de sí misma. Para lo cual utiliza la norma ISO 31000 para la identificación de riesgos que comprometa la imparcialidad de la ECD, entregando a la 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, especialmente aquellas que surjan por presiones comerciales, financieras u otras comprometan su imparcialidad.
21. Documentar y demostrar el compromiso de imparcialidad.
22. Velar que el personal administrativo, de gestión, técnico de la PKI, de la ECD asociado a las actividades de consultoría, mantenga completa independencia y autonomía respecto al personal del proceso de revisión y toma de decisión sobre la certificación de la misma ECD.

5 POLÍTICAS DEL SERVICIO DE GENERACION DE FIRMAS DIGITALES

Esta política define “**que**” requerimientos son necesarios para el Servicios de Generación de Firmas Digitales y “**como**” se cumplen los requerimientos de seguridad impuestos por la política.

6 MODELOS Y MINUTAS DE LOS DOCUMENTOS DE TÉRMINOS Y CONDICIONES Y/O RESPONSABLE

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

OID (Object Identifier)	1.3.6.1.4.1.31136.2.2
Ubicación de la PC	http://cps.gse.co