Documento	**Políticas de Certificado para Servicio de Estampado Cronológico**
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 (Objeto Identifier)	1.3.6.1.4.1.31136.2.3.3
Ubicación de la Política	http://cps.gse.co/
Elaboró	Gerente de operaciones ECD
Revisó	Area 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 la auditoria de ONAC.
2	01-10-2016	Actualización de información referente a la sede de ECD GSE
3	03-04-2018	Actualización conforme a recomendaciones de la auditoria de ONAC.
4	27-11-2018	Se cambia de V3 a V4 27/11/2018 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 actualizo la minuta de términos y condiciones y/o responsables, y se listo los documentos que se deben anexar para la solicitud del servicio

1 INTRODUCCIÓN

1.1 Resumen

Política de Servicio de Estampado Cronológico de GSE 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 ECD GSE)** como **Prestador de Servicios de Certificación digital (PSC)** aplica como lineamiento para prestar el servicio de estampado cronológico 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;
ii. ETSI EN 319 411-2: "Policy Requirements for certification authorities issuing qualified certificates".
iii. ETSI EN 319 412: "Qualified Certificate Profile".
iv. ETSI EN 319 411-3: "Policy Requirements for certification authorities issuing public key certificates".
v. RFC 3161 Internet X.509 Public Key Infraestructure Time-Stamp Protocol (TSP)
vi. RFC 5126 CMS Advanced Electronic Signatures (CAdES)
vii. RFC 5905 Network Time Protocol Version 4: Protocolo y especificación de algoritmos.
viii. RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs)

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.

DATOS DE GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A. – GSE:

Razón Social:	GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.
Sigla:	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
Fax:	+57 (1) 5185158
Correo electrónico:	info@gse.com.co
Página Web:	www.gse.co

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.

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

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 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 estampado cronológico.

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

Suscriptor: persona a cuyo nombre se expide un certificado.

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

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

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

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

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

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 ECD 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 público protegido mediante clave simétrico, actualmente no admitido como mecanismo para almacenar claves privadas para suscriptores.

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.

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

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

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

1.2.2 Acrónimos

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

TST: Token de Sello de Tiempo.
UTC: Hora Universal Coordinada.

1.2.3 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 SERVICIO DE ESTAMPADO CRONOLOGICO

2.1 Servicios de Estampado de Tiempo (TSS)

El Servicio de Estampado de Cronológico o Time Stamping Services (TSS) del inglés, es prestado por la Autoridad de Estampado Cronológico de GSE (TSA GSE) y su función principal es recibir las solicitudes de servicio de estampado cronológico del sistema administrado por el responsable o suscriptor y verificar los parámetros de la solicitud estén completos, si la verificación es correcta proceder a generar el estampado cronológico vinculando el mensaje de datos a la hora legal colombiana horalegal.inm.gov.co de conformidad con las políticas descritas en la presente Política. De esta forma, ECD GSE asegura que esos datos existían en una fecha y hora determinada.

2.2 Solicitud del servicio

Cualquier persona que requiera la prestación del servicio de estampado cronológico 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, ECD GSE validara 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 ECD GSE surte los procedimientos establecidos para la obtención del servicio de estampado cronológico.

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

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

aprobación 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.

2.2.1 Quién puede solicitar el servicio

Toda persona natural o jurídica legalmente facultada y debidamente identificada puede tramitar la solicitud del servicio de estampado cronológico.

2.2.2 Proceso de registro y responsabilidades

La ECD 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 ECD GSE.

2.3 Uso del servicio

2.3.1 Usos adecuados del certificado

Los servicios de estampado cronológico activos bajo esta Política pueden ser utilizados con los siguientes propósitos:

- **Integridad de la fecha del documento firmado:** La utilización del servicio de estampado cronológico para aplicar firmas digitales garantiza que el documento firmado es íntegro y el momento en el tiempo en el cual se aplicó la firma del servicio de estampado cronológico, es decir, garantiza que el documento no fue alterado o modificado después de firmado y la fecha exacta.

La política del servicio de estampado cronológico está identificada por un único identificador de objeto (OID) que además incluye el número de versión.

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

2.3.2 Usos prohibidos del servicio de estampado cronológico y exclusión de responsabilidad

Los servicios de estampado cronológico sólo podrán ser empleados para los usos para los que hayan sido emitidos y especificados en esta Política.

