



GSE  
GESTIÓN DE SEGURIDAD  
ELECTRÓNICA

## Declaración de prácticas de certificación

Fecha de  
vigencia 12/04/2019

Versión 5

<b>Título del Documento:</b>	<b>Declaración de Prácticas de Certificación</b>
<b>Versión:</b>	5
<b>Grupo de Trabajo:</b>	Comité de Gerencia
<b>Estado del documento:</b>	Final
<b>Fecha de emisión</b>	28-03-2018
<b>Fecha de inicio de vigencia</b>	12-04-2019
<b>OID (Object Identifier) - IANA</b>	1.3.6.1.4.1.31136.2.2
<b>Ubicación de la DPC</b>	<a href="http://cps.gse.co/sub/cps_sub001co_ca_gse.pdf">http://cps.gse.co/sub/cps_sub001co_ca_gse.pdf</a>
<b>Elaboró</b>	Gerente de Operaciones ECD
<b>Revisó</b>	Area calidad
<b>Aprobó</b>	Comité de Gerencia

La última versión aprobada de la Declaración de Prácticas de Certificación (DPC) se encuentra disponible en la página web de GSE S.A. ([www.gse.com.co](http://www.gse.com.co))

### Control de Modificaciones

Versión	Fecha	Cambio/Modificación
1	01-11-2016	Documento inicial
2	04-10-2017	<ul style="list-style-type: none"> <li>Actualización de datos de contacto de la ECD y Logo</li> <li>Actualización de las entidades de Enrolamiento</li> <li>Actualización datos de contacto Proveedores de servicios de certificación</li> <li>Información referente al Director General de GSE.</li> </ul>
2	27-10-2017	Actualización datos TSA GSE.
3	03-04-2018	Actualización información y ajustes con relación al CEA-4.1-10 de acuerdo con la revisión de las matrices de requisitos.
4	27-11-2018	Se cambio de la V3 a V4 el 27/11/2018 Actualización de tabla de contenido, información y ajustes con relación a nuevos cargos, tarifas, rutas de acceso a la página web, corrección de la subornidanada, se incluye la frase establecido y probado, se amplía el numeral 8.7.4 nombrando los mecanismos tecnológicos empleados para la protección de datos, se relacionaron todas las políticas de certificación, cambio de términos y actualización del representante legal.
5	12-04-2019	Se elimino el numeral de la EE, se aclaro que para el uso del certificado de firma centralizada, es necesario la adquisición de una plataforma tecnológica con costos adicionales Se hace la aclaración en el numeral 1.6.2 de los requisitos y restricciones de la RA Se actualizaron los roles de la RA

<b>1</b>	<b>INTRODUCCIÓN .....</b>	<b>8</b>
1.1	Resumen .....	8
1.2	Peticiones, Quejas, Reclamos, Solicitudes y Apelaciones .....	9
1.3	Nombre del documento e identificación .....	9
1.4	Marco Jurídico .....	10
1.4.1	Mecanismo de Resolución de Diferencias .....	10
1.5	Definiciones y acrónimos .....	10
1.5.1	Definiciones .....	10
1.5.2	Acrónimos .....	13
1.5.3	Estándares y Organismos de estandarización .....	14
1.6	PKI participantes .....	14
1.6.1	Autoridad de Certificación (CA) .....	14
1.6.2	Autoridad de Registro (RA) .....	15
1.6.3	Suscriptor y/o responsable .....	15
1.6.4	Responsable .....	15
1.6.5	Solicitante .....	15
1.6.6	Entidad a la cual se encuentra vinculado el suscriptor o responsable .....	16
1.6.7	Otros participantes .....	16
1.7	Administración de la DPC y PC .....	17
1.7.1	Organización administradora del documento .....	17
1.7.2	Persona de contacto: .....	17
1.7.3	Persona o área que determina la adecuación de las Políticas a la DPC .....	17
1.7.4	Procedimientos de aprobación de la DPC .....	17
1.8	Cambios que afecten los servicios de certificación digital .....	17
1.8.1	Procedimiento para los cambios .....	18
1.8.2	Mecanismo y periodo de notificación .....	18
<b>2</b>	<b>RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN .....</b>	<b>18</b>
2.1	Repositorios .....	18
2.2	Publicación de la información de certificación .....	20
2.3	Plazo o frecuencia de la publicación .....	20
2.4	Controles de acceso a los repositorios .....	20
<b>3</b>	<b>IDENTIFICACIÓN Y AUTENTICACIÓN .....</b>	<b>21</b>
3.1	Nombres .....	21
3.1.1	Tipos de nombres .....	21
3.1.2	Nombres Distintivos .....	24
3.1.3	Anonimato y pseudoanonimato del suscriptor o responsables .....	24
3.1.4	Reglas para la interpretación de varias formas de nombre .....	24
3.1.5	Singularidad de los nombres .....	24
3.1.6	Reconocimiento, autenticación y papel de las marcas reconocidas .....	24
3.2	Validación inicial de la identidad .....	24
3.2.1	Método para demostrar la posesión de la llave privada .....	24
3.2.2	Autenticación de la identidad de una entidad (Persona jurídica) .....	25
3.2.3	Autenticación de una identidad individual (Persona Natural) .....	25
3.2.4	Información de suscriptor o responsable no verificada .....	25
3.2.5	Criterios para la interoperabilidad .....	25
3.3	Identificación y autenticación para peticiones de renovación de llaves .....	25
3.3.1	Identificación y autenticación para renovación .....	25
3.3.2	Identificación y autenticación tras una revocación .....	25
3.4	Identificación y autenticación para peticiones de revocación .....	25

<b>4</b>	<b>Requisitos operacionales para el tiempo de vida de los certificados.....</b>	<b>26</b>
4.1	<b>Solicitud del certificado.....</b>	<b>26</b>
4.1.1	Quién puede solicitar un certificado.....	26
4.1.2	Proceso de registro y responsabilidades.....	26
4.2	<b>Uso del certificado.....</b>	<b>26</b>
4.2.1	Usos adecuados del certificado.....	27
4.2.2	Usos prohibidos del certificado y exclusión de responsabilidad.....	27
4.3	<b>Tramitación de solicitud de certificados.....</b>	<b>28</b>
4.3.1	Realización de las funciones de identificación y autenticación.....	28
4.3.2	Aprobación o rechazo de las solicitudes de certificado.....	28
4.3.3	Plazo para procesar las solicitudes de certificado.....	29
4.4	<b>Emisión de certificados.....</b>	<b>29</b>
4.4.1	Actuaciones de la ECD GSE durante la emisión de certificados.....	29
4.4.2	Notificación al solicitante por la ECD GSE de la emisión del certificado.....	29
4.4.3	Notificación de la emisión del certificado por la ECD a otras entidades.....	29
4.5	<b>Aceptación del certificado.....</b>	<b>29</b>
4.5.1	Forma en la que se acepta el certificado.....	29
4.6	<b>Uso de la llave privada y del certificado.....</b>	<b>29</b>
4.6.1	Uso de la llave privada y del certificado por parte del suscriptor o responsable.....	30
4.6.2	Uso de la llave privada y del certificado por terceros de buena fe.....	30
4.7	<b>Renovación del certificado sin cambio de llaves.....</b>	<b>31</b>
4.7.1	Circunstancias para la renovación de certificados sin cambio de llaves.....	31
4.7.2	Quién puede solicitar una renovación sin cambio de llaves.....	31
4.7.3	Trámites para la solicitud de renovación de certificados sin cambio de llaves.....	31
4.7.4	Notificación al suscriptor o responsable de la emisión de un nuevo certificado sin cambio de llaves.....	31
4.7.5	Forma en la que se acepta la renovación de un certificado sin cambio de llaves.....	31
4.7.6	Publicación del certificado renovado por la ECD sin cambio de llaves.....	31
4.7.7	Notificación de la emisión de un certificado renovado por la ECD a otras entidades.....	31
4.8	<b>Renovación del certificado con cambio de llaves.....</b>	<b>31</b>
4.8.1	Circunstancias para la renovación de certificados con cambio de llaves.....	31
4.8.2	Quién puede solicitar una renovación con cambio de llaves.....	31
4.8.3	Trámites para la solicitud de renovación de certificados con cambio de llaves.....	32
4.8.4	Notificación al suscriptor o responsable de la emisión de un nuevo certificado con cambio de llaves.....	32
4.8.5	Forma en la que se acepta la renovación de un certificado.....	32
4.8.6	Publicación del certificado renovado por la ECD con cambio de llaves.....	32
4.8.7	Notificación de la emisión de un certificado renovado por la ECD a otras entidades.....	32
4.9	<b>Modificación de certificados.....</b>	<b>32</b>
4.9.1	Circunstancias para la modificación de un certificado.....	32
4.9.2	Quién puede solicitar una modificación.....	32
4.9.3	Trámites para la solicitud de modificación de un certificado.....	33
4.9.4	Notificación al suscriptor o responsable de la emisión de un nuevo certificado.....	33
4.9.5	Forma en la que se acepta la modificación de un certificado.....	33
4.9.6	Publicación del certificado modificado por la ECD.....	33
4.9.7	Notificación de la emisión de un certificado por la ECD a otras entidades.....	33
4.10	<b>Revocación y suspensión de certificados.....</b>	<b>33</b>
4.10.1	Circunstancias para la revocación de un certificado.....	33
4.10.2	Quién puede solicitar una revocación.....	34
4.10.3	Procedimiento de solicitud de revocación.....	35
4.10.4	Periodo de gracia de solicitud de revocación.....	35
4.10.5	Plazo en el que la ECD debe resolver la solicitud de revocación.....	35
4.10.6	Requisitos de verificación de las revocaciones por los terceros de buena fe.....	36
4.10.7	Frecuencia de emisión de las CRLs.....	36
4.10.8	Tiempo máximo de latencia de las CRLs.....	36
4.10.9	Revocación on-line/disponibilidad de verificación del estado.....	36

4.10.10	Requisitos de comprobación de la revocación on-line .....	36
4.10.11	Notificación de la revocación de un certificado .....	36
4.10.12	Otras formas disponibles de divulgación de información de revocación .....	37
4.10.13	Requisitos especiales de renovación de llaves comprometidas .....	37
4.10.14	Circunstancias para la suspensión .....	37
<b>4.11</b>	<b>Perfiles de certificados .....</b>	<b>37</b>
4.11.1	Descripción del contenido de los certificados GSE Subordinate Certificate 001 Colombia .....	38
4.11.2	Descripción del contenido de los certificados GSE Subordinate Certificate 001 Perú .....	39
4.11.3	Descripción del contenido de los certificados GSE Timestamping Certificate 001 Colombia .....	40
4.11.4	Descripción del contenido de los certificados GSE Timestamping Certificate 001 Perú .....	41
<b>4.12</b>	<b>Servicios de información del estado de certificados .....</b>	<b>44</b>
4.12.2	Características operacionales .....	45
4.12.3	Características opcionales .....	45
<b>4.13</b>	<b>Finalización de la vigencia de un certificado .....</b>	<b>45</b>
<b>4.14</b>	<b>Custodia y recuperación de llaves .....</b>	<b>45</b>
4.14.1	Almacenamiento de la clave privada del suscriptor .....	45
4.14.2	Almacenamiento de la clave privada a un responsable .....	45
4.14.3	Prácticas y políticas de custodia y recuperación de llaves .....	46
4.14.4	Prácticas y políticas de custodia y recuperación de la clave de sesión .....	46
<b>5</b>	<b>CONTROLES FÍSICOS DE LA INSTALACION, GESTIÓN Y OPERACIONALES .....</b>	<b>46</b>
<b>5.1</b>	<b>Controles físicos de la infraestructura tecnológica a través de la cual ECD GSE presta sus servicios .....</b>	<b>46</b>
5.1.1	Ubicación física y construcción .....	46
5.1.2	Acceso físico .....	47
5.1.3	Alimentación eléctrica y aire acondicionado .....	47
5.1.4	Exposición al agua .....	47
5.1.5	Prevención y protección de incendios .....	47
5.1.6	Sistema de almacenamiento .....	47
5.1.7	Eliminación del material de almacenamiento de la información .....	47
5.1.8	Backup fuera de la instalación .....	48
<b>5.2</b>	<b>Controles de procedimiento .....</b>	<b>48</b>
5.2.1	Roles de confianza .....	48
5.2.2	Número de personas requeridas por tarea .....	48
5.2.3	Identificación y autenticación para cada rol .....	48
5.2.4	Roles que requieren segregación de funciones .....	48
<b>5.3</b>	<b>Controles de personal .....</b>	<b>48</b>
5.3.1	Requisitos sobre la cualificación, experiencia y conocimiento profesionales .....	49
5.3.2	Procedimiento de comprobación de antecedentes .....	49
5.3.3	Requisitos de formación .....	49
5.3.4	Requisitos y frecuencia de actualización de formación .....	49
5.3.5	Frecuencia y secuencia de rotación de tareas .....	49
5.3.6	Sanciones por actuaciones no autorizadas .....	49
5.3.7	Requisitos de contratación de terceros .....	49
5.3.8	Documentación proporcionada al personal .....	49
<b>5.4</b>	<b>Procedimientos de auditoría de seguridad de la PKI .....</b>	<b>50</b>
5.4.1	Tipos de eventos registrados .....	50
5.4.2	Frecuencia de procesado de registros de auditoría (log) .....	50
5.4.3	Periodo de retención de los registros de auditoría .....	50
5.4.4	Protección de los registros de auditoría .....	50
5.4.5	Procedimientos de backup de los registros de auditoría .....	50
5.4.6	Sistema de recogida de información de auditoría (interna o externa) .....	50
5.4.7	Notificación al sujeto causa del evento .....	50
5.4.8	Análisis de vulnerabilidades .....	51
<b>5.5</b>	<b>Archivo de registros y eventos de la PKI .....</b>	<b>51</b>
5.5.1	Tipos de eventos archivados .....	51

