

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN	ELABORÓ	REVISÓ	APROBÓ
1	24/10/2019	DOCUMENTO NUEVO	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS
2	15-11-2021	<ul style="list-style-type: none"> - Se Incluyó la Exclusión de responsabilidad de PKI SERVICES -Se hace referencia a los modelos y minutas de los contratos que utilizarán los usuarios - Se relacionan los servicios 2 y 3 - Se actualizó el procedimiento de Revocación enunciado en la DPC. - Se ajustó lo concerniente a la Administración de la política. - Se ajustan los mecanismos utilizados para la validación de la identidad. - Se revisan y ajustan los requisitos de Formación del Personal. - Se revisa y se ajusta el Uso de Claves y Certificados 	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS
3	12-03-2023	Se retiro punto 11 el cual se llevó al punto 4.1.3 que también se actualizo.	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS
4	17-04-2023	Se revisa y se cambia el protocolo RFC 5905, por el Protocolo RFC 3161 Time-Stamp Protocol, en el Numeral 5.5. "Requisitos para el Sellado del tiempo de los registros" y 6.6." Sellado de tiempo"	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS
5	31/10/2024	Se revisa y se ajustan las responsabilidades de los suscriptores sobre el uso de la plataforma desatendida y uso de los certificados (9.7.3)	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS

CONTENIDO

1. INTRODUCCIÓN	10
1.1. PRESENTACIÓN DEL DOCUMENTO	10
1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN	10
1.3. PARTICIPANTES DE LA PKI DE PKI SERVICES S.A.S	10
1.3.1. JERARQUÍA DE CERTIFICADOS DE LA PKI DE PKI SERVICES S.A.S	10
1.3.2 PKI SERVICES CA ROOT	11
1.3.3. IDENTIFICACIÓN DE LA ECD - AC PKI SERVICES S.A.S.	11
1.3.4. SOLICITANTE	12
1.3.5. SUSCRIPTOR	12
1.3.6. TERCERO QUE CONFÍA	12
1.3.7. ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL SUSCRIPTOR	12
1.3.8. ESTAMPA DE TIEMPO (TIME STAMPING)	12
1.3.9. AUTORIDAD DE LAS POLÍTICAS	13
1.3.10. PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (ECD)	13
1.3.11. AUTORIDAD DE REGISTRO (RA)	13
1.3.12. OFICIAL DE DECISIÓN	13
1.4.1 SERVICIOS DE CERTIFICACIÓN DIGITAL	13
1.4.1.1 TIPOS DE CERTIFICADOS DIGITALES	13
1.4.1.2 OTROS SERVICIOS DE CERTIFICACIÓN DIGITAL	14
1.4.2 USOS APROPIADOS DE LOS CERTIFICADOS	14
1.4.3. USOS NO AUTORIZADOS DE LOS CERTIFICADOS	14
1.5. ADMINISTRACIÓN DE LA DPC Y LAS PC	14
1.5.1 ORGANIZACIÓN RESPONSABLE	14
1.5.2 DATOS DE CONTACTO	14
1.5.3 PROCEDIMIENTO DE APROBACIÓN	14
1.6. DEFINICIONES Y ABREVIACIONES	15
1.6.1 DEFINICIONES	15
1.6.2 SIGLAS	17
2. RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN	18
2.1. REPOSITORIOS	18
2.2. PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN	19
2.3. PLAZO O FRECUENCIA DE LA PUBLICACIÓN	19
2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS	19

