Documento	**Políticas de Certificado para Servicio de Generación de Firmas Digitales**
Versión	5
Grupo de Trabajo	Comité de Gerencia
Estado del documento	Final
Fecha de emisión	01-11-2016
Fecha de inicio de vigencia	12-04-2019
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	Área de Calidad
Aprobó	Comité de Gerencia

Control de Modificaciones

Versión	Fecha	Cambio/Modificación
1	01-11-2016	Documento inicial conforme al desarrollo del plan de acción 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	Actualización de cargos, tarifas y rutas de acceso a la página web, modificación del título, actualización de términos, inclusión de los límites de responsabilidad de la entidad de certificación abierta y 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 suministrar para la solicitud del servicio
5	12-04-2019	Se eliminó el numeral de las obligaciones de la EE, se unificaron las responsabilidades del suscriptor y responsable, se actualizaron las obligaciones de los suscriptores de acuerdo con el tipo de servicio. Se cambió la palabra “revocación” por “cancelación” y se amplió la descripción de los paquetes ofertados en el numeral 3.1.1 tarifas de emisión o renovación del servicio

1. INTRODUCCIÓN

1.1 Resumen

Política de Servicios de Generación de Firmas Digitales, 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, 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:

- Criterios Específicos de Acreditación para las Entidades de Certificación Digital CEA-4.1-10 (**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;
- RFC 5126 Febrero 2008
- RFC 5652 Septiembre 2009
- ETSI TS 101 733 Marzo 2012
- W3C XML Febrero 2003
- ETSI TS (EN) 101 903 Junio 2009
- ETSI TS(EN) 102 778 Julio 2009
- FIPS 140-2 Nivel 3. Mayo 2001
- RFC 5280 Mayo 2008.
- RFC 6960 Junio 2013
- FIPS 140-2 Nivel 3 Mayo 2001

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 Gerente de Operaciones ECD y Área de Calidad, cualquier cambio o adecuación sobre el documento deberá ser revisado, analizado y aprobado por los integrantes del Comité de Gerencia, 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:

Nombre:	GESTION DE SEGURIDAD ELECTRONICA S.A. – GSE S.A.
Número de Identificación Tributaria:	900.204.272 - 8
Registro Mercantil No:	01779392
Dirección:	Calle 73 No. 7 – 31 Piso 7 Torre B
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:	https://www.indenova.com/

DATOS DE LAS ENTIDADES DE REGISTRO

La entidad de registro es la misma prestadora de servicios de certificación digital.

1.2 Peticiones, Quejas, Reclamos, Solicitudes y Apelaciones

Las peticiones, quejas, reclamos, solicitudes y apelaciones sobre los servicios prestados por ECD GSE o entidades subcontratadas, explicaciones sobre esta Política de Certificación; son recibidas y atendidas directamente por GSE como ECD y serán resueltas por las personas pertinentes e imparciales o por los comités que tengan la competencia técnica necesaria, para lo cual se disponen de los siguientes canales para la atención a suscriptores, responsables y terceros.

Teléfono:	+57 (1) 5185158
Correo electrónico:	pqrs@gse.co
Dirección:	Calle 73 No. 7 – 31 Piso 7 Torre B.
Página Web:	www.gse.com.co
Responsable:	Área de Calidad

Una vez presentado el caso, este es trasmitido con la información concerniente al área de calidad según procedimiento interno establecido para la gestión de estas, una vez recibida la queja se realiza seguimiento para dar respuesta oportuna al cliente.

Recibida la PQRSA se procede a realizar la investigación respectiva para determinar si existe o no la queja, reclamo o apelación. En caso de existir, se determina qué área es responsable de tomar acciones administrativas o técnicas y si se requiere adoptar acciones correctivas o preventivas, caso en el cual se debe aplicar el procedimiento de acciones.

Generada la investigación se procede a evaluar la respuesta para posteriormente tomar la decisión que resuelve la queja y su comunicación final al suscriptor, responsable o parte interesada.