5.5.2	Periodo de conservación .....	51
5.5.3	Protección de archivos.....	51
5.5.4	Procedimientos de backup del archivo de registros .....	51
5.5.5	Requisitos para el sellado de tiempo de los registros .....	51
5.5.6	Sistema de archivo de la información de auditoría (interna o externa) .....	51
5.5.7	Procedimientos para obtener y verificar información archivada .....	51
<b>5.6</b>	<b>Cambio de llaves de la ECD .....</b>	<b>52</b>
5.6.1	Cambio de llaves de la raíz ECD GSE .....	52
5.6.2	Cambio de llaves de una Subordinada de ECD GSE .....	52
<b>5.7</b>	<b>Recuperación en caso de compromiso de una llave y desastre natural u otro tipo de catástrofe .....</b>	<b>52</b>
5.7.1	Procedimientos de gestión de incidentes .....	52
5.7.2	Alteración de los recursos hardware, software o datos .....	52
5.7.3	Procedimiento de actuación ante la vulnerabilidad de la llave privada de una Autoridad .....	52
5.7.4	Capacidad de recuperación después de un desastre natural u otro tipo de catástrofe .....	53
<b>5.8</b>	<b>Cese de una ECD .....</b>	<b>53</b>
<b>6</b>	<b>CONTROLES TÉCNICOS DE SEGURIDAD .....</b>	<b>54</b>
<b>6.1</b>	<b>Generación e instalación del par de llaves .....</b>	<b>54</b>
6.1.1	Generación del par de llaves .....	54
6.1.2	Entrega de la llave privada a los suscriptores .....	54
6.1.3	Entrega de la llave pública al emisor del certificado .....	54
6.1.4	Entrega de la llave pública de la ECD a terceros aceptantes.....	54
6.1.5	Tamaño de las llaves .....	55
6.1.6	Parámetros de generación de la llave pública y verificación de la calidad .....	55
6.1.7	Usos permitidos de la llave (según el campo key usage de la X.509) .....	55
<b>6.2</b>	<b>Protección de la llave privada y controles de ingeniería de los módulos criptográficos .....</b>	<b>55</b>
6.2.1	Controles y estándares para los módulos criptográficos .....	56
6.2.2	Control multipersona (n de m) de la llave privada.....	56
6.2.3	Custodia de la llave privada .....	56
6.2.4	Backup de la llave privada .....	56
6.2.5	Archivo de la llave privada .....	56
6.2.6	Transferencia de la llave privada a/desde el módulo criptográfico .....	57
6.2.7	Almacenamiento de las llaves privadas en un módulo criptográfico .....	57
6.2.8	Método de activación de la llave privada .....	57
6.2.9	Método de desactivación de la llave privada .....	57
6.2.10	Método para destruir la llave privada .....	57
6.2.11	Características técnicas de los módulos criptográficos utilizados .....	57
6.2.12	Evaluación del módulo criptográfico .....	57
6.2.13	Evaluación del sistema de cifrado .....	57
<b>6.3</b>	<b>Otros aspectos de la gestión del par de llaves.....</b>	<b>58</b>
6.3.1	Archivo de la llave pública .....	58
6.3.2	Periodos operativos de los certificados y periodo de uso del par de llaves.....	58
<b>6.4</b>	<b>Datos de activación .....</b>	<b>58</b>
6.4.1	Generación e instalación de los datos de activación .....	58
6.4.2	Protección de los datos de activación .....	58
6.4.3	Otros aspectos de los datos de activación .....	58
<b>6.5</b>	<b>Controles de seguridad informática.....</b>	<b>58</b>
6.5.1	Requisitos técnicos de seguridad específicos .....	59
6.5.2	Evaluación de la seguridad informática .....	59
6.5.3	Acciones en caso de un evento o incidente de seguridad de la información .....	59
<b>6.6</b>	<b>Controles técnicos del ciclo de vida .....</b>	<b>60</b>
6.6.1	Controles de desarrollo de sistemas.....	60
6.6.2	Controles de gestión de seguridad .....	60
6.6.3	Controles de seguridad del ciclo de vida.....	60
<b>6.7</b>	<b>Controles de seguridad de la red .....</b>	<b>60</b>

6.8	Estampado cronológico .....	60
7	<b>AUDITORIA DE CONFORMIDAD Y OTROS CONTROLES .....</b>	<b>61</b>
7.1	Frecuencia o circunstancias de los controles.....	61
7.2	Identidad/cualificación del auditor.....	61
7.3	Relación entre el auditor y la entidad auditada .....	61
7.4	Aspectos cubiertos por los controles .....	61
7.5	Acciones que tomar como resultado de la detección de deficiencias .....	61
7.6	Comunicación de resultados .....	61
8	<b>OTROS ASUNTOS LEGALES Y COMERCIALES .....</b>	<b>61</b>
8.1	<b>Tarifas.....</b>	<b>61</b>
8.1.1	Tarifas de emisión o renovación de certificados.....	61
8.1.2	Tarifas de acceso a los certificados.....	62
8.1.3	Tarifas de revocación o acceso a la información de estado .....	62
8.1.4	Tarifas de otros servicios.....	63
8.1.5	Política de reembolso .....	63
8.2	<b>Responsabilidad .....</b>	<b>63</b>
8.3	<b>Imparcialidad.....</b>	<b>63</b>
8.4	<b>Exoneración de responsabilidad .....</b>	<b>64</b>
8.5	<b>Responsabilidades financieras y legales .....</b>	<b>64</b>
8.5.1	Otros bienes .....	64
8.5.2	Seguro o garantía de cobertura para suscriptores, responsables y terceros de buena fe.....	65
8.6	<b>Confidencialidad de la información .....</b>	<b>65</b>
8.6.1	Responsabilidad de proteger la información confidencial .....	65
8.6.2	Información confidencial.....	65
8.6.3	Información no confidencial.....	66
8.6.4	Deber de proteger la información confidencial.....	66
8.7	<b>Protección de la información personal .....</b>	<b>66</b>
8.7.1	Política de privacidad .....	66
8.7.2	Información tratada como privada.....	66
8.7.3	Información no calificada como privada .....	66
8.7.4	Responsabilidad de la protección de los datos de carácter personal .....	67
8.7.5	Notificación y consentimiento para usar datos de carácter personal.....	67
8.7.6	Revelación en el marco de un proceso administrativo o judicial .....	67
8.7.7	Otras circunstancias de revelación de información .....	67
8.7.8	Sistema de seguridad para proteger la información .....	67
8.8	<b>Derechos de propiedad intelectual .....</b>	<b>67</b>
8.9	<b>Obligaciones .....</b>	<b>68</b>
8.9.1	Obligaciones de la ECD GSE .....	68
8.9.2	Obligaciones de la RA .....	68
8.9.3	Obligaciones del suscriptor y/o responsable .....	69
8.9.4	Obligaciones de los Terceros de buena fe .....	70
8.9.5	Obligaciones de la Entidad (Cliente).....	70
8.9.6	Obligaciones de otros participantes .....	70
9	<b>Términos y condiciones de la DPC y PC .....</b>	<b>71</b>
9.1.1	Inicio de vigencia de la DPC y PC.....	71
9.1.2	Efectos de terminación e inicio de vigencia DPC y PC .....	72
9.1.3	Cambios que afectan la DPC y PC.....	72
9.1.4	Circunstancias bajo las cuales la OID debe cambiarse.....	72
10	<b>Políticas de Certificación para Certificados Digitales .....</b>	<b>72</b>
11	<b>ANEXO 1 PERFIL TÉCNICO CERTIFICADOS DIGITALES .....</b>	<b>73</b>
12	<b>ANEXO 2 – TÉRMINOS Y CONDICIONES .....</b>	<b>73</b>

## 1 INTRODUCCIÓN

### 1.1 Resumen

**La Declaración de Prácticas de Certificación (DPC)- Global Certification Authority Root GSE (en adelante DPC)** 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, declaraciones sobre las políticas y procedimientos que la **Entidad de Certificación Digital (en adelante ECD GSE)** como **Prestador de Servicios de Certificación digital (PSC)** aplica como lineamiento para prestar los servicios de certificación digital de acuerdo a lo establecido en la Ley 527 de 1999, el Decreto Ley 0019 de 2012, el Decreto 333 de 2014, el Decreto 1471 de 2014 y los reglamentos que los modifiquen o complementen, en el territorio de Colombia.

La DPC está conforme con los siguientes lineamientos:

- i. Criterios Específicos de Acreditación para las Entidades de Certificación Digital 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. La DPC está organizada bajo la estructura definida en el documento RFC3647 Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework de grupo de trabajo IETF - The Internet Engineering Task Force, (que sustituye a la RFC2527) <http://www.ietf.org/rfc/rfc3647.txt?number=3647>.
- iii. ETSI EN 319 411-2: “Policy Requirements for certification authorities issuing qualified certificates”.
- iv. ETSI EN 319 412-5: “Qualified Certificate Profile”.
- v. ETSI EN 319 411-3: “Policy Requirements for certification authorities issuing public key certificates”.

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

### DATOS DE GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.:

<b>Razón Social:</b>	GESTIÓN DE SEGURIDAD ELECTRÓNICA S.A.
<b>Sigla:</b>	GSE S.A.
<b>Número de Identificación Tributaria:</b>	900.204.272 - 8
<b>Registro Mercantil No:</b>	01779392
<b>Dirección:</b>	Calle 73 No. 7 – 31 Piso 7 Torre B.
<b>Ciudad / País:</b>	Bogotá D.C., Colombia.
<b>Teléfono:</b>	+57 (1) 5185158
<b>Fax:</b>	+57 (1) 5185158
<b>Correo electrónico:</b>	<a href="mailto:info@gse.co">info@gse.co</a>
<b>Página Web:</b>	<a href="http://www.gse.com.co">www.gse.com.co</a>





## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

### 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 DPC y sus políticas; son recibidas y atendidas directamente por GSE como ECD y serán resueltas por las personas pertinentes e imparciales o por los comités que tengan la competencia técnica necesaria, para lo cual se disponen de los siguientes canales para la atención a suscriptores, responsables y terceros.

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

Una vez presentado el caso, este es transmitido 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 Nombre del documento e identificación

La **DPC** para **ECD GSE** se denominará “Declaración de Prácticas de Certificación (DPC)- Global Certification Authority Root GSE Versión X. La versión cambia de acuerdo con las modificaciones sobre el mismo documento.

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

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

JERARQUIA OID	DESCRIPCION	NOMBRE
1.1.	ISO assigned OIDs	ISO(1)
1.3.	ISO Identified Organization	ORG(3)
1.3.6	US Department of Defense	DOD(6)
1.3.6.1.	OID assignments from	OID (1)
1.3.6.1.4	Internet Private	INTERNET(4)
1.3.6.1.4.1.3.6.1.4.1	IANA-registered Private Enterprises	ENTERPRISE(1)
1.3.6.1.4.1.3.6.1.4.1.31136	Enterprise number para GSE	GSE(31136)

De conformidad con esta jerarquía, la presente DPC se ha identificado con el OID: **1.3.6.1.4.1.31136.2.2**

### 1.4 Marco Jurídico.

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

#### 1.4.1 Mecanismo de Resolución de Diferencias.

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

- i. La prestación de los servicios de certificación digital descritos en esta DPC.
- ii. Durante la ejecución de los servicios contratados.
- iii. Por la interpretación del contrato, DPC y cualquier otro documento entregado por ECD GSE.

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

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

### 1.5 Definiciones y acrónimos

#### 1.5.1 Definiciones

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

**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 “Certificación 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 (CA).** 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.