3. IDENTIFICACIÓN Y AUTENTICACIÓN	19
3.1.1 CUMPLIMIENTO AL PRINCIPIO CONSTITUCIONAL DE LA BUENA FE	19
3.1.2 FALSEDAD EN DOCUMENTO PRIVADO	19
3.2. NOMBRES	19
3.2.1. TIPOS DE NOMBRES	19
3.2.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO	20
3.2.3. ANONIMATO Y SEUDOANONIMATO DE LOS SUSCRIPTORES	20
3.2.4. UNICIDAD DE LOS NOMBRES	20
3.2.5. RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS REGISTRADAS	20
3.3 VALIDACIÓN DE LA IDENTIDAD	20
3.3.1 MÉTODO DE PRUEBA DE POSESIÓN DE LA CLAVE PRIVADA	20
3.3.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA NATURA	20
3.3.3. AUTENTICACIÓN DE LA IDENTIDAD DE UNA ENTIDAD	20
3.3.4. INFORMACIÓN DE SUSCRIPTOR Y SOLICITANTE NO VERIFICADA	21
3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN DE CAMBIO DE CLAVES	21
3.5. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN	21
4. REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE CERTIFICADOS	22
4.1. SOLICITUD DE CERTIFICADOS	22
4.1.1. QUIÉN PUEDE SOLICITAR UN CERTIFICADO	22
4.1.2 COMERCIALIZACIÓN	22
4.1.3 CONTRATACIÓN Y PAGO	23
4.1.4 SOLICITUD	23
4.2. TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS	24
4.2.1 REVISIÓN	24
4.2.2 DECISIÓN	24
4.3. EMISIÓN DE CERTIFICADOS	24
4.3.1 ACCIONES DE PKI SERVICES S.A.S. DURANTE LA EMISIÓN DE CERTIFICADOS	24
4.3.2 NOTIFICACIÓN AL SOLICITANTE POR PKI SERVICES S.A.S. DE LA EMISIÓN DEL CERTIFICADO	25
4.4. ACEPTACIÓN DEL CERTIFICADO	25
4.4.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO	25
4.4.2 PUBLICACIÓN DEL CERTIFICADO POR PKI SERVICES S.A.S.	25
4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR PKI SERVICES S.A.S. A OTRAS ENTIDADES	25
4.5. USOS DE LAS CLAVES Y EL CERTIFICADO	25

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR ELSUSCRIPTOR	25
4.5.2. USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROSQUE CONFÍAN	25
4.6. RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES	25
4.7. RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES	26
4.8. MODIFICACIÓN DE CERTIFICADOS	26
4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS	26
4.9.1 CIRCUNSTANCIAS O CAUSAS PARA LA REVOCACIÓN DE UN CERTIFICADO	26
4.9.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN	26
4.9.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN	27
4.9.3.1 Procedimiento Online	27
4.9.3.2 Mediante PQRS	27
4.9.4 PLAZO EN EL QUE PKI SERVICES S.A.S. DEBE RESOLVER LA SOLICITUD DEREVOCACIÓN	27
4.9.5 OBLIGACIÓN DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN	27
4.9.6 FRECUENCIA DE EMISIÓN DE LAS CRLS	27
4.9.7 TIEMPO MÁXIMO ENTRE LA GENERACIÓN Y LA PUBLICACIÓN DELAS CRLS	27
4.9.8 DISPONIBILIDAD DEL SISTEMA EN LÍNEA DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS	28
4.9.9 REQUISITOS DE COMPROBACIÓN DE REVOCACIÓN EN LÍNEA	28
4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS	28
4.10.1 CARACTERÍSTICAS OPERACIONALES	28
4.10.2 DISPONIBILIDAD DEL SERVICIO	28
4.10.3 CARACTERÍSTICAS ADICIONALES	28
4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN	28
4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES (KEY ESCROW AND RECOVERY)	28
5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES	29
5.1. CONTROLES FÍSICOS	29
5.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN	29
5.1.2 ACCESO FÍSICO	29
5.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO	29
5.1.4 EXPOSICIÓN AL AGUA	29
5.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS	30
5.1.6 SISTEMA DE ALMACENAMIENTO	30