Se consideran usos indebidos aquellos que no están definidos en esta Política y en consecuencia para efectos legales, ECD GSE queda eximida de toda responsabilidad por el empleo del servicio de estampado cronológico en operaciones que estén fuera de los límites y condiciones establecidas para el uso de servicio de estampado cronológico según esta Política, dentro de los que se incluyen, pero sin limitarse a los siguientes usos prohibidos:

- Fines u operaciones ilícitas bajo cualquier régimen legal del mundo.
- Cualquier práctica contraria a la legislación colombiana.
- Cualquier práctica contraria a los convenios internacionales suscritos por el estado colombiano.
- Cualquier práctica contraria a las normas supranacionales.
- Cualquier práctica contraria a las buenas costumbres y prácticas comerciales.
- Cualquier uso en sistemas cuyo fallo pueda ocasionar:
  - Muerte.
  - Lesiones a personas.
  - Perjuicios al medio ambiente.
- Como sistema de control para actividades de alto riesgo como son:
  - Sistemas de navegación marítimo.
  - Sistemas de navegación de transporte terrestre,
  - Sistemas de navegación aéreo
  - Sistemas de control de tráfico aéreo.
  - Sistemas de control de armas.

2.4 Tramitación de solicitud del servicio

2.4.1 Realización de las funciones de identificación y autenticación

Las funciones de autenticación y verificación de la identidad del solicitante son realizadas por la RA 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.

2.4.2 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 estampado cronológico. ECD GSE no asume ninguna responsabilidad por las consecuencias que puedan derivarse de la no aprobación del servicio de estampado 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 estampado cronológico a pesar que la identificación del solicitante o la información suministrada por este haya sido plenamente autenticada, cuando la activación del servicio de estampado cronológico en particular por razones de orden legal o de conveniencia comercial, buen nombre o reputación de GSE pueda poner en peligro el sistema de certificación digital.

2.4.3 Plazo para procesar las solicitudes del servicio

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

2.5 Activación del servicio

2.5.1 Actuaciones de la ECD GSE durante la activación del servicio.

El paso final del proceso de activación del servicio de estampado cronológico es la entrega de las credenciales de acceso por parte de la ECD GSE y su entrega de manera segura al responsable.

El proceso de activación del servicio de estampado cronológico vincula de una manera segura la información de registro y las credenciales entregadas.

2.5.2 Notificación al solicitante por la ECD GSE de la activación del servicio

Mediante correo electrónico se informa al responsable la activación del servicio de estampado y por consiguiente el solicitante acepta y reconoce que una vez reciba el citado correo electrónico, se entenderá entregado el servicio de estampado cronológico. Se entenderá que se ha recibo 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.

2.5.3 Notificación de la activación del servicio por la ECD GSE a otras entidades

No aplica.

2.6 Aceptación del servicio

2.6.1 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 estampado cronológico 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 revocación por parte del responsable y éste así lo acepta, según procedimiento descrito en el apartado

2.7 Uso del servicio de estampado cronológico

2.7.1 Uso del servicio por parte del responsable

El responsable del servicio emitido por 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, los servicios de estampado cronológico no deberán ser usados 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 expirada la vigencia. ECD GSE no asume ningún tipo de responsabilidad por los usos no autorizados.

2.8 Renovación del servicio sin cambio de credenciales

Para ECD 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.

2.8.1 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.

2.8.2 Quién puede solicitar una renovación sin cambio de credenciales.

Para el servicio de estampado cronológico el responsable puede solicitar la renovación sin cambio de credenciales.

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

El procedimiento para renovación del servicio de estampado cronológico 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, 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.

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

Mediante correo electrónico se informa al responsable la activación del servicio de estampado cronológico 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 recibo 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.

2.8.5 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 responsable y éste así lo acepta.

2.8.6 Notificación de la renovación por la ECD a otras entidades

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

2.9 Renovación del servicio con cambio de llaves

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.

2.9.1 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.

2.9.2 Quién puede solicitar una renovación con cambio de llaves.

Para el servicio de estampado cronológico el responsable puede solicitar la renovación con cambio de credenciales.

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

El procedimiento para renovación del servicio de estampado cronológico 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, 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.

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

Mediante correo electrónico se informa al responsable la activación del servicio de estampado cronológico 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 recibo 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.