**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.



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

**Suscriptor:** persona a cuyo nombre se expide un certificado.

**Tercero de buena fe:** persona o entidad diferente del suscriptor o responsable 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 suscriptor o responsable del certificado.

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

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

**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.



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

**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.

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

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

**Archivo confiable de datos:** Es el servicio que GSE ofrece a sus clientes por medio de una plataforma tecnológica. En esencia, consiste en un espacio de almacenamiento seguro y encriptado al cual se accede con credenciales o con un certificado digital. La documentación que se almacene en esta plataforma tendrá valor probatorio siempre y cuando este firmada digitalmente.

**Generación de firmas digitales:** Plataforma de firma electrónica y digital, accesible mediante certificado digital o usuario y contraseña, que permite a sus usuarios la firma electrónica y digital de un documento y su envío a un tercero usuario o no del servicio.

### 1.5.2 Acrónimos

**CA:** Certification Authority

**CA Sub:** Autoridad de Certificación Subordinada

**CP:** Política de Certificación (Certificate Policy)

**DPC:** Declaración de Prácticas de Certificación (Certificate Practice Statement)

**CRL:** Certificate Revocation List

**CSP:** Certification Service Provider

**DNS:** Domain Name System

**FIPS:** Federal Information Processing Standard

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

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

**HSM:** Módulo de seguridad criptográfico (Hardware Security Module)

**IEC:** International Electrotechnical Commission

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

**IP:** Internet Protocol

**ISO:** International Organization for Standardization

**LDAP:** Lightweight Directory Access Protocol

**OCSP:** Online Certificate Status Protocol.

**OID:** Object identifier (Identificador de objeto único)

**PIN:** Personal Identification Number

**PUK:** Personal Unlocking Key

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

**PKI:** Public Key Infrastructure (Infraestructura de Llave Pública)

**PKIX:** Public Key Infrastructure (X.509)

**RA:** Registration Authority

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

**URL:** Uniform Resource Locator

**VA:** Autoridad de validación (Validation Authority)

### 1.5.3 Estándares y Organismos de estandarización

**CEN:** Comité Europeo de Normalización

**CWA:** CEN Workshop Agreement

**ETSI:** European Telecommunications Standard Institute

**FIPS:** Federal Information Processing Standard

**IETF:** Internet Engineer Task Force

**PKIX:** Grupo de trabajo del IETF sobre PKI

**PKCS:** Public Key Cryptography Standards

**RFC:** Request For Comments

## 1.6 PKI participantes.

### 1.6.1 Autoridad de Certificación (CA).

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

**GSE** tiene como Autoridad de Certificación CA:

<b>Nombre:</b>	InDenova Sociedad Limitada
<b>Dirección:</b>	Dels Traginers 14 2º B, Pol. Ind. Vara de Quart 46014
<b>Ciudad / País:</b>	Valencia - España.
<b>Teléfono:</b>	+34 (96) 381 99 47
<b>Correo electrónico:</b>	info@indenova.com
<b>Página Web:</b>	www.indenova.com
<b>Datos Registrales:</b>	Registro Mercantil de Valencia, Tomo: 7818, Libro: 5114, Folio: 139, Sección: 8, Hoja: V 97187, Inscripción: 1.



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

C.I.F.: B-97458996

### 1.6.2 Autoridad de Registro (RA)

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

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

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

ECD GSE tiene como autoridad de registro RA:

<b>Nombre:</b>	GESTION DE SEGURIDAD ELECTRONICA S.A.
<b>Número de Identificación Tributaria:</b>	900.204.272 - 8
<b>Registro Mercantil No:</b>	01779392
<b>Naturaleza:</b>	Privada (Sociedad Anónima)
<b>Tipo de Empresa</b>	PyME
<b>Dirección:</b>	Calle 73 No. 7 – 31 Piso 7 Torre B
<b>Ciudad / País:</b>	Bogotá D.C., Colombia.
<b>Teléfono:</b>	+57 (1) 5185158
<b>Correo electrónico:</b>	<a href="mailto:info@gse.co">info@gse.co</a>
<b>Página Web:</b>	<a href="http://www.gse.co">www.gse.co</a>

### 1.6.3 Suscriptor y/o responsable

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

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

### 1.6.4 Responsable

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

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

### 1.6.5 Solicitante

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

### 1.6.6 Entidad a la cual se encuentra vinculado el suscriptor o responsable

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

### 1.6.7 Otros participantes

#### 1.6.7.1 Comité de Gerencia

El comité de Gerencia es un organismo interno de ECD GSE, conformado por el Director General y directores quienes tienen la responsabilidad de la aprobación de la DPC como documento inicial, así como autorizar los cambios o modificaciones requeridas sobre la DPC aprobada y autorizar su publicación.

#### 1.6.7.2 Proveedores de servicios de certificación

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

A efectos de esta DPC, la empresa INDENOVA SOCIEDAD LIMITADA en adelante inDenova será el proveedor y administrador de la infraestructura de la ECD GSE.

GSE tiene como entidad proveedor del servicio de certificación:

<b>Nombre:</b>	InDenova Sociedad Limitada
<b>Dirección:</b>	Dels Traginers 14 2º B, Pol. Ind. Vara de Quart 46014
<b>Ciudad / País:</b>	Valencia - España.
<b>Teléfono:</b>	+34 (96) 381 99 47
<b>Correo electrónico:</b>	info@indenova.com
<b>Página Web:</b>	www.indenova.com
<b>Datos Registrales:</b>	Registro Mercantil de Valencia, Tomo: 7818, Libro: 5114, Folio: 139, Sección: 8, Hoja: V 97187, Inscripción: 1.
<b>C.I.F.:</b>	B-97458996

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

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

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



### 1.6.7.3 Entidades de Certificación Digital Recíprocas

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

Actualmente ECD GSE no cuenta con acuerdos vigentes de reciprocidad.

## 1.7 Administración de la DPC y PC

### 1.7.1 Organización administradora del documento

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

#### 1.7.2 Persona de contacto:

**Nombre:** Luis Fernando Mora Navarro  
**Cargo:** Representante Legal  
**Dirección:** Calle 73 No. 7 – 31 Piso 7 Torre B  
**Domicilio:** Bogotá D.C., Colombia.  
**Teléfono:** +57 (1) 5185158  
**Correo electrónico:** [info@gse.co](mailto:info@gse.co)

#### 1.7.3 Persona o área que determina la adecuación de las Políticas a la DPC.

**Area encargada:** Gerente de operaciones ECD  
**Dirección:** Calle 73 No. 7 – 31 Piso 7 Torre B  
**Domicilio:** Bogotá D.C., Colombia.  
**Teléfono:** +57 (1) 5185158  
**Correo electrónico:** [info@gse.co](mailto:info@gse.co)

#### 1.7.4 Procedimientos de aprobación de la DPC

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

## 1.8 Cambios que afecten los servicios de certificación digital

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

- Por cambios normativos en la legislación para ECD.

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

### 1.8.1 Procedimiento para los cambios

#### 1.8.1.1 Cambios que no requieren notificación

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

#### 1.8.1.2 Cambios que requieren notificación

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

### 1.8.2 Mecanismo y periodo de notificación

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

- a. El Comité de Gerencia y el Equipo de Calidad de la ECD GSE considere que los cambios a los servicios de certificación digital afectan el funcionamiento y aceptabilidad de los mismos.
- b. Los cambios introduzcan nuevos requisitos para la prestación de los servicios de certificación digital por actualizaciones tecnológicas o cambios normativos que afecten los servicios.

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

## 2 RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

### 2.1 Repositorios



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

- **Certificado Raíz ECD GSE**  
[http://certs.gse.co/root/crt\\_root\\_gse\\_sha2.crt](http://certs.gse.co/root/crt_root_gse_sha2.crt)
- **Lista de Certificados Revocados Raíz ECD GSE (CRL)**  
[http://crl.gse.co/root/crl\\_root\\_gse\\_sha2.crl](http://crl.gse.co/root/crl_root_gse_sha2.crl)
- **Certificados Subordinadas ECD GSE**  
[http://certs.gse.co/sub/crt\\_gse\\_sub001co\\_sha2.crt](http://certs.gse.co/sub/crt_gse_sub001co_sha2.crt)  
[http://certs.gse.co/sub/crt\\_gse\\_sub001pe\\_sha2.crt](http://certs.gse.co/sub/crt_gse_sub001pe_sha2.crt)
- **Certificados Subordinadas TSA GSE**  
[http://certs.gse.co/tsa/crt\\_tsa001co\\_gse\\_sha2.crt](http://certs.gse.co/tsa/crt_tsa001co_gse_sha2.crt)  
[http://certs.gse.co/tsa/crt\\_tsa001pe\\_gse\\_sha2.crt](http://certs.gse.co/tsa/crt_tsa001pe_gse_sha2.crt)
- **Lista de Certificados Revocados Subordinadas ECD GSE (CRL)**  
[http://crl.gse.co/root/crl\\_root\\_gse\\_sha2.crl](http://crl.gse.co/root/crl_root_gse_sha2.crl)
- **Certificado Unidad de Estampado Cronológico TSA GSE**  
[http://certs.gse.co/GSE\\_TSU001\\_CO.crt](http://certs.gse.co/GSE_TSU001_CO.crt)  
[http://certs.gse.co/GSE\\_TSU001\\_PE.crt](http://certs.gse.co/GSE_TSU001_PE.crt)
- **Lista de Certificados Revocados certificados de entidad final de Subordinada (CRL)**  
[http://crl.gse.co/sub/crl\\_gse\\_sub001co\\_sha2.crl](http://crl.gse.co/sub/crl_gse_sub001co_sha2.crl)  
[http://crl.gse.co/sub/crl\\_gse\\_sub001pe\\_sha2.crl](http://crl.gse.co/sub/crl_gse_sub001pe_sha2.crl)
- **Declaración de Prácticas de Certificación (DPC)- Global Certification Authority Root GSE**  
[http://cps.gse.co/sub/cps\\_sub001co\\_ca\\_gse.pdf](http://cps.gse.co/sub/cps_sub001co_ca_gse.pdf)
- **Validación en línea de Certificados Digitales**  
<http://ocsp.gse.co>  
[http://certs.gse.co/GSE\\_OCSP001\\_CO.crt](http://certs.gse.co/GSE_OCSP001_CO.crt)  
[http://certs.gse.co/GSE\\_OCSP001\\_PE.crt](http://certs.gse.co/GSE_OCSP001_PE.crt)  
[http://certs.gse.co/GSE\\_OCSP002\\_CO.crt](http://certs.gse.co/GSE_OCSP002_CO.crt)  
[http://certs.gse.co/GSE\\_OCSP002\\_PE.crt](http://certs.gse.co/GSE_OCSP002_PE.crt)

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

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

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



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

### 2.2 Publicación de la información de certificación

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

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

### 2.3 Plazo o frecuencia de la publicación

#### Certificado Raíz

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

#### Certificado Subordinada

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

#### Lista de Certificados Revocados (CRL)

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

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

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

#### Validación en línea de Certificados Digitales

ECD GSE publicará los certificados emitidos en un repositorio en formato X.509 V3 los cuales podrán ser consultados en la dirección <http://ocsp.gse.co>

### 2.4 Controles de acceso a los repositorios

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

### 3 IDENTIFICACIÓN Y AUTENTICACIÓN

#### 3.1 Nombres

##### 3.1.1 Tipos de nombres

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

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

##### 3.1.1.1 Certificado raíz de ECD GSE

El DN del ‘issuer name’ del certificado raíz, tiene los siguientes campos y valores fijos:

C = CO  
L = BOGOTÁ, D.C.  
STREET = <https://www.gse.co>  
OU = Internet Certification Authority <http://www.gse.co>  
SERIALNUMBER = 9002042728  
O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE  
CN = Global Certification Authority Root GSE  
E = [ca@gse.co](mailto:ca@gse.co)

En el DN del ‘subject name’ se incluyen los siguientes campos:

C = CO  
L = BOGOTÁ, D.C.  
STREET = <https://www.gse.co/address>  
OU = Internet Certification Authority <http://www.gse.co>  
SERIALNUMBER = 9002042728  
O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE  
CN = Global Certification Authority Root GSE  
E = [ca@gse.co](mailto:ca@gse.co)

##### 3.1.1.2 Certificados de las Subordinadas de ECD GSE

El DN del ‘issuer name’ de los certificados de las subordinadas de ECD GSE, tienen las siguientes características:

C = CO  
L = BOGOTÁ, D.C.



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

STREET = <https://www.gse.co/address>  
OU = Internet Certification Authority <http://www.gse.co>  
SERIALNUMBER = 9002042728  
O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE  
CN = Global Certification Authority Root GSE  
E = [ca@gse.co](mailto:ca@gse.co)

En el DN del 'subject name' se incluyen los siguientes campos:

C = CO  
L = Localidad de Operación de la Subordinada  
STREET = <http://www.gse.co/address>  
OU = Internet Certification Authority <http://www.gse.co>  
T = Subordinate Certificate  
O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE  
E = [ca@gse.co](mailto:ca@gse.co)  
SERIALNUMBER = 9002042728  
CN = Nombre distintivo de la Subordinada.  
Description = GSE Subordinate Certificate X Y HW-KUSU, X = Consecutivo, Y = Pais.