5.1.7. ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN.....	30
5.1.8. COPIAS DE SEGURIDAD FUERA DE LA INSTALACIÓN	30
5.2. CONTROLES DE PROCEDIMIENTO	30
5.2.1 ROLES DE CONFIANZA.....	30
5.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA	30
5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL.....	31
5.2.4. ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES	31
5.3. CONTROLES DE PERSONAL.....	31
5.3.1. REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES	31
5.3.2. PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES	31
5.3.3. REQUISITOS DE FORMACIÓN.....	31
5.3.4. REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN.....	31
5.3.5. SANCIONES POR ACTUACIONES NO AUTORIZADAS.....	31
5.3.6. REQUISITOS DE CONTRATACIÓN DE TERCEROS.....	31
5.3.7. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL.....	32
5.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD	32
5.4.1. TIPOS DE EVENTOS REGISTRADOS.....	32
5.4.2. FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA(LOG).....	32
5.4.3. PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA.....	32
5.4.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA	32
5.4.5. PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA.....	33
5.4.6. SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA(INTERNA O EXTERNA).....	33
5.4.7. ANÁLISIS DE VULNERABILIDADES.....	33
5.4.8. SUPERVISIÓN.....	33
5.5. ARCHIVO DE REGISTROS.....	33
5.5.1. TIPOS DE EVENTOS ARCHIVADOS	33
5.5.2. PERIODO DE CONSERVACIÓN DE REGISTROS	33
5.5.3. PROTECCIÓN DEL ARCHIVO.....	33
5.5.4. PROCEDIMIENTOS DE COPIA DE SEGURIDAD DEL ARCHIVO.....	34
5.5.5. REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS.....	34
5.5.6. SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA(INTERNO O EXTERNO).....	34
5.5.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA	34
5.6. CAMBIO DE CLAVES	34

5.7. PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES.....	34
5.7.1. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE	35
5.7.2. CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE	35
5.8. CESE DEL SERVICIO DE EMISIÓN DE CERTIFICADOS	35
6. CONTROLES TÉCNICOS DE SEGURIDAD.....	35
6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....	35
6.1.1. GENERACIÓN DEL PAR DE CLAVES	35
6.1.2. ENTREGA DE LA CLAVE PRIVADA A LOS SUSCRIPTORES	36
6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO	36
6.1.4. ENTREGA DE LA CLAVE PÚBLICA DE PKI SERVICES S.A.S. A TERCEROS QUECONFÍAN.....	36
6.1.5. TAMAÑO DE LAS CLAVES Y PERIODO DE VALIDEZ.....	36
6.1.6. PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD	36
6.1.7 USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509).....	37
6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS	37
6.2.1. CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS 	37
6.2.2. CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA.....	37
6.2.3. CUSTODIA DE LA CLAVE PRIVADA	37
6.2.4. COPIA DE SEGURIDAD DE LA CLAVE PRIVADA	37
6.2.5. ARCHIVO DE LA CLAVE PRIVADA.....	38
6.2.6. ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULO CRIPTOGRÁFICO	38
6.2.7. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA.....	38
6.2.8. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA	38
6.2.9 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA.....	38
6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES.....	38
6.3.1. ARCHIVO DE LA CLAVE PÚBLICA	38
6.3.2. PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES	38
6.4. DATOS DE ACTIVACIÓN.....	38
6.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN	38
6.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN	39
6.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN.....	39
6.5. CONTROLES DE SEGURIDAD INFORMÁTICA	39

6.5.1. REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS	39
6.5.2. CONTROLES DE SEGURIDAD DE LA RED	39
6.5.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	39
6.5.3.1 CONTROLES DE DESARROLLO DE SISTEMAS	40
6.5.3.2 CONTROLES DE GESTIÓN DE SEGURIDAD	40
6.5.3.2.1 Gestión de seguridad.....	40
6.5.3.2.2 Clasificación y gestión de información y bienes.....	40
6.5.3.3 Operaciones de gestión.....	40
6.5.3.4 Tratamiento de los soportes y seguridad.....	40
6.5.3.5 Planning del sistema.....	40
6.5.3.6 Gestión del sistema de acceso.....	40
6.5.3.7 Gestión general de PKI SERVICES S.A.S:.....	40
6.5.4. EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA	41
6.6. SELLADO DE TIEMPO	41
7. PERFILES DE CERTIFICADO, CRL Y OCSP	42
7.1. PERFIL DE CERTIFICADO	42
7.1.1. FORMATO DEL CERTIFICADO	42
7.1.2. EXTENSIONES DEL CERTIFICADO	43
7.1.3. IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS	44
7.1.4. FORMATOS DE NOMBRES	44
7.1.5. RESTRICCIONES DE LOS NOMBRES	45
7.1.6. IDENTIFICADORES DE OBJETO (OID) DE LA POLÍTICA DE CERTIFICADOS	45
7.1.7. USO DE LA EXTENSIÓN POLICY CONSTRAINTS	46
7.1.8. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS	46
7.1.9. TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICY	46
7.2. PERFIL DE CRL	46
7.2.1. FORMATO Y PERIODO DE VALIDEZ DE LA CRL	46
7.2.2. EXTENSIONES DE LA CRL Y DE ENTRADA DE CRL	47
EXTENSIONES DE LA CRL	47
Extensión.....	47
Crítica.....	47
Valor.....	47
7.3. PERFIL DE OCSP	47
7.4. PERFIL DE CERTIFICADO OCSP	47
7.4.1. FORMATO DEL CERTIFICADO	47
7.4.2. EXTENSIONES DEL CERTIFICADO	47
7.4.3. IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS	48
7.4.4. FORMATOS DE NOMBRES	48