1.3 Definiciones y acrónimos

1.3.1 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 aquella que ofrece servicios propios de las entidades de certificación, tales que:

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

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

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

Autoridad de Registro (RA): En inglés "Registration Authority" (RA), es la entidad encargada de certificar la validez de la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

Declaración de Prácticas de Certificación (DPC): En inglés "Certification Practice Statement" (CPS), manifestación de la entidad de certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.
Política de Certificación (PC): Es un conjunto de reglas que definen las características de los distintos tipos de certificados y su uso.

Certificado digital: Mensaje de datos electrónico firmado por la entidad de certificación digital, el cual identifica tanto a la entidad de certificación que lo expide, como al suscriptor y contiene la llave pública de éste último.

Estampado cronológico: Mensaje de datos que vincula a otro mensaje de datos con un momento o periodo de tiempo concreto, el cual permite establecer con una prueba que estos datos existían en ese momento o periodo de tiempo y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado.

Autoridad de sellado de tiempo (TSA): Sigla en inglés de "Time Stamp Authority", entidad de confianza que emite sellos de tiempo.

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

Tercero de buena fe: Persona o entidad diferente del titular que decide aceptar y confiar en un servicio prestado por GSE.

Infraestructura de Llave Pública (PKI), Sigla en inglés de "Public Key Infrastructure", conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas (llave privada y llave pública), logran identificar al emisor de un mensaje de datos, impedir que terceras personas puedan observar los mensaje que se envían o alterar la información en la misma.

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, y es conocida únicamente por el titular del certificado.

Llave pública: Datos o códigos que son utilizados para verificar que una firma digital fue generada con la clave privada del suscriptor.

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.

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

Servicio del estado del certificados en línea: Sigla en inglés "Online Certificate Status Protocol" (OCSP), actividad de consulta en tiempo real al sistema de la ECD, sobre el estado de un certificado digital a través del protocolo OCSP.
CA de GSE: Es la Autoridad de Certificación de GSE, ente prestador de Servicios de Certificación digital.

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

Servicio 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 que puede ser 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 time stamping o "sellado de tiempo", que acredita la fecha y hora oficial del documento electrónico. Los documentos que se firman a través de esta plataforma quedaran activados como LTV.

LTV: "Long Term Validation" hace referencia al proceso de validación da la ruta completa de certificación de un certificado digital, en donde se aplica una estampa de tiempo acreditada en cada validación. Con lo anterior, se obtienen documentos cuya validez legal prevalece en el tiempo, sin importar si la entidad de certificación deja de existir o los certificados usados para firmar caducan.

1.3.2 Acrónimos

CA: Certification Authority
CPS: CertificationPractice Statement
CRL: Certificate Revocation List
CSP: Certification Service Provider
DNS: Domain Name System
FIPS: Federal Information Processing Standard
HTTP: El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.
HTTPS: Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por su acrónimo HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.
IEC: International Electrotechnical Commission
IETF: Internet Engineering Task Force (Organismo de estandarización de Internet)
IP: Internet Protocol
ISO: International Organization for Standardization
OCSP: Online Certificate Status Protocol.
OID: Object identifier (Identificador de objeto único)
PIN: Personal Identification Number
PUK: Personal Unlocking Key
PKCS: Public Key Cryptography Standards. Estándares de PKI desarrollados por RSA Laboratories y aceptados internacionalmente.
PKI: Public Key Infrastructure (Infraestructura de Llave Pública)
PKIX: Public Key Infrastructure (X.509)
RA: Registration Authority
RFC: Request For Comments (Estándar emitido por la IETF)
URL: Uniform Resource Locator

1.3.3 Estándares y Organismos de Estandarización

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

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 que puede ser 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 time stamping 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 de los 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 otros usuarios de la aplicación o a terceros que no sean 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 base 64, 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.

Así mismo, ambos formatos incluyen sellado de tiempo o time stamping, 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 servicio de generación de firmas digitales, debe utilizar el formato dispuesto para tal fin en la página web 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 y condiciones del servicio especificadas en la presente Política.
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 de la presentación de cualquier documento cuando la identidad del solicitante haya sido suficientemente verificada por GSE a través de otros medios.