### **3.1.1.2.1 Certificado GSE Timestamping Certificate 001 Colombia**

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](mailto:tsa@gse.co)  
SERIALNUMBER = 9002042728  
CN = GSE TSA001\_CO  
Description = GSE Timestamping Certificate 001 Colombia HW-KUSU

### **3.1.1.2.2 Certificado GSE Timestamping Certificate 001 Perú**

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](mailto:tsa@gse.co)  
SERIALNUMBER = 9002042728



## Declaración de prácticas de certificación

Fecha de vigencia  
12/04/2019

Versión  
5

CN = GSE TSA001\_PE  
Description = GSE Timestamping Certificate 001 Perú HW-KUSU

### **3.1.1.2.3 Certificado GSE Subordinate Certificate 001 Colombia HW-KUSU**

C = CO  
L = BOGOTÁ, D.C.  
STREET = <http://www.gse.co/address>  
OU = Internet Certification Authority <http://www.gse.co>  
T = Subordinate Certificate  
O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE  
E = [ca@gse.co](mailto:ca@gse.co)  
SERIALNUMBER = 9002042728  
CN = GSE SUB001\_CO  
Description = GSE Subordinate Certificate 001 Colombia HW-KUSU

### **3.1.1.2.4 Certificado GSE Subordinate Certificate 001 Perú HW-KUSU**

C = CO  
L = BOGOTÁ, D.C.  
STREET = <http://www.gse.co/address>  
OU = Internet Certification Authority <http://www.gse.co>  
T = Subordinate Certificate  
O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE  
E = [ca@gse.co](mailto:ca@gse.co)  
SERIALNUMBER = 9002042728  
CN = GSE SUB001\_PE  
Description = GSE Subordinate Certificate 001 Perú HW-KUSU

### **3.1.1.2.5 Certificados de suscriptor de ECD GSE**

El DN del 'issuer name' de los certificados de suscriptor de ECD GSE, tienen las siguientes características generales:

C = CO  
L = BOGOTÁ, D.C.  
STREET = <http://www.gse.co/address>  
OU = Internet Certification Authority <http://www.gse.co>  
T = Subordinate Certificate  
O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE  
E = [ca@gse.co](mailto:ca@gse.co)  
SERIALNUMBER = 9002042728  
CN = GSE SUB001\_CO  
Description = GSE Subordinate Certificate 001 Colombia HW-KUSU

En el DN del 'subject name' se incluyen como mínimo los siguientes campos:

CN=<APELLIDO1> <APELLIDO2> <NOMBRE1> <NOMBRE2>  
GN=<NOMBRE1> <NOMBRE2>  
SN=<APELLIDO1> <APELLIDO2>  
NUMERO DE SERIE=<Número del documento de Identificación>

La descripción de los DN para cada tipo de certificado cubiertos por esta DPC.

### 3.1.2 Nombres Distintivos.

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

### 3.1.3 Anonimato y pseudoanonimato del suscriptor o responsables

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

### 3.1.4 Reglas para la interpretación de varias formas de nombre

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

### 3.1.5 Singularidad de los nombres

El DN de los certificados digitales emitidos es único.

### 3.1.6 Reconocimiento, autenticación y papel de las marcas reconocidas

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

## 3.2 Validación inicial de la identidad

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

### 3.2.1 Método para demostrar la posesión de la llave privada

Para garantizar la emisión, posesión y control de la llave privada por parte del suscriptor o responsable, se hace entrega directamente al suscriptor o responsable o persona autorizada por el mismo, en un dispositivo



criptográfico seguro token o “*Hardware Security Module (HSM)*”, de generación segura de llaves y transmitida mediante un canal seguro.

### 3.2.2 Autenticación de la identidad de una entidad (Persona jurídica)

Para asegurar la identidad de una persona jurídica, RA GSE exige la presentación del documento oficial que acredite la existencia legal de la misma y su representante legal o apoderados quienes serán las únicas personas que puedan solicitar el certificado digital a nombre de dicha organización.

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

### 3.2.3 Autenticación de una identidad individual (Persona Natural)

Para asegurar la identidad de una persona natural, RA GSE, exige la presentación de copia del documento de identidad del suscriptor y verifica su existencia y correspondencia contra bases de datos propias o de terceros, sean oficiales o privadas. Cuando el servicio es solicitado por un menor de edad, su identidad será asegurada con la fotocopia autenticada de la tarjeta de identidad

### 3.2.4 Información de suscriptor o responsable no verificada

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

### 3.2.5 Criterios para la interoperabilidad

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

## 3.3 Identificación y autenticación para peticiones de renovación de llaves

### 3.3.1 Identificación y autenticación para renovación.

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

### 3.3.2 Identificación y autenticación tras una revocación

Debido a que una revocación implica la expedición de un nuevo certificado, ECD GSE, realiza un nuevo proceso de autenticación del solicitante.

## 3.4 Identificación y autenticación para peticiones de revocación

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

#### 4 Requisitos operacionales para el tiempo de vida de los certificados

##### 4.1 Solicitud del certificado

Cualquier persona que requiera la prestación del servicio de certificación digital, debe diligenciar el formulario de solicitud de certificado digital publicado en la página Web o enviado al correo electrónico del solicitante, aceptar el documento términos y condiciones de la ECD y aportarlos junto con la documentación requerida para autenticar la información suministrada. Una vez completada y confirmada la información por parte del solicitante, el formulario de solicitud es enviado a la Autoridad de Registro quien se encargará de validar la información suministrada y aprobarla de conformidad con el cumplimiento de los requisitos exigidos para cada tipo de certificado.

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

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

El solicitante aporta los documentos necesarios y se surten los procedimientos establecidos por ECD GSE, para la obtención de su certificado digital.

ECD GSE, se reserva el derecho de solicitar documentos adicionales a los exigidos en el formulario de solicitud, 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 de certificado digital cuando a su juicio se pueda poner en riesgo la credibilidad, valor comercial, buen nombre de GSE o idoneidad legal o moral de todo el sistema de certificación digital, notificando la no aprobación.

##### 4.1.1 Quién puede solicitar un certificado

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

##### 4.1.2 Proceso de registro y responsabilidades

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

##### 4.2 Uso del certificado



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

### 4.2.1 Usos adecuados del certificado

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

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

- **Identificación del Suscriptor:** El Suscriptor del Certificado Digital puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado Digital.
- **Integridad del documento firmado:** La utilización del Certificado Digital para aplicar firmas digitales garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Suscriptor. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Suscriptor.
- **No repudio de origen:** Con el uso de este Certificado Digital también se garantiza que la persona que firma digitalmente el documento no puede repudiarlo, es decir, el Suscriptor que ha firmado no puede negar la autoría o la integridad del mismo.

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

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

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

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

### 4.2.2 Usos prohibidos del certificado y exclusión de responsabilidad

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

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

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

### 4.3 Tramitación de solicitud de certificados

#### 4.3.1 Realización de las funciones de identificación y autenticación

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

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

#### 4.3.2 Aprobación o rechazo de las solicitudes de certificado

Si una vez verificada la identidad del solicitante, la información suministrada cumple con los requisitos establecidos por esta DPC, se aprueba la solicitud. Si no es posible la identificación plena de la identidad del suscriptor o no existe autenticidad plena de la información suministrada, se niega la solicitud y no se emite el certificado. ECD GSE no asume ninguna responsabilidad por las consecuencias que puedan derivarse de la no aprobación de la emisión de un certificado digital y así lo acepta y reconoce el solicitante al que le haya sido negada la expedición del respectivo certificado.

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

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

### 4.3.3 Plazo para procesar las solicitudes de certificado

El plazo para la aprobación de una solicitud por parte de la RA de GSE, es de uno a cinco días hábiles desde el momento de recibir la documentación e información completa. El tiempo de entrega del certificado digital posterior a la emisión, depende del lugar de destino, sin exceder los ocho (8) días hábiles.

## 4.4 Emisión de certificados

### 4.4.1 Actuaciones de la ECD GSE durante la emisión de certificados

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

La RA de GSE genera la documentación formal de la certificación digital:

- a) Cuando se ha tomado la decisión de otorgar el certificado digital;
- b) Se ha completado/firmado el acuerdo de Certificación Digital.

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

### 4.4.2 Notificación al solicitante por la ECD GSE de la emisión del certificado

Mediante correo electrónico se notifica al suscriptor la emisión de su certificado digital y por consiguiente el suscriptor acepta y reconoce que una vez reciba el citado correo electrónico, se entenderá entregado el certificado. Se entenderá que se ha recibido el correo electrónico donde se notifica la emisión de un certificado, cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección de correo electrónico que el suscriptor reporto en el formulario de solicitud.

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

### 4.4.3 Notificación de la emisión del certificado por la ECD a otras entidades

No aplica.

## 4.5 Aceptación del certificado

### 4.5.1 Forma en la que se acepta el certificado

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

## 4.6 Uso de la llave privada y del certificado

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

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

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

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

En este sentido deberá:

- Comprobar que el certificado asociado no incumple las fechas de inicio y final de vigencia.
- Comprobar que el certificado asociado a la llave privada no está revocado.
- Comprobar que la huella digital (**fingerpint**) del certificado de la ECD raíz y la del certificado de la subordinada de ECD GSE coinciden con el publicado por GSE en su página Web.
  - Huella digital (fingerprint) del certificado de la ECD raíz:  
  
ec b1 fc 57 84 ee 97 27 51 c1 5a 7a b2 ee a1 52 85 27 31 62  
[http://certs.gse.co/root/crt\\_root\\_gse\\_sha2.crt](http://certs.gse.co/root/crt_root_gse_sha2.crt)
  - Huella digital (fingerprint) del certificado de la subordinada de ECD GSE Timestamping Certificate 001 Colombia:  
  
0d f7 68 36 0d a8 3e cc 3a cd 42 73 29 95 a9 b3 f3 6d da 0f  
[http://certs.gse.co/tsa/crt\\_tsa001co\\_gse\\_sha2.crt](http://certs.gse.co/tsa/crt_tsa001co_gse_sha2.crt)
  - Huella digital (fingerprint) del certificado de la subordinada de ECD GSE Subordinate Certificate 001 Colombia:  
  
98 b2 ce 98 5d 62 fb a4 f3 e4 8f 52 76 63 14 22 4c b6 88 b8  
[http://certs.gse.co/sub/crt\\_gse\\_sub001co\\_sha2.crt](http://certs.gse.co/sub/crt_gse_sub001co_sha2.crt)

### 4.7 Renovación del certificado sin cambio de llaves

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

#### 4.7.1 Circunstancias para la renovación de certificados sin cambio de llaves

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

#### 4.7.2 Quién puede solicitar una renovación sin cambio de llaves

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

#### 4.7.3 Trámites para la solicitud de renovación de certificados sin cambio de llaves

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

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

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

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

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

#### 4.7.6 Publicación del certificado renovado por la ECD sin cambio de llaves.

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

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

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

### 4.8 Renovación del certificado con cambio de llaves

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

#### 4.8.1 Circunstancias para la renovación de certificados con cambio de llaves.

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

#### 4.8.2 Quién puede solicitar una renovación con cambio de llaves.

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

**4.8.3 Trámites para la solicitud de renovación de certificados con cambio de llaves.**

El procedimiento para renovación de certificados digitales es igual al procedimiento de solicitud de un certificado nuevo. El suscriptor tiene que ingresar a la página Web, descargar el formulario de solicitud e iniciar el proceso de solicitud de renovación del certificado de la misma forma que lo hizo cuando solicitó el certificado por primera vez. Igualmente, ECD GSE atenderá los requerimientos de renovación cuando sea solicitado por el suscriptor a través del diligenciamiento y envío del formulario respectivo firmado digitalmente por dicho suscriptor haciendo uso del certificado del que sea suscriptor o responsable siempre y cuando el mismo se encuentre vigente. Su información será nuevamente validada con el fin de actualizar datos si se requiere.

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

Mediante correo electrónico se informa al suscriptor la emisión de su certificado digital y por consiguiente el solicitante acepta y reconoce que una vez reciba el citado correo electrónico se entenderá entregado el certificado. Se entenderá que se ha recibido el correo electrónico donde se notifica la emisión de un certificado cuando dicho correo ingrese en el sistema de información designado por el solicitante, esto es en la dirección correo electrónico que consta en el formulario de solicitud.