7.4.5. RESTRICCIONES DE LOS NOMBRES.....	48
7.4.6. IDENTIFICADORES DE OBJETO (OID) DE LAS POLÍTICAS DE CERTIFICADOS	48
7.4.7. USO DE LA EXTENSIÓN POLICY CONSTRAINTS.....	49
7.4.8. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS	49
7.4.9. TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATE POLICY	49
8. AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES	49
8.1. FRECUENCIA DE LAS AUDITORÍAS	49
8.2. IDENTIDAD/CUALIFICACIÓN DEL AUDITOR	49
8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA.....	49
8.4. ASPECTOS CUBIERTOS POR LOS CONTROLES.....	49
8.5. ACCIONES PARA TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS	49
8.6. COMUNICACIÓN DE RESULTADOS.....	49
9. OTROS ASUNTOS LEGALES Y COMERCIALES	50
9.1. TARIFAS.....	50
9.1.1. TARIFAS DE EMISIÓN DE CERTIFICADOS	50
9.1.2. TARIFAS DE ACCESO A LOS CERTIFICADOS	50
9.1.3. TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO.....	50
9.1.4. TARIFAS DE OTROS SERVICIOS.....	50
9.1.5. POLÍTICA DE REEMBOLSO.....	50
9.2. RESPONSABILIDADES FINANCIERAS	50
9.2.1. COBERTURA DEL SEGURO.....	50
9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN	50
9.3.1. INFORMACIÓN CONFIDENCIAL	51
9.3.2. INFORMACIÓN NO CONFIDENCIAL	51
9.4. POLÍTICA DE PROTECCIÓN DE DATOS	51
9.5. DERECHOS DE PROPIEDAD INTELECTUAL	52
9.6. OBLIGACIONES	52
9.6.1. OBLIGACIONES DE PKI SERVICES S.A.S.....	52
9.6.2. OBLIGACIONES DE LOS PROVEEDORES.....	53
9.6.3. OBLIGACIONES DE LOS SOLICITANTES	53
9.6.4. OBLIGACIONES DE LOS SUSCRIPTORES.....	54
9.6.5. OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN	54
9.6.6. OBLIGACIONES DE LA ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL SUSCRIPTOR.....	54