2.9.5 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 responsable y éste así lo acepta.

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

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

2.10 Modificación del servicio

El servicio de estampado cronológico activado por ECD GSE, puede ser modificado las siguientes características:

a. Por cambio de credenciales.
b. Por cambio en el número de estampas cronológicas solicitadas.

El responsable debe solicitar la modificación del servicio. En este evento se modificará el servicio y se informará al responsable, el costo de esta modificación será asumido completamente por el responsable conforme a las tarifas informadas por ECD GSE.

2.11 Cancelación y suspensión del servicio

2.11.1 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 ECD 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 estampado cronológico debe 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. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometida de manera material que afecte la confiabilidad del servicio de estampado cronológico.
j. Por el cese de actividades de la entidad de certificación.
k. Por orden judicial o de entidad administrativa competente.

l. Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
m. Por incapacidad sobrevenida del responsable o entidad.
n. Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
o. Por la terminación del documento términos y condiciones, de conformidad con las causales establecidas en el contrato.
p. 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.
q. Por el manejo indebido por parte del responsable del servicio.
r. 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 de TSA GSE.
s. 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.
t. En cualquier momento que se evidencie falsedad en los datos suministrados por el solicitante, suscriptor o responsable.
u. Por incumplimiento por parte de la ECD GSE, el suscriptor o responsable de las obligaciones establecidas en la Política.
v. Por incumplimiento en el pago de los valores por los servicios de certificación, acordados entre el solicitante y ECD GSE.

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

2.11.2 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 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 ECD 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 ECD GSE.

2.11.3 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 estampado

cronológico 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.

2.11.4 Periodo de gracia de solicitud de cancelación

Previa validación de la autenticidad de una solicitud de cancelación, ECD 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 ECD GSE para que proceda a reactivar el servicio si este fue revocado.

El procedimiento utilizado por ECD 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 ECD GSE, toda vez que reconoce y acepta que el control, custodia y confidencialidad de las credenciales es responsabilidad exclusiva de este.

2.11.5 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, ECD GSE como prestador de servicios de certificación responderá por los perjuicios que se causen a los suscriptores o terceros de buena fe derivados de errores y omisiones, de mala fe de los administradores, representantes legales o empleados de ECD GSE en el desarrollo de las actividades para las cuales cuenta con autorización y para ello cuenta con un seguro de responsabilidad civil de conformidad con el *Artículo 9°. Garantías, del Decreto 333 de 20142.* ECD GSE no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante titulares de certificados o terceros de confianza a excepción de lo establecido por las disposiciones de la presente Política.

2.11.6 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.

2.11.7 Notificación de la cancelación del servicio

Dentro de las 24 horas siguientes a la cancelación del servicio de estampado cronológico, ECD GSE informa al suscriptor o responsable, mediante correo electrónico, la cancelación del servicio de estampado cronológico 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 recibo el correo electrónico donde se notifica la cancelación del servicio de estampado cronológico 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.

2.11.8 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 de estampado cronológico 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 de estampado cronológico.

2.11.9 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.

2.11.9.1 Quién puede solicitar la suspensión

Para el servicio de estampado cronológico el responsable puede solicitar la suspensión.

2.11.9.2 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 servicio estampado cronológico 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.

2.11.9.3 Límites del periodo de suspensión

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

2.12 Perfiles de certificados

2.12.1 Perfil de certificado de la Unidad de Estampado Cronológico ECD GSE

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

CRL Profile, Requisitos establecidos por FIPS 140-1 Level 3, ISO/IEC 27001:2013.