**4.8.5 Forma en la que se acepta la renovación de un certificado**

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

**4.8.6 Publicación del certificado renovado por la ECD con cambio de llaves.**

No aplica por cuanto ECD GSE no publica los certificados.

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

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

**4.9 Modificación de certificados**

Los certificados digitales emitidos por ECD GSE, no pueden ser modificados. A cambio el suscriptor debe solicitar la emisión de uno nuevo. En este evento se expedirá un nuevo certificado al suscriptor, el costo de esta modificación será asumido completamente por el suscriptor conforme a las tarifas informadas por ECD GSE.

**4.9.1 Circunstancias para la modificación de un certificado**

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

**4.9.2 Quién puede solicitar una modificación**

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



### 4.9.3 Trámites para la solicitud de modificación de un certificado

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

### 4.9.4 Notificación al suscriptor o responsable de la emisión de un nuevo certificado

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

### 4.9.5 Forma en la que se acepta la modificación de un certificado

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

### 4.9.6 Publicación del certificado modificado por la ECD

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

### 4.9.7 Notificación de la emisión de un certificado por la ECD a otras entidades

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

## 4.10 Revocación y suspensión de certificados

### 4.10.1 Circunstancias para la revocación de un certificado.

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

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

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

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

- A petición del suscriptor, responsable o un tercero en su nombre y representación.
- Por muerte del suscriptor o responsable.
- Por liquidación en el caso de las personas jurídicas (entidad) representadas en la información del certificado digital.
- Por la confirmación o evidencia de que alguna información o hecho contenido en el certificado digital es falso.
- La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometida de manera material que afecte la confiabilidad del certificado.
- 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 suscriptor o responsable.
- j. Por liquidación de la persona jurídica representada que consta en el certificado digital.
- k. Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
- l. Por pérdida o inutilización del dispositivo criptográfico que haya sido entregado por ECD GSE.
- m. Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato.
- n. Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la confiabilidad del certificado digital.
- o. Por el manejo indebido por parte del suscriptor del certificado digital.
- p. Por el incumplimiento del suscriptor o de la persona jurídica que representa o a la que está vinculado a través del documento términos y condiciones o responsable de certificados digitales de la ECD GSE.
- q. 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.
- r. En cualquier momento que se evidencie falsedad en los datos suministrados por el solicitante, suscriptor o responsable.
- s. Por incumplimiento por parte de la ECD GSE, el suscriptor o responsable de las obligaciones establecidas en la DPC.
- t. Por incumplimiento en el pago de los valores por los servicios de certificación, acordados entre el solicitante y ECD GSE.

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

#### 4.10.2 Quién puede solicitar una revocación

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

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

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

El equipo de TI de la CA y la RA como máximo ente de control que tiene atribuida la administración de la seguridad de la infraestructura tecnológica de ECD GSE, está en capacidad de solicitar la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la llave privada del suscriptor,

responsable o cualquier otro hecho que tienda al uso indebido de llave privada del suscriptor, responsable o de la ECD GSE.

#### 4.10.3 Procedimiento de solicitud de revocación

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

- En las oficinas de GSE.  
En horario de atención al público se reciben las solicitudes escritas de revocación de certificados digitales firmadas por los suscriptores y/ responsables.
- Servicio de Revocación telefónica.  
A través de la línea de atención telefónica permanente, los suscriptores y responsables pueden solicitar la revocación siempre y cuando envíen un oficio formal con la solicitud de revocación.
- Servicio de Revocación vía correo electrónico  
Por medio de nuestro correo electrónico [area.operaciones@gse.co](mailto:area.operaciones@gse.co), los suscriptores y responsables pueden solicitar la revocación de certificados digitales conforme a las causales de revocación mencionadas en el apartado Circunstancias para la revocación de un certificado de esta DPC.

#### 4.10.4 Periodo de gracia de solicitud de revocación

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

El procedimiento utilizado por ECD GSE para verificar la autenticidad de una solicitud de revocación formulada por una persona determinada, es verificar la solicitud 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 revocación del certificado, si se evidencia que dicho certificado es utilizado vinculado con la llave privada, el suscriptor o responsable releva de toda responsabilidad legal a ECD GSE, toda vez que reconoce y acepta que el control, custodia y confidencialidad de la llave privada es responsabilidad exclusiva de este.

#### 4.10.5 Plazo en el que la ECD debe resolver la solicitud de revocación

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

Una vez cumplidas las formalidades previstas para la revocación y si por alguna razón, no se hace efectiva la revocación de un certificado en los términos establecidos por esta DPC, ECD GSE como prestador de servicios de certificación responderá por los perjuicios que se causen a los suscriptores o terceros de buena



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

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

### 4.10.6 Requisitos de verificación de las revocaciones por los terceros de buena fe

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

### 4.10.7 Frecuencia de emisión de las CRLs

Cada vez que se produzca una revocación de un certificado, ECD GSE generará y publicará una nueva CRL de manera inmediata en su repositorio y a pesar de que no se produzca ninguna revocación cada veinticuatro (24) horas se generará y publicará una nueva CRL con una disponibilidad de consulta en línea 7x24x365, 99.9% uptime por año.

### 4.10.8 Tiempo máximo de latencia de las CRLs

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

### 4.10.9 Revocación on-line/disponibilidad de verificación del estado

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

### 4.10.10 Requisitos de comprobación de la revocación on-line

Para obtener la información del estado de revocación de un certificado en un momento dado, se puede hacer la consulta en línea en la dirección <http://ocsp.gse.co>, para lo cual se debe contar con un software que sea capaz de operar con el protocolo RFC2560. La mayoría de navegadores ofrecen este servicio.

### 4.10.11 Notificación de la revocación de un certificado

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

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

### 4.10.12 Otras formas disponibles de divulgación de información de revocación

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

### 4.10.13 Requisitos especiales de renovación de llaves comprometidas

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

### 4.10.14 Circunstancias para la suspensión

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

#### 4.10.14.1 Quién puede solicitar la suspensión

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

#### 4.10.14.2 Procedimiento de solicitud de suspensión

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

#### 4.10.14.3 Límites del periodo de suspensión

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

## 4.11 Perfiles de certificados

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

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

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

### 4.11.1 Descripción del contenido de los certificados GSE Subordinate Certificate 001 Colombia

Campo	Valor o restricciones
Versión	V3 (X.509 versión 3)
Número de Serie	Identificador único emitido por ECD GSE
Algoritmo de Firma	SHA2RSA
Emisor	Ver sección "Reglas para la interpretación de varias formas de nombre". Para ECD GSE como emisor se especifica: ca@gse.co GSE SUB001_CO GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE 9002042728 Internet Certification Authority <a href="http://www.gse.co">http://www.gse.co</a> Subordinate Certificate <a href="http://www.gse.co/address">http://www.gse.co/address</a> BOGOTÁ, D.C. CO GSE Subordinate 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 la 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 CRÍTICO.
Punto de distribución de la CRL	Es usado para indicar las direcciones donde se encuentra publicada la CRL de ECD GSE. En el certificado de la ECD Raíz, este atributo no se especifica.
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.



## Declaración de prácticas de certificación

Fecha de vigencia  
12/04/2019

Versión  
5

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.

### 4.11.2 Descripción del contenido de los certificados GSE Subordinate Certificate 001 Perú

Campo	Valor o restricciones
Versión	V3 (X.509 versión 3)
Número de Serie	Identificador único emitido por ECD GSE
Algoritmo de Firma	SHA2RSA
Emisor	Ver sección "Reglas para la interpretación de varias formas de nombre". Para ECD GSE como emisor se especifica: C = CO L = BOGOTÁ, D.C. STREET = http://www.gse.co/address OU = Internet Certification Authority http://www.gse.co T = Subordinate Certificate O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE E = ca@gse.co SERIALNUMBER = 9002042728 CN = GSE SUB001_PE Description = GSE Subordinate Certificate 001 Perú 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 la 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 CRÍTICO.



## Declaración de prácticas de certificación

Fecha de vigencia  
12/04/2019

Versión  
5

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.

### 4.11.3 Descripción del contenido de los certificados GSE Timestamping Certificate 001 Colombia

Campo	Valor o restricciones
Versión	V3 (X.509 versión 3)
Número de Serie	Identificador único emitido por ECD GSE
Algoritmo de Firma	SHA2RSA
Emisor	Ver sección "Reglas para la interpretación de varias formas de nombre". Para ECD GSE como emisor se especifica: C = CO L = BOGOTÁ, D.C. STREET = <a href="http://www.gse.co/address">http://www.gse.co/address</a> OU = Trusted Timestamp Service <a href="http://www.gse.co">http://www.gse.co</a> T = Service Timestamping O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE E = <a href="mailto:tsa@gse.co">tsa@gse.co</a> 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 la 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 CRÍTICO.
Punto de distribución de la CRL	Es usado para indicar las direcciones donde se encuentra publicada la CRL de ECD GSE. En el certificado de la ECD Raíz, este atributo no se especifica.
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.

#### 4.11.4 Descripción del contenido de los certificados GSE Timestamping Certificate 001 Perú.

Campo	Valor o restricciones
Versión	V3 (X.509 versión 3)
Número de Serie	Identificador único emitido por ECD GSE
Algoritmo de Firma	SHA2RSA
Emisor	Ver sección "Reglas para la interpretación de varias formas de nombre". Para ECD GSE como emisor se especifica: C = CO L = BOGOTÁ, D.C. STREET = <a href="http://www.gse.co/address">http://www.gse.co/address</a> OU = Trusted Timestamp Service <a href="http://www.gse.co">http://www.gse.co</a> T = Service Timestamping O = GESTION DE SEGURIDAD ELECTRONICA S.A. - GSE E = tsa@gse.co SERIALNUMBER = 9002042728 CN = GSE TSA001_PE Description = GSE Timestamping Certificate 001 Perú 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 la 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 CRÍTICO.
Punto de distribución de la CRL	Es usado para indicar las direcciones donde se encuentra publicada la CRL de ECD GSE. En el certificado de la ECD Raíz, este atributo no se especifica.
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.

#### 4.11.4.1 Número de versión

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

#### 4.11.4.2 Extensiones del certificado

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

#### 4.11.4.3 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".

#### 4.11.4.4 Extensión de política de certificados

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

#### 4.11.4.5 Nombre alternativo del sujeto

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

#### 4.11.4.6 Restricciones básicas

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

#### 4.11.4.7 Uso extendido de la llave

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

OID	Descripción	Tipos de Certificados
1.3.6.1.5.5.7.3.1	Autenticación de Servidor	Autenticación Agente Electrónico
1.3.6.1.5.5.7.3.2	Autenticación del Cliente	Autenticación persona Natural. Firma digital. Agente electrónico.
1.3.6.1.5.5.7.3.4	Protección de correo.	Firma Digital de persona natural y Agente Electrónico
1.3.6.1.5.5.7.3.8	Sellado de tiempo	Sellado de tiempo
1.3.6.1.4.1.311.20.2.2	Smart Card Logon	Autenticación Persona Natural.

#### 4.11.4.8 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

#### 4.11.4.9 Formatos de nombres.

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

#### 4.11.4.10 Restricciones de los nombres.

Los nombres se deben escribir en mayúsculas y sin tildes.

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

### 4.11.4.11 Identificador de objeto de la Política de Certificación

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

### 4.11.4.12 Uso de la extensión Policy Constrains

No se estipula.

### 4.11.4.13 Sintaxis y semántica de los Policy Qualifiers

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

### 4.11.4.14 Tratamiento semántico para la extensión Certificate Policies

No se estipula.

## 4.12 Servicios de información del estado de certificados

### 4.12.1.1 Perfil de CRL

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

### 4.12.1.2 Número de versión

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

### 4.12.1.3 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).

### 4.12.1.4 Disponibilidad CRL

Conforme a lo indicado en el numeral 4.10.9 Revocación on-line/disponibilidad de verificación del estado

### 4.12.1.5 Perfil OCSP

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

### 4.12.1.6 Número de versión

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

### 4.12.1.7 Extensiones OCSP

No aplica.



## Declaración de prácticas de certificación

Fecha de vigencia  
12/04/2019

Versión  
5

### 4.12.1.8 Disponibilidad OCSP

Conforme a lo indicado en el numeral 4.10.9 Revocación on-line/disponibilidad de verificación del estado

### 4.12.2 Características operacionales

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

### 4.12.3 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 o consulta a la CRL publicada en el portal <https://gse.com.co/productos/>

### 4.13 Finalización de la vigencia de un certificado

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

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

### 4.14 Custodia y recuperación de llaves

#### 4.14.1 Almacenamiento de la clave privada del suscriptor.

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

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

#### 4.14.2 Almacenamiento de la clave privada a un responsable.

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



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

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

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

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

### 4.14.3 Prácticas y políticas de custodia y recuperación de llaves

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

### 4.14.4 Prácticas y políticas de custodia y recuperación de la clave de sesión

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

## 5 CONTROLES FÍSICOS DE LA INSTALACION, GESTIÓN Y OPERACIONALES

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

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

#### 5.1.1 Ubicación física y construcción

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

Dicho proveedor cuenta con procedimientos para realizar las operaciones de administración de la infraestructura de ECD GSE y a donde únicamente tiene acceso el personal autorizado.