9.6.7. OBLIGACIONES (DEBERES Y DERECHOS) DEL SOLICITANTE Y/O SUScriptor	54
9.6.7.1. USO DE MARCA.	55
9.6.7.2. DEBERES DE LOS SOLICITANTES.	55
9.6.7.3. DERECHOS DE LOS SOLICITANTES.	55
9.6.7.4. DEBERES DE LOS SUSCRIPTORES.	55
9.6.7.5. DERECHOS DE LOS SUSCRIPTORES.	56
9.7. RESPONSABILIDADES	56
9.7.1. RESPONSABILIDADES DE PKI SERVICES S.A.S.	56
9.7.2 EXCLUSIÓN DE RESPONSABILIDAD DE PKI SERVICES S.A.S	56
9.7.3. RESPONSABILIDADES DEL SUSCRIPTOR	57
9.8. LIMITACIÓN DE RESPONSABILIDAD	58
9.9. INDEMNIZACIONES	58
9.9.1. INDEMNIZACIONES POR DAÑOS OCASIONADOS POR PKI SERVICES S.A.S.	58
9.9.2. INDEMNIZACIONES POR LOS DAÑOS CAUSADOS POR LOS SOLICITANTES, POR LOS SUSCRIPTORES Y POR LOS TERCEROS QUE CONFÍAN	59
9.10 PERIODO DE VALIDEZ	59
9.10.1. PLAZO	59
9.10.2. SUSTITUCIÓN Y DEROGACIÓN DE LA DPC Y LAS PC	59
9.10.3. EFECTOS DE LA FINALIZACIÓN	59
9.11. PQRS 59	
9.12. CAMBIOS EN DPC Y PC	59
9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS	59
9.14. LEY APLICABLE	60
9.15. CONFORMIDAD CON LA LEY APLICABLE	60
9.16. ESTIPULACIONES DIVERSAS	60
9.16.1. CONTRATO DE SUSCRIPCIÓN	60
9.16.2. CLÁUSULA DE ACEPTACIÓN COMPLETA	60
9.16.3. INDEPENDENCIA	60
9.17. OTRAS ESTIPULACIONES	60
10.POLÍTICAS DE LOS CERTIFICADOS DIGITALES QUE EXPIDE PKI SERVICES	60
10.6. TARIFAS:	60

1. INTRODUCCIÓN

1.1. PRESENTACIÓN DEL DOCUMENTO

Este documento constituye la Declaración de Prácticas de Certificación (DPC) para prestar los servicios de certificación digital de PKI SERVICES S.A.S., en el marco del cumplimiento de las leyes, normas, estándares técnicos y criterios, conforme a la legislación vigente.

Esta DPC establece las prácticas que lleva a cabo PKI SERVICES S.A.S. para emitir, gestionar, revocar y renovar certificados digitales, siguiendo los estándares internacionales aceptados para la infraestructura de llave pública (PKI) como lo es el estándar RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.

El presente documento es de carácter público y se encuentra dirigido a todas las personas naturales y jurídicas, Solicitantes, Suscriptores, Terceros que confían y público en general.

En el caso de que se detecten vulnerabilidades o se pierda la vigencia de los estándares técnicos o infraestructura indicados en la presente DPC, PKI SERVICES S.A.S se encargará de informar de tal hecho a ONAC, para proceder con la respectiva actualización.

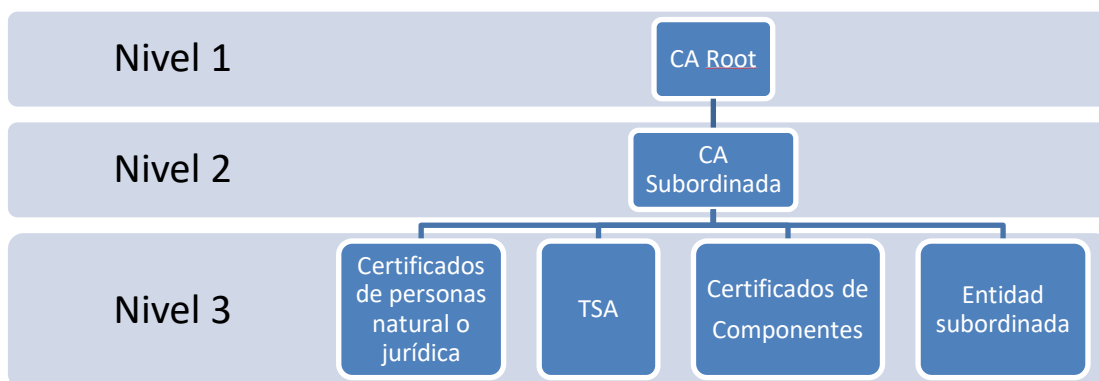
El Gerente General administra y revisa anualmente La Declaración de Prácticas de Certificación, con el fin de que la misma cumpla con los Criterios Específicos de Acreditación. Esta revisión debe hacerse con suficiente anticipación a la renovación anual de la póliza.