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

2.4.1 Quién puede solicitar el servicio

Toda persona natural o jurídica legalmente facultada y debidamente identificada puede tramitar la solicitud del servicio de generación de firmas digitales.

2.4.2 Proceso de registro y responsabilidades

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

2.5 Procedimiento 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 RA de 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.

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

- Formulario de solicitud diligenciado, especificando el servicio de generación de firmas digitales.
- Formulario de solicitud diligenciado, especificando el tipo de certificado digital.
- Términos y condiciones firmados.
- Copia del documento de identidad del suscriptor.
- Documento de Existencia y Representación Legal de la empresa (no mayor a 30 días).
- Registro Único Tributario – RUT.

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 servicio de generación de firmas digitales. La ECD no asume ninguna responsabilidad por las consecuencias que puedan derivarse de la no aprobación del servicio 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 ECD GSE se reserva el derecho de no activar el servicio de generación de firmas digitales a pesar que la identificación del solicitante o la información suministrada por este haya sido plenamente autenticada, en particular por razones de orden legal o de conveniencia comercial, buen nombre o reputación de la ECD GSE; pueda poner en peligro 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 RA de 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 RA de GSE durante la activación del servicio

El paso final del proceso de activación del servicio de generación de firmas digitales es la entrega de las credenciales de acceso por parte de la RA de GSE y su entrega de manera segura al responsable.

El proceso de activación del servicio 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 ECD GSE de la activación del servicio

Mediante correo electrónico se informa al responsable de la activación del servicio 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 servicio 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, 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 servicio de generación de firmas digitales es aceptado por el responsable desde el momento que lo solicita, 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 2.12.

2.8 Uso del Servicio de Generación de Firmas Digitales

2.8.1 Uso del servicio por parte del responsable

El responsable del servicio emitido por la ECD 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, el servicio de generación de firmas digitales no deberá ser usado en otras actividades que estén por fuera de los usos mencionados. Una vez perdida la vigencia del servicio, el responsable está obligado a no seguir usando las credenciales y/o dispositivo criptográfico 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 expirada la vigencia. ECD GSE no asume ningún tipo de responsabilidad por los usos no autorizados.

2.9 Renovación del servicio sin cambio de credenciales

Para la ECD, un requerimiento de renovación del servicio sin cambio de credenciales es un proceso normal y por consiguiente implica solo procesar nuevamente la solicitud con la información que ha cambiado, el suscriptor lo reconoce y acepta. La emisión del certificado digital asociado a la cuenta del servicio de generación de firmas digitales se tratará como una solicitud nueva, para lo cual el cliente debe aportar la documentación correspondiente.

2.9.1 Circunstancias para la renovación del servicio sin cambio de credenciales

El servicio puede ser renovado a solicitud del responsable por vencimiento de vigencia.

2.9.2 Quién puede solicitar una renovación del servicio sin cambio de credenciales

Para la renovación sin cambio de credenciales del servicio de generación de firmas digitales, lo debe solicitar el responsable.

2.9.3 Trámites para la solicitud de renovación del servicio sin cambio de credenciales

El procedimiento para renovación del servicio 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, la ECD 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 completarlos 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 servicio 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, en la dirección correo electrónico que consta en el formulario de solicitud.

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 cancelación por parte del responsable y éste así lo acepta.

2.9.6 Notificación de la renovación por la ECD a otras entidades

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

2.10 Renovación del servicio con cambio de credenciales

Para la ECD 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. La emisión del certificado digital asociado a la cuenta del servicio de generación de firmas digitales se tratará como una solicitud nueva, para lo cual el cliente debe aportar la documentación correspondiente.

2.10.1 Circunstancias para la renovación del servicio con cambio de credenciales

El servicio puede ser renovado a solicitud del responsable por vencimiento de vigencia.

2.10.2 Quién puede solicitar una renovación con cambio de credenciales

Para el servicio 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 credenciales

El procedimiento para renovación del servicio de generación de firmas digitales con 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, la ECD 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 credenciales

Mediante correo electrónico se informa al responsable la activación del servicio de generación de firmas digitales con cambio de credenciales 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 cancelación por parte del y éste así lo acepta.