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

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

2.12.2 Descripción del contenido de los certificados

Campo	Valor o restricciones
Versión	V3 (X.509 versión 3)
Número de Serie	Identificador único emitido por TSA GSE
Algoritmo de Firma	SHA2RSA
Emisor	Ver sección "Reglas para la interpretación de varias formas de nombre". Para TSA GSE como emisor se especifica: C = CO L = BOGOTÁ, D.C. STREET = http://www.gse.co/address OU = Trusted Timestamp Service http://www.gse.co T = Service Timestamping O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE E = tsa@gse.co SERIALNUMBER = 9002042728 CN = GSE TSA001_CO Description = GSE Timestamping Certificate 001 Colombia HW-KUSU
Válido desde	Especifica la fecha y hora a partir de la cual el certificado es válido. Se encuentra sincronizado con el servicio de tiempo UTC-5.
Válido hasta	Especifica la fecha y hora a partir de la cual el certificado deja de ser válido. Se encuentra sincronizado con el servicio de tiempo UTC-5.
Sujeto	Conforme a la política del Anexo 1 y las *"Reglas para la interpretación de Varias formas de nombre".*
Llave pública del Sujeto	Codificado de acuerdo con el RFC 5280. Los certificados emitidos por ECD GSE tienen una longitud de 2048 bits y algoritmo RSA.
Identificador de llave de la autoridad	Es utilizado para identificar el certificado raíz en la jerarquía de certificación. Normalmente referencia el campo "Subject Key Identifier" de ECD GSE como entidad emisora de certificación digital.
Identificador de la llave del sujeto	Es usado para identificar un certificado que contiene una determinada llave pública.
Política de certificado	Describe las políticas aplicables al certificado, especifica el OID y la dirección URL donde se encuentra disponible las políticas de certificación.
Uso de la llave	Especifica los usos permitidos de la llave. Es un CAMPO CRITICO.
Punto de distribución de la CRL	Es usado para indicar las direcciones donde se encuentra publicada la CRL De ECD GSE. En el certificado de la ECD Raíz, este atributo no

	se especifica.
Acceso a la información de la Autoridad	Es usado para indicar las direcciones donde se encuentra el certificado raíz de ECD GSE. Además, para indicar la dirección para acceder al servicio de OCSP. En el certificado raíz de ECD GSE, este atributo no se especifica.
Usos extendidos de la llave	Se especifican otros propósitos adicionales al uso de la llave.
Restricciones básicas	La extensión "PathLenConstraint" indica el número de sub-niveles que se admiten en la ruta del certificado. No existe restricción para ECD GSE, por tanto, es cero.

2.12.2.1 Número de versión

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

2.12.2.2 Extensiones del certificado

En el Anexo 2 de esta Política se describe de forma detallada los certificados emitidos bajo esta Política

2.12.2.3 Key Usage

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

2.12.2.4 Extensión de política de certificados

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

2.12.2.5 Nombre alternativo del sujeto

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

2.12.2.6 Restricciones básicas

- Para el caso de la TSA GSE en el campo "PathLenghtConstraint" de certificado de las subordinadas tiene un valor de 0, para indicar que la TSA GSE no permite más sub-niveles en la ruta del certificado. Es un campo crítico.
- Producir un sello de tiempo al recibir una solicitud válida del solicitante.
- Incluir dentro de cada ficha de tiempo un identificador que permita indicar de manera única la política de seguridad empleada.
- No examinar la impresión a la marca de tiempo en ningún momento.
- No incluir identificación de la entidad solicitante en los sellos de tiempo.
- La aplicación cliente debería verificar el campo de la política.
- La TSA GSE utiliza el protocolo NTP, el cual permite la sincronización en dos niveles con la hora

Legal del Instituto Nacional de Metrología de Colombia.

2.12.2.7 Uso extendido de la llave

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

OID	Descripción	Tipos de Certificados
1.3.6.1.5.5.7.3.8	Sellado de tiempo	Sellado de tiempo

2.12.2.8 Identificadores de objeto (OID) de los algoritmos

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

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

2.12.2.9 Formatos de nombres.

De conformidad con lo especificado en el numeral **Tipos de nombres** de esta Política.

2.12.2.10 Restricciones de los nombres.

El nombre se debe escribir en mayúsculas y sin tildes, la letra Ñ solo se permite para los nombres de personas naturales o jurídicas.

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

2.12.2.11 Identificador de objeto de la Política de Certificación

El identificador de objeto de la Política de certificado correspondiente a cada tipo de certificado, es una subclase de la clase definida en el numeral **Nombre del documento e identificación** de esta Política, conforme se establece en las Políticas de certificación de certificados digitales de firma (Anexo 1 de esta Política).

2.12.2.12 Uso de la extensión Policy Constrains

No se estipula.

2.12.2.13 Sintaxis y semántica de los Policy Qualifiers

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

2.12.2.14 Tratamiento semántico para la extensión Certificate Policies

No se estipula.