Esta área restringida cumple con los siguientes requisitos:

- a. Ingresan únicamente personas autorizadas.
- b. Los equipos de misión crítica están debidamente protegidos en racks.

- c. No posee ventanas hacia el exterior del edificio.
- d. Cuenta con un circuito cerrado de televisión las 24 horas, con cámaras tanto al interior como al exterior del centro de cómputo.
- e. Cuenta con control de acceso.
- f. Sistemas de protección y prevención de incendios: detectores de humo, sistema de extinción de incendios.
- g. Cuenta con personal capacitado para actuar ante eventos catastróficos
- h. Cuenta con un sistema detector de intrusos
- i. El cableado está debidamente protegido contra daños, intentos de sabotaje o interceptación por medio de canaletas.
- j. Está separado de áreas de carga y descarga.
- k. No existe tránsito frecuente de personas por los alrededores.

### 5.1.2 Acceso físico

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

### 5.1.3 Alimentación eléctrica y aire acondicionado

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

### 5.1.4 Exposición al agua

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

### 5.1.5 Prevención y protección de incendios

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

### 5.1.6 Sistema de almacenamiento

Se cuenta con procedimientos de toma de backups, restauración y pruebas de los mismos. Los medios magnéticos son almacenados en sitios seguros de acceso restringido. Una copia reposa dentro de las instalaciones y otra en un sitio externo.

### 5.1.7 Eliminación del material de almacenamiento de la información

Todo documento en papel que contenga información sensible de la entidad y que ha cumplido su vida útil deberá ser destruido físicamente para garantizar la imposibilidad de recuperación de información. Si el

documento o información está almacenado en un medio magnético se debe formatear, borrar permanentemente o destruir físicamente el dispositivo en casos extremos como daños de dispositivos de almacenamiento o dispositivos no reutilizables, siempre garantizando que no sea posible la recuperación de la información por cualquier medio conocido o no conocido por el momento.

### 5.1.8 Backup fuera de la instalación

ECD GSE mantendrá una copia de respaldo de las bases de datos en custodia fuera de las instalaciones.

## 5.2 Controles de procedimiento

### 5.2.1 Roles de confianza

Para la operación del sistema se han definido los siguientes roles dentro del sistema de emisión de certificados digitales:

- **Operador RA:** Persona encargada de recibir, verificar, firmar y decidir sobre la emisión de certificados digitales de la ECD GSE.
- **Administrador RA:** Persona encargada de la administración de usuarios en la plataforma PKI.
- **Registrador RA:** Persona encargada de llevar a cabo los procesos de validación y verificación de identidad de los posibles suscriptores o responsables de certificados emitidos por ECD GSE. y validaciones de solicitudes de otros servicios de certificación digital.

### 5.2.2 Número de personas requeridas por tarea

Para cada uno de los roles mencionados se requiere una persona.

La ECD garantiza al menos la colaboración de dos personas para realizar las tareas que afectan a la gestión de claves criptográficas de la propia ECD.

### 5.2.3 Identificación y autenticación para cada rol

El Operador RA, Administrador RA, Registrador RA se autentican mediante certificados digitales emitidos por ECD GSE.

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

El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales, tarjetas de acceso físico y llaves.

### 5.2.4 Roles que requieren segregación de funciones

El rol de Administrador RA, Operador RA y Registrador RA son incompatibles.

## 5.3 Controles de personal



### 5.3.1 Requisitos sobre la cualificación, experiencia y conocimiento profesionales

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

### 5.3.2 Procedimiento de comprobación de antecedentes

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

### 5.3.3 Requisitos de formación

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

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

### 5.3.4 Requisitos y frecuencia de actualización de formación

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

### 5.3.5 Frecuencia y secuencia de rotación de tareas

No existe rotación de tareas en los cargos mencionados.

### 5.3.6 Sanciones por actuaciones no autorizadas

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

### 5.3.7 Requisitos de contratación de terceros

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

### 5.3.8 Documentación proporcionada al personal

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

### 5.4 Procedimientos de auditoría de seguridad de la PKI.

Los procedimientos de auditoría de seguridad son ejecutados por el proveedor de los servicios de infraestructura PKI, Indenova SL.

#### 5.4.1 Tipos de eventos registrados

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

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

#### 5.4.2 Frecuencia de procesamiento de registros de auditoría (log)

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

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

#### 5.4.3 Periodo de retención de los registros de auditoría

Los registros de auditoría se mantienen durante tres (3) años después de la última modificación del fichero, con eso se garantiza poder revisar los problemas presentados con los que se hayan presentado en el histórico. Una vez transcurridos los 3 años y con autorización de el comité de Gerencia de GSE, se puede proceder a destruirlos.

#### 5.4.4 Protección de los registros de auditoría

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

#### 5.4.5 Procedimientos de backup de los registros de auditoría

Los backups de los registros de auditoría siguen los mismos procedimientos para la generación de backups de los sistemas de información.

#### 5.4.6 Sistema de recogida de información de auditoría (interna o externa)

El sistema de recopilación de información de auditoría se basa en los registros automáticos de las aplicaciones que soportan el ciclo de certificación incluyendo los logs de aplicación, logs de seguridad y logs del sistema.

#### 5.4.7 Notificación al sujeto causa del evento

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

### 5.4.8 Análisis de vulnerabilidades

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

### 5.5 Archivo de registros y eventos de la PKI

El registro de archivo y registro de eventos es ejecutado por el proveedor de los servicios de infraestructura PKI, Indenova SL.

#### 5.5.1 Tipos de eventos archivados

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

#### 5.5.2 Periodo de conservación

El periodo de conservación de este tipo de documentación es de 3 años.

#### 5.5.3 Protección de archivos

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

#### 5.5.4 Procedimientos de backup del archivo de registros

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

#### 5.5.5 Requisitos para el sellado de tiempo de los registros

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

#### 5.5.6 Sistema de archivo de la información de auditoría (interna o externa)

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

#### 5.5.7 Procedimientos para obtener y verificar información archivada.

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

### 5.6 Cambio de llaves de la ECD

#### 5.6.1 Cambio de llaves de la raíz ECD GSE

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

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

#### 5.6.2 Cambio de llaves de una Subordinada de ECD GSE

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

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

### 5.7 Recuperación en caso de compromiso de una llave y desastre natural u otro tipo de catástrofe

#### 5.7.1 Procedimientos de gestión de incidentes

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

#### 5.7.2 Alteración de los recursos hardware, software o datos

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

#### 5.7.3 Procedimiento de actuación ante la vulnerabilidad de la llave privada de una Autoridad

ECD GSE tiene establecido y probado un Plan de Continuidad de Negocio de la CA que define las acciones a seguir en caso de producirse una vulnerabilidad de la llave privada de la raíz de ECD GSE o de una de sus subordinadas. En estos casos se deben revocar de manera inmediata las llaves privadas comprometidas de la ECD GSE y los certificados firmados bajo su jerarquía. Se debe generar una nueva llave privada y a

solicitud de los suscriptores y/ responsables se deben emitir nuevos certificados. Dicho plan se ejecutará bajo los siguientes escenarios:

- Cuando el sistema de seguridad de la entidad de certificación ha sido vulnerado.
- Cuando se presenten fallas en el sistema de la entidad de certificación que comprometan la prestación del servicio.
- Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.

En caso de compromiso de la ECD:

- Informará a todos los Suscriptores, Responsables, Tercero que confía y otras CA con los cuales tenga acuerdos u otro tipo de relación del compromiso.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.
- Informará ONAC y a la Superintendencia de Industria y Comercio.

#### 5.7.4 Capacidad de recuperación después de un desastre natural u otro tipo de catástrofe

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

#### 5.8 Cese de una ECD

Conforme a lo dispuesto en el artículo 34 de la ley 527 de 1999, modificado por el artículo 163 del decreto ley 19 de 2012 y conforme al Decreto 333 de 2014, las entidades de certificación abiertas deberán informar de la cesación de actividades a ONAC y a la Superintendencia de Industria y Comercio con una antelación mínima de 30 días. Una vez informada la cesación de actividades la ECD GSE deberá informar a todos los suscriptores o responsables a través de la página de ECD GSE y un aviso publicado en un diario de amplia circulación nacional, sobre la terminación de su actividad o actividades, plan de continuidad del servicio y la fecha precisa de cesación y las consecuencias jurídicas de ésta respecto de los certificados expedidos.

ECD GSE informara el nombre de la entidad que garantizara la continuidad del servicio para quienes hayan contratado, directamente o a través de terceros servicios de la ECD GSE, sin costos adicionales, de no aceptar la continuación del servicio a través del tercero el suscriptor o responsable podrá solicitar la revocación y el reembolso equivalente al valor del tiempo de vigencia restante del servicio de certificación digital, si lo solicitan dentro de los treinta (30) días calendario siguientes a la publicación en la página web y aviso.

Si por causas de fuerza mayor el servicio es suspendido temporalmente, GSE informará al suscriptor o responsable dentro de las veinticuatro (24) horas siguientes de ocurrido el incidente.

## 6 CONTROLES TÉCNICOS DE SEGURIDAD

### 6.1 Generación e instalación del par de llaves

#### 6.1.1 Generación del par de llaves.

##### 6.1.1.1 Generación del par de llaves de la ECD Raíz.

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

##### 6.1.1.2 Generación del par de llaves de las subordinadas de ECD GSE.

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

##### 6.1.1.3 Generación del par de llaves de los suscriptores o responsables de ECD GSE.

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

#### 6.1.2 Entrega de la llave privada a los suscriptores

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

#### 6.1.3 Entrega de la llave pública al emisor del certificado

La llave pública es enviada a la ECD GSE como parte de la petición de solicitud del certificado digital en formato PKIX-CMP.

#### 6.1.4 Entrega de la llave pública de la ECD a terceros aceptantes

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

El certificado de la ECD Raíz puede ser consultado por los terceros de confianza en la dirección [http://certs.gse.co/root/crt\\_root\\_gse\\_sha2.crt](http://certs.gse.co/root/crt_root_gse_sha2.crt)

El certificado de la ECD Subordinada puede ser consultado por los terceros de confianza en la dirección

- [http://certs.gse.co/tsa/crt\\_tsa001co\\_gse\\_sha2.crt](http://certs.gse.co/tsa/crt_tsa001co_gse_sha2.crt)

- [http://certs.gse.co/sub/crt\\_gse\\_sub001co\\_sha2.crt](http://certs.gse.co/sub/crt_gse_sub001co_sha2.crt)

### 6.1.5 Tamaño de las llaves

**El tamaño de las llaves de la ECD Raíz de ECD GSE es de 4096 bits.**

**El tamaño de las llaves de las Subordinadas de ECD GSE es de 4096 bits.**

**El tamaño de las llaves de los certificados emitidos por ECD GSE a usuarios finales es de 2048 bits.**

Al intentar derivar la llave privada, a partir de la llave pública de 2048 bits contenida en los certificados de usuarios finales, el problema radica, en encontrar los factores primos de dos números grandes, ya que se tendrían  $2^{2047}$  posibilidades por cada número. Se estima que descifrar una llave pública de 2048 bits requeriría un trabajo de procesamiento del orden de  $3 \times 10^{20}$  MIPS-año\*.

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

### 6.1.6 Parámetros de generación de la llave pública y verificación de la calidad

La llave pública de la ECD Raíz está codificada de acuerdo con el estándar RFC 5280 y PKCS#1. El algoritmo de firma utilizado en la generación de las llaves es el RSA.

La llave pública de las subordinadas de ECD GSE está codificada de acuerdo con el estándar RFC 5280 y PKCS#1. El algoritmo de firma utilizado en la generación de las llaves es el RSA.

La llave pública de los certificados de usuario final está codificada de acuerdo con el estándar RFC 5280 y PKCS#1. El algoritmo de firma utilizado en la generación de las llaves es el RSA.

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

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

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

#### TIPO DE CERTIFICADO

Certificado de Firma

Certificado de Autenticación

#### KEY USAGE

Digital Signature

Non Repudiation

## 6.2 Protección de la llave privada y controles de ingeniería de los módulos criptográficos

### 6.2.1 Controles y estándares para los módulos criptográficos

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

### 6.2.2 Control multipersona (n de m) de la llave privada

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

### 6.2.3 Custodia de la llave privada

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

Los datos técnicos del dispositivo son los siguientes:

- **SafeNet Luna SA.**

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

### 6.2.4 Backup de la llave privada

Las llaves privadas de la ECD GSE se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (ver 6.2.3 **Custodia de la llave privada**).