2.10.6 Notificación de la renovación por 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 servicio de generación de firmas digitales, activado por la ECD, puede ser modificado las siguientes características:

- **Por cambio de credenciales.** El responsable puede solicitar las credenciales de acceso al servicio sin costos adicionales.

En caso de que se requiera cambiar el titular del servicio, se podrá realizar una única vez y no aplicarán costos adicionales. En cuanto al certificado digital, aplicará el costo del dispositivo criptográfico. Para poder proceder con estas modificaciones, es necesario remitir comunicación formal a GSE y formato de solicitud de revocación (en el caso del certificado digital).

- **Por cambio en el número de gigas solicitadas:** El solicitante podrá solicitar la ampliación de espacio contratado aplicando costos adicionales. Dicho almacenamiento adicional tendrá la vigencia restante que tenga el servicio de archivo contratado.

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 las cuales GSE autorizo el servicio.

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 servicio de generación de firmas digitales debe ser cancelado cuando GSE conoce o tiene indicios o confirmación de ocurrencia de alguna de las siguientes circunstancias:

a) A petición del responsable o un tercero en su nombre y representación.
b) Por cambio del responsable.
c) Por muerte del responsable.
d) Por liquidación en el caso de las personas jurídicas (entidad) que adquirieron el servicio.
e) Por la confirmación o evidencia de que alguna información es falsa.
f) Por el cese de actividades de la entidad de certificación.
g) Por orden judicial o de entidad administrativa competente.
h) Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
i) Por incapacidad sobrevenida del responsable o entidad.
j) Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
k) Por la terminación del documento términos y condiciones, de conformidad con las causales establecidas en el contrato.
l) Por cualquier causa que razonablemente induzca a creer que el servicio de generación de firmas digitales haya sido comprometido.
m) Por el manejo indebido por parte del suscriptor y/o responsable del servicio.
n) 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.
o) Conocimiento de eventos que modifiquen el estado inicial de los datos suministrados, entre otros: terminación de la Representación Legal, terminación del vínculo laboral, liquidación o extinción de la personería jurídica, cesación en la función pública o cambio a una distinta.
p) En cualquier momento que se evidencie falsedad en los datos suministrados por el solicitante, suscriptor o responsable.
q) Por incumplimiento por parte de GSE, el suscriptor o responsable de las obligaciones establecidas en la Política.

r) 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 cancelar el servicio de generación de firmas digitales, cuando a su juicio se pueda poner en riesgo la credibilidad, confiabilidad, valor comercial, buen nombre de la ECD, idoneidad legal o moral de todo el sistema de certificación.

2.12.2 Quién puede solicitar una cancelación

Lo puede solicitar el responsable, un tercero de buena fe o cualquier persona interesada; cuando tenga constancia demostrable de conocimiento de hechos y causales mencionados en el apartado 2.12.1 ***Circunstancias para la cancelación del servicio*** de esta Política, o que el servicio ha sido empleado con fines diferentes a los expuestos en el aparte ***Usos del servicio por parte del responsable.***

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

El equipo de TI tanto de la RA como la CA 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 cancelación del servicio si tuviera el conocimiento o sospecha del compromiso de las credenciales o cualquier otro hecho que tienda al uso indebido del servicio por parte del responsable o de GSE.

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 servicio de generación de firmas digitales firmadas por los suscriptores y/ responsables.
- *Servicio por cancelación telefónica*
  A través de la línea de atención telefónica permanente, los suscriptores y responsables pueden solicitar la cancelación siempre y cuando envíen un oficio formal con la solicitud de cancelación.

- *Servicio de cancelación vía correo electrónico*
  Por medio de nuestro correo electrónico area.operaciones@gse.com.co, responsables pueden solicitar la cancelación del servicio conforme a las causales de cancelación mencionadas en el apartado 2.12.1 de esta Política.

2.12.4 Periodo de gracia de solicitud de cancelación

Previa 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 solicitud errónea, el responsable debe notificar a la GSE para que proceda a reactivar el servicio si este fue cancelado.