2.13 Perfil de CRL

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

2.13.1 Número de versión
Las CRL´s emitidas por TSA GSE cumplen con el estándar X.509 versión 2.

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

2.14 Perfil OCSP

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

2.14.1 Número de versión
Cumple con la OCSP Versión 1 del RFC2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

2.14.2 Extensiones OCSP
No aplica.

2.15 Servicios de información del estado de certificados

2.15.1 Características operacionales
Para la consulta del estado de los certificados emitidos por ECD GSE, se dispone de un servicio de consulta en línea basada en el protocolo OCSP (**Online Certificate Status Protocol:** Protocolo que permite revisar en línea el estado de un certificado digital) en la dirección http://ocsp.gse.co. El suscriptor o responsable envía una petición de consulta sobre el estado del certificado a través del protocolo OCSP, que, una vez consultada la base de datos, es atendida mediante una respuesta vía http, https, o por socket IP 318.

2.15.2 Disponibilidad del servicio
El servicio de consulta del estado de certificados digitales está disponible en la página Web de forma permanente las 24 horas durante todos los días del año.

La ECD GSE realizará todos los esfuerzos necesarios para que el servicio nunca se encuentre inaccesible de forma continua más de 24 horas, siendo este un servicio crítico en las actividades de la ECD GSE y por lo tanto tratado de forma adecuada en el plan de contingencias y de continuidad de negocio.

2.15.3 Características opcionales
Para obtener la información del estado de certificado en un momento dado, se puede hacer la consulta en línea en la dirección http://ocsp.gse.co, para lo cual se debe contar con un software que sea capaz de operar con el protocolo OCSP. La mayoría de navegadores ofrecen este servicio y será re direccionado según sea el caso por medio de los protocolos IPv4 o IPv6.

2.16 Finalización de la vigencia de un certificado

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

- Pérdida de validez por revocación del certificado digital.
- Vencimiento del periodo para el cual un suscriptor contrato la vigencia del certificado.
- Cuando ya no se use una TSA, pero la clave privada de la TSA ha sido comprometida, el certificado de la autoridad será revocado.

2.17 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.
- Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.
- Fraude en la documentación presentada por el solicitante.

2.18 Vigencia de los servicios.

El servicio de Estampado Cronológico (TSA) emitido por ECD GSE tiene una vigencia máxima de un (1) año o por el número de transacciones contratadas.

3 OTROS ASUNTOS LEGALES Y COMERCIALES

3.1 Tarifas

3.1.1 Tarifas de emisión o renovación del servicio

Estampado Cronológico			
Descripción	Valor Unitario	IVA	Valor Total
Paquete Ilimitado SaaS Servicio ilimitado dedicado (SaaS), incluye apliance de Estampado Cronológico en comodato con vigencia un (1) año.	$ 150.000.000	$ 28.500.000	$ 178.500.000
Paquete Ilimitado Servicio ilimitado de estampado cronológico.	$ 95.000.000	$ 18.050.000	$ 113.050.000
Paquete Premium Servicio de hasta 1.000.000 estampas cronológicas.	$ 60.000.000	$ 11.400.000	$ 71.400.000
Paquete 750mil Servicio de hasta 750.000 estampas cronológicas.	$ 19.000.000	$ 3.610.000	$ 22.610.000
Paquete 500mil Servicio de hasta 500.000 estampas cronológicas.	$ 15.000.000	$ 2.850.000	$ 17.850.000
Paquete 250mil Servicio de hasta 250.000 estampas cronológicas.	$ 7.500.000	$ 1.425.000	$ 8.925.000
Paquete 100mil Servicio de hasta 100.000 estampas cronológicas.	$ 4.200.000	$ 798.000	$ 4.998.000
Paquete 50mil Servicio de hasta 50.000 estampas cronológicas.	$ 3.100.000	$ 589.000	$ 3.689.000
Paquete 20mil Servicio de hasta 20.000 estampas cronológicas.	$ 2.500.000	$ 475.000	$ 2.975.000
Paquete 10mil Servicio de hasta 10.000 estampas cronológicas.	$ 1.700.000	$ 323.000	$ 2.023.000
Paquete 5000 Servicio de hasta 5.000 estampas cronológicas.	$ 1.400.000	$ 266.000	$ 1.666.000
Paquete 2000 Servicio de hasta 2.000 estampas cronológicas.	$ 700.000	$ 133.000	$ 833.000
Paquete 500 Servicio de hasta 500 estampas cronológicas.	$ 250.000	$ 47.500	$ 297.500

*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.