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

### 6.2.5 Archivo de la llave privada

Las llaves privadas de ECD GSE se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (ver 6.2.3 **Custodia de la llave privada**).

El archivo de las copias de backup de las llaves privadas está archivado en la caja de seguridad de un centro externo.



### 6.2.6 Transferencia de la llave privada a/desde el módulo criptográfico

Las llaves privadas de ECD GSE se encuentran almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (Ver 6.2.3 Custodia de la llave privada).

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

### 6.2.7 Almacenamiento de las llaves privadas en un módulo criptográfico

Las llaves privadas de la ECD GSE son generadas y almacenadas en dispositivos criptográficos que cumplen los requisitos establecidos de acuerdo con ITSEC, Common Criteria o FIPS 140-2 Nivel 3 o superior nivel de seguridad. (Ver 6.2.3 Custodia de la llave privada).

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

### 6.2.8 Método de activación de la llave privada

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

Se requiere un control multi-persona para la activación de la llave privada de la ECD. Se necesitan al menos 2 de 4 personas para la activación de las llaves.

### 6.2.9 Método de desactivación de la llave privada

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

### 6.2.10 Método para destruir la llave privada

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

### 6.2.11 Características técnicas de los módulos criptográficos utilizados

Los dispositivos criptográficos utilizados por ECD GSE se ajustan a lo indicado en el Anexo F: Dispositivos Criptográficos, del CEA-4.1-10

### 6.2.12 Evaluación del módulo criptográfico

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

### 6.2.13 Evaluación del sistema de cifrado

ECD GSE acoge las recomendaciones para el uso de algoritmos criptográficos y longitudes de clave que sean publicados por el NITS (Instituto Nacional de Estándares y Tecnología por sus siglas en inglés) y por el

ONAC, si se materializa alguna circunstancia en donde los algoritmos utilizados para firma y cifrado por ECD GSE sea vean comprometidos a todos los niveles, ECD GSE tomará inmediatamente las medidas y recomendaciones impartidas para devolver la confiabilidad.

### 6.3 Otros aspectos de la gestión del par de llaves

#### 6.3.1 Archivo de la llave pública

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

#### 6.3.2 Periodos operativos de los certificados y periodo de uso del par de llaves

El periodo de uso del par de llaves está determinado por la vigencia del certificado.

El periodo de validez del certificado digital y el par de llaves de ECD Raíz de la ECD GSE es de treinta (30) años.

El periodo de validez del certificado digital y el par de llaves de las ECD Subordinadas de ECD GSE es de veinticinco (25) años.

### 6.4 Datos de activación

#### 6.4.1 Generación e instalación de los datos de activación

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

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

#### 6.4.2 Protección de los datos de activación

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

#### 6.4.3 Otros aspectos de los datos de activación

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

### 6.5 Controles de seguridad informática

La ECD GSE emplea sistemas fiables para ofrecer sus servicios de certificación digital. GSE ha realizado controles y auditorías a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información se sigue el esquema ISO 27001 y este se hace exigible la certificación para el proveedor de la infraestructura sobre la cual se emiten los servicios de certificación digital.



## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

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

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

### 6.5.1 Requisitos técnicos de seguridad específicos

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

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

### 6.5.2 Evaluación de la seguridad informática

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

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

Este análisis se realiza de forma continua de forma que se localicen nuevas vulnerabilidades de los sistemas.

### 6.5.3 Acciones en caso de un evento o incidente de seguridad de la información.

El sistema de gestión de la seguridad de la Información implementado por ECD GSE tiene establecido un procedimiento de gestión de incidentes tanto para la CA como para la RA que especifica las acciones a ejecutar, componentes o recursos a utilizar y como debe reaccionar el personal en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación digital de ECD GSE.

- a. **Detección y reporte del incidente:** Conocimiento del incidente a través de sistemas de monitorización, sistemas de detección de intrusos, registros del sistema, aviso por parte del personal o por parte de suscriptores o responsables.

- b. **Análisis y evaluación del incidente:** Una vez detectado el incidente se determina el procedimiento de respuesta y se contacta con las personas responsables para evaluar y documentar las acciones a tomar según la gravedad de la incidencia. Se efectúa una investigación para determinar cuál fue el alcance del incidente, es decir averiguar hasta donde llegó el ataque y la máxima información posible de la incidencia.
- c. **Control de daños ocasionados por incidente:** Reaccionar rápidamente para contener la incidencia y evitar que se propague tomando medidas como bloquear accesos al sistema.
- d. **Investigación y recopilación de evidencias:** Revisar registros de auditoría para realizar un seguimiento de lo ocurrido.
- e. **Recuperación y medidas contra incidencia:** Restaurar el sistema a su correcto funcionamiento y documentar el procedimiento y formas de evitar que vuelva a presentarse la incidencia.
- f. **Análisis posterior de la incidencia para la mejorar del procedimiento:** Realizar un análisis de todo lo ocurrido, detectar la causa de la incidencia, corregir la causa para el futuro, analizar la respuesta y corregir errores en la respuesta.

### 6.6 Controles técnicos del ciclo de vida

#### 6.6.1 Controles de desarrollo de sistemas

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

#### 6.6.2 Controles de gestión de seguridad

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

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

#### 6.6.3 Controles de seguridad del ciclo de vida

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

### 6.7 Controles de seguridad de la red

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

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

### 6.8 Estampado cronológico

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

## 7 AUDITORIA DE CONFORMIDAD Y OTROS CONTROLES

### 7.1 Frecuencia o circunstancias de los controles

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

### 7.2 Identidad/cualificación del auditor

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

Requisitos de aseguramiento: Empresa de auditoría legalmente constituida en Colombia en cuyo objeto social esté incluido: servicios de auditoría de sistemas, seguridad de la información e infraestructura de llave pública PKI. Debe contar o haber tenido el reconocimiento Web Trust, auditores profesionales en la ingeniería de sistemas o ingenierías afines los cuales deben demostrar: 10 años de experiencia en auditoría de sistemas, 5 años de experiencia en ISO/IEC 27001 y 5 años de experiencia en infraestructura de llave pública (PKI), Competencia y experiencia certificada. Auditor con formación en ISO/IEC 17065, ISO/IEC 27001, ISO 31000, PKI. Todos con tarjeta profesional vigente en Ingeniería.

### 7.3 Relación entre el auditor y la entidad auditada

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

### 7.4 Aspectos cubiertos por los controles

De conformidad con lo establecido en el numeral REQUISITOS DE ASEGURAMIENTO del documento de CEA establecidos por ONAC el entregable es el Informe de conformidad, no se permite con salvedad o razonabilidad.

### 7.5 Acciones que tomar como resultado de la detección de deficiencias

Las deficiencias detectadas durante el proceso de Auditoría deben ser subsanadas a través de un Plan de Mejoramiento que contenga las acciones, procedimientos e implementación de los controles requeridos para atender los hallazgos.

### 7.6 Comunicación de resultados

Una vez terminada la Auditoría, la firma Auditora debe presentar el Informe de Auditoría a ECD GSE y si se requiere ECD GSE debe establecer un Plan de Mejoramiento. El informe final deber ser remitido a ONAC.

## 8 OTROS ASUNTOS LEGALES Y COMERCIALES

### 8.1 Tarifas

#### 8.1.1 Tarifas de emisión o renovación de certificados

EMISIÓN	
Tipo de Certificado	Precio*
Certificados de Pertenencia a Empresa	\$ 190.000
Certificados de Representación Empresa	\$ 190.000
Certificados de Función Pública	\$ 190.000
Certificados de Profesional Titulado	\$ 190.000
Certificados de Técnico Profesional	\$ 190.000
Certificados Sector Educativo	\$ 190.000
Certificados de Persona Natural	\$ 190.000
Certificados Persona Jurídica	\$ 550.000
Certificados de Factura Electrónica	\$ 550.000
Certificados Correo Electrónico	\$ 190.000
Certificados para Firma Centralizada	\$ 190.000

Renovación	
Tipo de Certificado	Precio*
Certificados de Pertenencia a Empresa	\$ 190.000
Certificados de Representación de Empresa	\$ 190.000
Certificados de Función Pública	\$ 190.000
Certificados de Profesional Titulado	\$ 190.000
Certificados de Técnico Profesional	\$ 190.000
Certificados Sector Educativo	\$ 190.000
Certificados de Persona Natural	\$ 190.000
Certificados Persona Jurídica	\$ 550.000
Certificados de Factura Electrónica	\$ 550.000
Certificados Correo Electrónico	\$ 190.000
Certificados para Firma Centralizada	\$ 190.000

\*Estos precios no incluyen I.V.A y están calculados sobre vigencia de un año. Las cifras aquí indicadas para cada tipo de certificado podrán variar según acuerdos comerciales especiales a los que se pueda llegar con los suscriptores, entidades o solicitantes, en desarrollo de campañas promocionales adelantadas por GSE.

\*Para poder hacer uso del certificado de firma centralizada, es necesario la adquisición de una plataforma tecnológica con costos adicionales.

### 8.1.2 Tarifas de acceso a los certificados

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

### 8.1.3 Tarifas de revocación o acceso a la información de estado

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

### 8.1.4 Tarifas de otros servicios

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

### 8.1.5 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 con 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 y Apelaciones del apartado 1.2 de esta DPC para solicitar el reembolso.

## 8.2 Responsabilidad

La ECD GSE dispondrá en todo momento de un seguro de responsabilidad civil en los términos que marque la legislación vigente.

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

Las responsabilidades de la ECD GSE incluyen las establecidas por la presente DPC, así como las que resulten de aplicación como consecuencia de la normativa colombiana e internacional.

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

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

## 8.3 Imparcialidad

ECD GSE, en cabeza de la Comité de Gerencia y sus colaboradores se comprometen a salvaguardar la imparcialidad e independencia en los procesos y servicios de certificación digital, con el fin de prevenir conflictos de interés al interior de la empresa, con las partes interesadas pertinentes y externos, actuando dentro del marco legal Ley 527 de 1999, Decretos 019 de 2012, 333 de 2014 y 1471 de 2014, y de los criterios específicos

de acreditación del Organismo Nacional de Acreditación de Colombia (ONAC), por lo que se establecen los siguientes mecanismos de cumplimiento:

- El Comité de Gerencia y los colaboradores de GSE declaran que no participan directa o indirectamente en servicios o actividades, que puedan poner en peligro la libre competencia, la responsabilidad, la transparencia.
- Los colaboradores utilizarán el levantamiento de acciones preventivas y correctivas para responder a cualquier riesgo que comprometa la imparcialidad de la empresa.
- Los colaboradores que hacen parte de los servicios de certificación digital acreditados, no podrán prestar servicios de consultoría, ni involucrar al equipo desarrollador a prestar servicio de soporte técnico al suscriptor o cliente.
- GSE es responsable de la imparcialidad en el desarrollo de sus actividades y no permite que las presiones comerciales, financiera u otras comprometan su imparcialidad.
- GSE no emitirá certificados de firma digital a persona natural o jurídica que tenga relación con grupos al margen de la ley o que desarrollen actividades ilícitas.

**Nota:**

Cualquier caso que ponga en riesgo la imparcialidad de la ECD GSE como ECD o de su personal, organismo u organización, se pondrá en conocimiento del Equipo de Calidad

#### 8.4 Exoneración de responsabilidad

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

#### 8.5 Responsabilidades financieras y legales

##### 8.5.1 Otros bienes

ECD GSE cuenta con la capacidad económica y financiera suficiente para prestar los servicios autorizados y responder por sus deberes como entidad de certificación. ECD GSE como prestador de servicios de certificación responderá por los perjuicios que se causen a los suscriptores, entidades o terceros de buena fe derivados de errores y omisiones, de mala fe de los administradores, representantes legales o empleados de ECD GSE en el desarrollo de las actividades para las cuales cuenta con autorización y para ello cuenta





## Declaración de prácticas de certificación

Fecha de vigencia 12/04/2019

Versión 5

con un seguro de responsabilidad civil de conformidad con el del Artículo 9°. Garantías, del Decreto 333 de 2014. ECD GSE no asume ningún otro compromiso ni brinda ninguna otra garantía, así como tampoco asume ninguna otra responsabilidad ante suscriptor o responsables de certificados o terceros de confianza a excepción de lo establecido por las disposiciones de la presente DPC.

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

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

## 8.6 Confidencialidad de la información

### 8.6.1 Responsabilidad de proteger la información confidencial

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

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

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

### 8.6.2 Información confidencial

La siguiente Información es considerada confidencial:

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

### 8.6.3 Información no confidencial

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

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

### 8.6.4 Deber de proteger la información confidencial

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

## 8.7 Protección de la información personal

### 8.7.1 Política de privacidad

ECD GSE tiene como política de privacidad lo establecido ley 1581 de 2012: La Ley de Protección de Datos Personales.