El procedimiento utilizado por GSE para verificar la autenticidad de una solicitud de cancelación 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 y mientras se procede, 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 2014.* 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.

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 servicio de generación de firmas digitales 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 generación de firmas digitales, 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, en la dirección correo electrónico que consta en el formulario de solicitud.

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 servicio 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 siempre y cuando envíen un oficio formal con la solicitud de suspensión.

- *Servicio de suspensión vía correo electrónico*
  Por medio de nuestro correo electrónico area.operaciones@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 servicio 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.
- 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.
- Si el servicio es solicitado con certificado digital, aplica lo establecido en la Declaración de Prácticas de Certificación.
- 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

*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.

PLATAFORMA			
Descripción	Valor Unitario	IVA	Valor Total
Paquete Personal, vigencia un (1) año, incluye: • Cinco (5) transacciones de firmas al mes • Cinco (5) transacciones de comunicaciones certificadas al mes • 2 Gb de almacenamiento. • Un (1) Certificado Digital Firma Centralizada de acuerdo al perfil requerido por el usuario.	$ 300.000	$ 57.000	$ 357.000
Paquete Business, vigencia un (1) año, cuenta administradora (primera cuenta creada) incluye: • Veinte (20) transacciones de firmas al mes • Veinte (20) transacciones de comunicaciones certificadas al mes • 2 Gb de almacenamiento. • Un (1) Certificado Digital Firma Centralizada de acuerdo al perfil requerido por el usuario.	$ 750.000	$ 142.500	$ 892.500

ADICIONALES			
Descripción	Valor Unitario	IVA	Valor Total
Precio GIGA adicional por año	$ 12.000	$ 2.280	$ 14.280

3.1.2 Tarifas de cancelación o acceso a la información de estado

La solicitud de cancelación del servicio no tiene costo.

3.1.3 Tarifas de otros servicios

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

3.1.4 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:

- **Satisfacción 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, y Apelaciones.

4. Políticas de seguridad de la plataforma.

La plataforma que se entrega atiende a los distintos aspectos de la seguridad:

- **Seguro**

El sistema no permite los accesos no autorizados a la información, a través de la plataforma y de ataques directos sobre los servidores sobre los que funciona.

- Todos los documentos se encuentran cifrados en el servidor y se descifran únicamente durante el tiempo que requiera alguna operación del usuario.
- Se utilizan cifrados seguros (SHA 256) con claves distintas para cada elemento.
- Protección contra SQL Injection por medio de filtros software en los accesos.
- Protección contra Cross Scripting por defecto. Viene implementada la protección en el framework GWT que se utiliza para el cliente.
- Comprobación de autorización en todas las operaciones que puede realizar el usuario.

- **Trazable**

- Todas las acciones de los usuarios que implican una modificación en un documento se registran.
- En algunos servicios como el de comunicaciones certificadas, la auditoría de eventos se firma y sella con TSA para asegurar su autenticidad.
- Existen 4 niveles de bitácora: Aplicación, Gestor documental, Log del contenedor de aplicaciones y Sistema Operativo.

- **Fidedigno**

- No se modifican los originales de los documentos. Los cambios se realizan mediante versionado de forma que se puedan revertir.
- Adicionalmente, en los casos en los que el documento se transforma para su visualización, se puede acceder al original para comprobar la fidelidad de lo que se visualiza.

- **Integridad**

- Todos los documentos cuentan con un HASH obtenido mediante algoritmo SHA256 que permite asegurar que el archivo físico almacenado en los medios de persistencia no ha sido modificado o alterado en modo alguno.

- En el caso de los documentos firmados, los propios formatos de firma que aplica la plataforma (PDF -> Pades LTV en formato PDF/A y Otros -> XADES LTV) permiten asegurar que un documento no ha sido modificado en ningún momento sin importar el tiempo que pase desde su firma.

- **Ciclo vital de larga duración**

  - La plataforma permite la conversión de los documentos compatibles al formato PDF/A. Este formato garantiza que el documento se visualizará de igual manera siempre.
  - Las firmas digitales aplicadas son siempre de larga duración con sellado de tiempo de tercero confiable el cual está sincronizad con la hora legal colombiana.