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 contrato de prestación de servicios, 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 ECD 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 ECD 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 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.
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.

4.5 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.

4.6 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.

4.7 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.

4.8 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 subscriptor, 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 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 ESTAMPADO CRONOLOGICO

Esta política define "**que**" requerimientos son necesarios para el servicio de estampado cronológico y "**como**" se cumplen los requerimientos de seguridad impuestos por la política.

6 PERFIL TÉCNICO CERTIFICADOS DIGITALES TSA GSE

GSE TIMESTAMPING CERTIFICATE 001 COLOMBIA				
Campo	**contenido**	**Obligatorio**	**Crítico**	**Observaciones**
1 TBSCertificate				
1.1 Versión	V3	√	X	[RFC5280]
1.2 Serial number	"02"	√	X	Asignado por la plataforma al momento de generar el certificado
1.3 Signature algorithm	Sha256RSA	√	X	OID 1.2.840.113549.1.1.11
1.4 Signature hash algorithm	SHA256	√	X	
2 Issuer				
2.1 Email (E)	ca@gse.co	√	-	
2.2 Common Name (CN)	Global Certification Authority Root GSE	√	X	OID 2.5.4.3
2.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
2.4 Serial Number	9002042728	√	-	OID 2.5.4.5
2.5 Organizational Unit	Internet Certification Authority http://www.gse.co	√	-	OID 2.5.4.11
2.6 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
2.7 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
2.8 Country	CO	√	X	OID 2.5.4.6
3 Validity				
3.1 notBefore	martes, 19 de enero de 2016 2:00:00 a. m.	√	X	
3.2 notAfter	miércoles, 10 de enero de 2046 2:00:00 a. m.	√	X	
4 Subject				
4.1 Email Address	tsa@gse.co	√	-	
4.2 Common Name (CN)	GSE TSA001_CO	√	X	OID 2.5.4.3
4.3 Organization	GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE	√	-	OID 2.5.4.10
4.4 Serial Number	9002042728	√	-	OID 2.5.4.5 Numero de identificación de ECD
4.5 Organizational Unit (OU)	Trusted Timestamp Service http://www.gse.co	√	-	OID 2.5.4.11
4.6 Title	Service Timestamping			OID 2.5.4.12
4.7 StreetAddress	http://www.gse.co/address	√	-	OID 2.5.4.9
4.8 Locality	BOGOTÁ, D.C.	√	-	OID 2.5.4.7
4.9 Country	CO	√	X	OID 2.5.4.6

4.10 Description	GSE Timestamping Certificate 001 Colombia HW-KUSU	√	-	OID 2.5.4.13
4.11 Subject Public Key Info		√	X	OID 1.2.840.113549.1.1.1 Clave pública de 2048 bits [RFC3279]
4.12 Public key parameters	"05 00"	√	X	

5Extensions				
5.1 Standard Extensions				
5.1.1 Authority Key Identifier	KeyID=47 a0 0c 09 87 8f 6a 38 41 d3 be af 7f a2 e6 14 3a 81 bf a0	√	X	OID 2.5.29.35
5.1.1.1 keyIdentifier		√	-	
5.1.1.2 authorityCertIssuer		√	-	
5.1.1.3 authorityCertSerialNumber		√	-	
5.1.2 Subject Key Identifier		√	-	OID 2.5.29.14
5.1.3 Key Usage		√	-	OID 2.5.29.15
5.1.3.1 digitalSignature	"0"	X	-	
5.1.3.2 nonRepudiation-ContentCommitment	"0"	X	-	
5.1.3.3 keyEncipherment	"0"	X	-	
5.1.3.4 dataEncipherment	"0"	X	-	
5.1.3.5 keyAgreement	"0"	X	-	
5.1.3.6 keyCertSign	"1"	√	-	
5.1.3.7 cRLSign	"1"	√	-	
5.1.3.8 encipherOnly	"0"	X	-	
5.1.3.9 decipherOnly	"0"	X	-	
5.1.4 Certificate Policies	1.3.6.1.4.1.31136.2.1.3.2	√	X	OID 2.5.29.32
5.1.4.1 Policy Identifier		√	-	OID Definido por ECD GSE
5.1.4.2 Policy Qualifier ID		√	-	
5.1.4.2.1 CPS Pointer	http://cps.gse.co/	√	-	OID 1.3.6.1.5.5.7.2.1
5.1.4.2.2 User Notice	Terms of use at TSA CA GSE http://cps.gse.co	√	-	
5.1.5 Subject Alternative Name	info@gse.co	√	X	
5.1.6 Issuer Alternative Name	URI:http://www.gse.co	√	X	OID 2.5.29.18
5.1.7 Subject Directory Attributes	No está presente	X	X	OID 2.5.29.9
5.1.8 Basic Constraints		√	√	
5.1.8.1 cA	CA	√	-	
5.1.8.2 pathLenConstraint	0	√	-	
5.1.9 Name Constraints	No está presente	X	X	