Las disposiciones sobre protección de datos establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación:

- Dato Público:** Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.
- Dato Semiprivado:** Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su suscriptor o responsable sino a cierto sector o grupo de personas.
- Dato Privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el suscriptor o responsable de la información.
- Dato Sensible:** Es el dato que afecta la intimidad del suscriptor o responsable o cuyo uso indebido puede generar su discriminación.

### 8.7.2 Información tratada como privada

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

### 8.7.3 Información no calificada como privada

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

### 8.7.4 Responsabilidad de la protección de los datos de carácter personal

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

GSE ECD hace uso de mecanismos tecnológicos como el directorio activo donde se instrumentaliza la política de control de acceso y un repositorio centralizado donde se encuentra la información protegida por un firewall que previene intrusiones dentro de la red.

### 8.7.5 Notificación y consentimiento para usar datos de carácter personal

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

### 8.7.6 Revelación en el marco de un proceso administrativo o judicial

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

### 8.7.7 Otras circunstancias de revelación de información

ECD GSE tiene como política de privacidad a lo estrictamente establecido en el derecho la ley de protección de datos: “La información privada, será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, solo puede ser obtenida u ofrecida a los terceros autorizados por el Suscriptor o responsable o por la ley.

### 8.7.8 Sistema de seguridad para proteger la información

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

- a. El proveedor de la infraestructura debe contar con las siguientes certificaciones:
  - i. ISO 27001
  - ii. ISO 9001
  - iii. ISO 15504 nivel 3
- b. Pruebas de penetración y escaneo de vulnerabilidades en la red, realizada por una empresa especializada en Ethical Hacking.

## 8.8 Derechos de propiedad intelectual

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

### 8.9 Obligaciones

#### 8.9.1 Obligaciones de la ECD GSE

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

1. Respetar lo dispuesto en la normatividad vigente, en esta DPC y en las Políticas de Certificación PC.
2. Publicar esta DPC y cada una de las Políticas de Certificación en la página Web de GSE.
3. Informar a ONAC sobre las modificaciones de la DPC y de las Políticas de Certificación.
4. Mantener la DPC con su última versión publicada en la página Web de GSE.
5. Proteger y custodiar de manera segura y responsable su llave privada.
6. Emitir certificados conforme a las Políticas de Certificación y a los estándares definidos en la presente DPC.
7. Generar certificados consistentes con la información suministrada por el solicitante o suscriptor.
8. Conservar la información sobre los certificados emitidos de conformidad con la normatividad vigente.
9. Emitir certificados cuyo contenido mínimo este de conformidad con la normativa vigente para los diferentes tipos de certificados.
10. Publicar el estado de los certificados emitidos en un repositorio de acceso libre.
11. No mantener copia de la llave privada del solicitante o suscriptor.
12. Revocar los certificados según lo dispuesto en la Política de revocación de certificados digitales.
13. Actualizar y publicar la lista de certificados revocados CRL con los últimos certificados revocados.
14. Notificar al Solicitante, Suscriptor o Entidad la revocación del certificado digital dentro de las 24 horas siguientes a la revocación del certificado de conformidad con la política de revocación de certificados digitales.

#### 8.9.2 Obligaciones de la RA

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

1. Conocer y dar cumplimiento a lo dispuesto en la presente DPC y en la Política de Certificación correspondiente a cada tipo de certificado.
2. Custodiar y proteger su llave privada.
3. Comprobar la identidad de los Solicitantes, Responsables o Suscriptores de certificados digitales.
4. Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
5. Archivar y custodiar la 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 certificados digitales vigentes.

### 8.9.3 Obligaciones del suscriptor y/o responsable.

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

- a. Usar su certificado digital según los términos de esta DPC.
- b. Verificar dentro del día siguiente hábil que la información del certificado digital es correcta. En caso de encontrar inconsistencias, notificar a la ECD.
- c. Abstenerse de: prestar, ceder, escribir, publicar la contraseña de uso su certificado digital y tomar todas las medidas necesarias, razonables y oportunas para evitar que éste sea utilizado por terceras personas.
- d. No transferir, compartir ni prestar el dispositivo criptográfico a terceras personas.
- e. Suministrar toda la información requerida en el Formulario de Solicitud de Certificados digitales para facilitar su oportuna y plena identificación.
- f. Solicitar la revocación del Certificado Digital ante el cambio de nombre y/o apellidos.
- g. Solicitar la revocación del Certificado Digital cuando el Suscriptor haya variado su nacionalidad.
- h. Cumplir con lo aceptado y firmado en el documento términos y condiciones o responsable de certificados digitales.
- i. Proporcionar con exactitud y veracidad la información requerida.
- j. Informar durante la vigencia del certificado digital cualquier cambio en los datos suministrados inicialmente para la emisión del certificado.
- k. Custodiar y proteger de manera responsable su llave privada.
- l. Dar uso al certificado de conformidad con las PC establecidos en la presente DPC para cada uno de los tipos de certificado.
- m. Solicitar como suscriptor o responsable de manera inmediata la revocación de su certificado digital cuando tenga conocimiento que existe una causal definida en numeral *Circunstancias para la revocación de un certificado* de la presente DPC.
- n. No hacer uso de la llave privada ni del certificado digital una vez cumplida su vigencia o se encuentre revocado.
- o. Informar a los terceros de confianza de la necesidad de comprobar la validez de los certificados digitales sobre los que esté haciendo uso en un momento dado.
- p. Informar al tercero de buena fe para verificar el estado de un certificado dispone de la lista de certificados revocados CRL, publicada de manera de periódica por ECD GSE.
- q. No realizar ninguna declaración relacionada con su certificación digital en la ECD GSE pueda considerar engañosa o no autorizada, conforme a lo dispuesto por esta DPC y PC.
- r. Una vez caducado o revocado el servicio de certificación digital el suscriptor debe inmediatamente dejar de utilizarla en todo el material publicitario que contenga alguna referencia al servicio.
- s. El suscriptor al hacer referencia al servicio de certificación digital prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, debe informar que cumple con los requisitos especificados en las PC de esta DPC, indicando la versión.
- t. El suscriptor podrá utilizar las marcas de conformidad y la información relacionada con el servicio de certificación digital prestado por ECD GSE en medios de comunicación, tales como documentos, folletos o publicidad, desde que cumpla lo requerido en el literal anterior.

### 8.9.4 Obligaciones de los Terceros de buena fe

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

- Conocer lo dispuesto sobre Certificación Digital en la Normatividad vigente.
- Conocer lo dispuesto en la DPC.
- Verificar el estado de los certificados antes de realizar operaciones con certificados digitales.
- Verificar la Lista de certificados Revocados CRL antes de realizar operaciones con certificados digitales.
- Conocer y aceptar las condiciones sobre garantías, usos y responsabilidades al realizar operaciones con certificados digitales.

### 8.9.5 Obligaciones de la Entidad (Cliente).

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

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

### 8.9.6 Obligaciones de otros participantes.

El Comité de Gerencia y el Equipo de Calidad como organismos internos de ECD GSE está en la obligación de:

- Revisar la consistencia de DPC con la normatividad vigente.
- Aprobar y decidir sobre los cambios a realizar sobre los servicios de certificación digital, por decisiones de tipo normativo o por solicitudes de suscriptores o responsables.
- Aprobar la notificación de cualquier cambio a los suscriptores y/ responsables analizando su impacto legal, técnico o comercial.
- Revisar y tomar acciones sobre cualquier comentario realizado por suscriptores o responsables cuando un cambio en el servicio de certificación digital se realice.
- 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 certificación digital, de acuerdo con el R-AC-01.
- Autorizar los cambios o modificaciones requeridas sobre la DPC.
- Autorizar la publicación de la DPC en la página Web de la ECD GSE.
- Aprobar los cambios o modificaciones a las Políticas de Seguridad de la ECD GSE.
- Asegurar la integridad y disponibilidad de la información publicada en la página Web de la ECD GSE.

- j. Asegurar la existencia de controles sobre la infraestructura tecnológica de la ECD GSE.
- k. Solicitar la revocación de un certificado si tuviera el conocimiento o sospecha del compromiso de la llave privada del suscriptor, entidad o cualquier otro hecho que tienda al uso indebido de llave privada del suscriptor, entidad o de la propia ECD.
- l. Conocer y tomar acciones pertinentes cuando se presenten incidentes de seguridad.
- m. Realizar con una frecuencia máxima anual, una revisión de la DPC para verificar que las longitudes de las llaves y periodos de los certificados que se estén empleando son adecuados.
- n. Revisar, aprobar y autorizar cambios sobre los servicios de certificación digital acreditados por el organismo competente.
- o. Revisar, aprobar y autorizar la propiedad y el uso de símbolos, certificados y cualquier otro mecanismo que requiera ECD GSE para indicar que el servicio de certificación digital está acreditado.
- p. Velar que las condiciones de acreditación otorgado por el organismo competente se mantengan.
- q. Velar por el uso adecuado en documentos o en cualquier otra publicidad que los símbolos, los certificados, y cualquier otro mecanismo que indique que ECD GSE cuenta con un servicio de certificación acreditado y cumple con lo dispuesto en las Reglas de Acreditación de ONAC RAC 3.0-01 y RAC-3.0-03
- r. Velar por mantener informados a sus proveedores críticos y ECD recíproca en caso de existir, de la obligación de cumplimiento de los requisitos del CEA-4.1-10, en los numerales que correspondan.
- s. El Equipo de Calidad 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 el Comité de Gerencia el mecanismo que elimina o minimiza tal riesgo, de manera continua.
- t. Velar que todo el personal y los comités de la ECD (sean internos o externos), que puedan tener influencia en las actividades de certificación actúen con imparcialidad, especialmente aquellas que surjan por presiones comerciales, financieras u otras comprometan su imparcialidad.
- u. Documentar y demostrar el compromiso de imparcialidad.
- v. Velar que el personal administrativo, de gestión, técnico de la PKI, de la ECD asociado a las actividades de consultoría, mantenga completa independencia y autonomía respecto al personal del proceso de revisión y toma de decisión sobre la certificación de la misma ECD.

## 9 Términos y condiciones de la DPC y PC

### 9.1.1 Inicio de vigencia de la DPC y PC

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

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



## Declaración de prácticas de certificación

Fecha de vigencia  
12/04/2019

Versión  
5

### 9.1.2 Efectos de terminación e inicio de vigencia DPC y PC

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

### 9.1.3 Cambios que afectan la DPC y PC

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

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

### 9.1.4 Circunstancias bajo las cuales la OID debe cambiarse

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

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

## 10 Políticas de Certificación para Certificados Digitales

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

- La DPC** es que el conjunto de prácticas adoptadas por ECD GSE para la prestación de los servicios acreditados por ONAC y contiene información detallada sobre su sistema de seguridad, soporte, administración y emisión de los certificados, además sobre la relación de confianza entre Solicitante, Suscriptor, Responsable, Entidad, Tercero de buena fe y la ECD.
- Políticas de certificación de certificados digitales** constituye el conjunto de reglas que definen las características de los distintos certificados ECD GSE y la aplicabilidad de estos certificados para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos.

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

Por este motivo, se adjunta las siguientes Políticas de Certificado



- Políticas de Certificado para Servicio de Certificados Digitales.

<b>OID (Object Identifier) - IANA</b>	1.3.6.1.4.1.31136.2.2.3
<b>Ubicación de la DPC</b>	<a href="http://cps.gse.co/">http://cps.gse.co/</a>

- Políticas de Certificado para Servicio de Estampado Cronológico.

<b>OID (Object Identifier) – IANA</b>	1.3.6.1.4.1.31136.2.3.3
<b>Ubicación de la PC</b>	<a href="http://cps.gse.co/">http://cps.gse.co/</a>

- Políticas de Certificado para Servicio de Archivo Confiable de Datos.

<b>OID (Object Identifier) – IANA</b>	1.3.6.1.4.1.31136.3.1
<b>Ubicación de la PC</b>	<a href="http://cps.gse.co/">http://cps.gse.co/</a>

- Políticas de Certificado para Servicio de Correo Electrónico Certificado.

<b>OID (Object Identifier) – IANA</b>	1.3.6.1.4.1.31136.3.3
<b>Ubicación de la PC</b>	<a href="http://cps.gse.co/">http://cps.gse.co/</a>

- Políticas de Certificado para Servicio de Generación de Firmas Digitales.

<b>OID (Object Identifier) – IANA</b>	1.3.6.1.4.1.31136.3.2
<b>Ubicación de la PC</b>	<a href="http://cps.gse.co/">http://cps.gse.co/</a>

### 11 ANEXO 1 PERFIL TÉCNICO CERTIFICADOS DIGITALES.

### 12 ANEXO 2 – TÉRMINOS Y CONDICIONES.