- **Certificado**
  - La plataforma cumple con los estándares internacionales definidos para el tratamiento seguro de la información y el tratamiento de información de carácter sensible o privado. Así lo acredita la certificación que a tal efecto ha obtenido de AENOR en la norma ISO/IEC 27001 y el cumplimiento del nuevo "Reglamento General de Protección de Datos (RGPD)" de la Unión Europea.

- **Auditado**
  - Se realizan auditorías internas de seguridad periódicamente utilizando herramientas de Ethical Hacking como OWASP ZAP.

5. OBLIGACIONES

5.1 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. Cancelar los servicios según lo dispuesto en las Políticas de Certificado.
10. Notificar al Solicitante, Suscriptor o Entidad la cancelación del servicio digital dentro de las 24 horas siguientes de conformidad con la Política del servicio.

5.2 Obligaciones de la RA

La RA son las entidades delegadas por la ECD de GSE para realizar la labor de identificación y registro, por lo 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. Comprobar la identidad de los Solicitantes, Responsables o Suscriptores de servicios de generación de firmas digitales.
3. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
4. Archivar y custodiar la documentación suministrada por el solicitante o suscriptor, durante el tiempo establecido por la legislación vigente.
5. Respetar lo dispuesto en los contratos firmados entre ECD GSE y el suscriptor y/o responsable.
6. Identificar e informar a la ECD GSE las causas de revocación/cancelación suministradas por los solicitantes sobre los servicios de certificación vigentes.

5.3 Obligaciones del suscriptor/o responsable

El Suscriptor como suscriptor o responsable de un servicio de generación de firmas digitales está obligado a cumplir con lo dispuesto por la normativa vigente y lo dispuesto en la PC y DPC como es:

1. Usar el servicio contratado según los términos de la DPC y PC.
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 las credenciales del 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.
6. Cumplir con las políticas de seguridad de la plataforma establecidas por GSE.
7. Proporcionar con exactitud y veracidad la información requerida.
8. Custodiar y proteger de manera responsable sus credenciales.
9. Abstenerse de usar el servicio para cometer actos ilícitos.
10. 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.
11. Una vez cancelado el servicio el suscriptor debe inmediatamente dejar de mencionarlo en todo el material publicitario que contenga alguna referencia al servicio.
12. 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 del momento en que adquirió el servicio.

13. El suscriptor podrá utilizar la marca GSE 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.

5.4 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 y PC.
3. Verificar el estado de los servicios antes de realizar operaciones.
4. Conocer y aceptar las condiciones sobre garantías, usos y responsabilidades al realizar operaciones con los servicios contratados.

5.5 Obligaciones de la Entidad (Cliente)

La entidad cliente es la encargada de solicitar los servicios para sus funcionarios y los suscriptores son las personas que hacen uso del servicio.

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

1. Solicitar a la RA de GSE la cancelación 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 GSE 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.

5.6 Obligaciones de otros participantes

El Comité de Gerencia y el área de Calidad 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 ONAC y SIC sobre todo cambio que tenga impacto sobre la infraestructura PKI y que afecte los servicios, de acuerdo con el RAC-3.0-01.
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. Conocer y tomar acciones pertinentes cuando se presenten incidentes de seguridad.
12. Revisar, aprobar y autorizar cambios sobre los servicios de certificación digital acreditados por el organismo competente.
13. 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.
14. Velar que las condiciones de acreditación otorgado por el organismo competente se mantengan.
15. 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 RAC-3.0-01 y RAC-3.0-03.
16. 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.
17. El área de Calidad ejecutará planes de acción preventivos y correctivos 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.
18. 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.

6. POLÍTICAS DEL SERVICIO DE GENERACION DE FIRMAS DIGITALES

Esta política define "**que**" requerimientos son necesarios para los servicios de generación de firmas digitales y "**como**" se cumplen los requerimientos de seguridad impuestos por la política.

7. 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)	**1.3.6.1.4.1.31136.3.2**
Ubicación de la PC	http://cps.gse.co