5.1.10 Policy Constraints	No está presente	X	X	
5.1.11 Extended Key Usage	No está presente	X	X	OID 2.5.29.37
5.1.11.1 serverAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.1
5.1.11.2 clientAuth	"0"	-	-	OID 1.3.6.1.5.5.7.3.2
5.1.11.3 codeSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.3
5.1.11.4 emailProtection	"0"	-	-	OID 1.3.6.1.5.5.7.3.4
5.1.11.5 timeStamping	"0"	-	-	OID 1.3.6.1.5.5.7.3.8
5.1.11.6 OCSPSigning	"0"	-	-	OID 1.3.6.1.5.5.7.3.9
5.1.11.7 Microsoft Smart Card Logon for Windows 1.3.6.2.1.311.20.2.2	"0"	-	-	OID 1.3.6.1.4.1.311.20.2.2
5.1.11.8 Microsoft Commercial Code Signing 1.3.6.2.1.311.2.1.22	"0"	-	-	OID 1.3.6.1.4.1.311.2.1.22
5.1.11.9 Microsoft Encrypting File System 1.3.6.2.1.31136.10.3.4	"0"	-	-	OID 1.3.6.1.4.1.311.10.3.4
5.1.12 CRL Distribution Points		√	-	OID 2.5.29.31
5.1.12.1 CRL Distribution Point 1	URL=http://crl.gse.co/root/crl_root_gse_sha2.crl	√	-	
5.1.12.2 CRL Distribution Point 2	URL=http://crl1.gse.co/root/crl_root_gse_sha2.crl	√	-	
5.1.13 qcStatements	No está presente	-	-	OID 1.3.6.1.5.5.7.1.3
5.1.13.1 id-etsi-qcs-QcCompliance	No está presente	-	-	
5.1.13.2 id-etsi-qcs-QcLimitValue	No está presente	-	-	
5.1.13.3 id-etsi-qcs-QcSSCD	No está presente	-	-	
5.1.14 Netscape Cert Type	No está presente	√	-	
5.1.15 Netscape Revocation URL	No está presente	-	-	
5.1.16 Netscape CA Policy URL	No está presente	-	-	
5.1.17 Netscape Comment	No está presente	-	-	
5.1.18 biometricInfo	No está presente	-	-	
5.1.19 Inhibit Any-Policy	No está presente	-	-	
5.1.20 Freshest CRL	No está presente	-	-	

5.2 Internet Certificate Extensions				
5.2.1 Authority Information Access 1		√	-	OID 1.3.6.1.5.5.7.1.1
5.2.1.1 accessMethod	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	√	-	
5.2.1.2 accessLocation	URI:http://certs.gse.co/root/crt_root			

	_gse_sha2.crt	√	-	
5.2.2 Authority Information Access 2		-	-	
5.2.2.1 accessMethod	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	-	-	
5.2.2.2 accessLocation	URI:http://ocsp.gse.co	-	-	
5.2.3 Subject Information Access	No está presente	-	-	
6 PKCS#12				
6.1. Friendly Name		-	-	
7 Huella Digital				
7.1 Thumbprint algorithm	sha1	√	X	
7.2 Thumbprint	0 d f7 68 36 0d a8 3e cc 3a cd 42 73 29 95 a9 b3 f3 6d da 0f	√	X	

OID (Objeto Identifier)	1.3.6.1.4.1.31136.2.3.3
Ubicación de la Política	http://cps.gse.co/

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)	**1.3.6.1.4.1.31136.2.2**
Ubicación de la PC	http://cps.gse.co