1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN

Los datos de identificación del presente documento están especificados en la tabla inicial *Identificación del documento*.


1.3. PARTICIPANTES DE LA PKI DE PKI SERVICES S.A.S

1.3.1. JERARQUÍA DE CERTIFICADOS DE LA PKI DE PKI SERVICES S.A.S.



Nivel 1: Autoridad de Certificación Raíz

Se denomina Autoridad de Certificación Raíz (o AC Root) a la entidad dentro de la jerarquía que emite certificados a otras Autoridades de Certificación y cuyo certificado de clave pública ha sido autofirmado. Su función es firmar el certificado de las otras AC pertenecientes a la Jerarquía de Certificación. Los datos de identificación del Certificado Raíz actual de PKI SERVICES S.A.S. ROOT, se detalla en el documento Políticas de Certificados – PC.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 11 de 61

Nivel 2: Autoridad de Certificación Subordinada.

Se llama Autoridad de Certificación Subordinada a la entidad de certificación dentro de la jerarquía que de una parte hereda la confianza de la CA RAIZ y emite los Certificados de Nivel 3. Su certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Raíz PKI SERVICES S.A.S. ROOT En el presente caso, los datos de identificación del actual Certificado de Nivel 2, generado y gestionado por PKI SERVICES S.A.S. a través del cual emite los Certificados de Nivel 3, se detalla en el documento Políticas de Certificados – PC.

La CA Raíz de PKI SERVICES S.A.S. también emite el certificado de la Unidad de Sellado de Tiempo (TSU) de la Autoridad de Sellado de Tiempo (TSA) de la ECD PKI SERVICES S.A.S. (PKI SERVICES TSA – TSU 01).

Asimismo, la CA Raíz de PKI SERVICES S.A.S podrá emitir certificados de otras CA Subordinadas del grupo PKI SERVICES, lo cual deberá quedar reflejado en las correspondientes DPC de estas CA Subordinadas. Por tanto, PKI SERVICES Root también podrá ser la CA Raíz de otras PKI de PKI SERVICES.

Nivel 3: Autoridad de Certificación Intermedia.

Se llama Intermedia de Nivel 3 o Autoridad de Certificación Subordinada a la entidad de certificación dentro de la jerarquía que emite los certificados de entidad de los usuarios finales, y su certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Subordinada de PKI SERVICES S.A.S. N2 Emite los certificados finales a suscriptores. En este caso, PKI SERVICES S.A.S. actuará como prestador de servicios de certificación para la SubCA ubicada en Colombia. La SubCA tiene la siguiente Autoridad de Certificación Intermedia de Nivel 3, cuya información más relevante, se detalla en el documento Políticas de Certificados – PC. d) Certificados de usuarios finales

1.3.2 PKI SERVICES CA ROOT

PKI SERVICES Root es la Autoridad de Certificación Raíz (CA Raíz) de PKI SERVICES S.A.S. que emite el certificado de la Autoridad de Certificación Subordinada (CA Subordinada) de la ECD PKI SERVICES S.A.S. (ECD PKI SERVICES). Por tanto, PKI SERVICES Root es la CA Raíz de la jerarquía de certificados de la PKI de PKI SERVICES S.A.S.

PKI SERVICES S.A.S., en su papel de Entidad de Certificación Digital (ECD), es la persona jurídica privada que presta indistintamente servicios de certificación digital.

A PKI SERVICES S.A.S., como ECD, le corresponderá la realización de todos los trámites y procedimientos administrativos necesarios ante ONAC a fin de lograr y mantener la acreditación.

La ECD PKI SERVICES S.A.S., en su papel de CA Subordinada, emite y revoca certificados, y presta los servicios de comprobación de revocación mediante CRL y OCSP.

Asimismo, la ECD PKI SERVICES S.A.S. presta los servicios de Autoridad de Registro, la cual es la encargada de certificar la validez de la información suministrada por el Solicitante de un certificado digital, mediante la verificación de su identidad y el respectivo registro de evidencias, y de gestionar las solicitudes de emisión y de revocación de certificados digitales.

A continuación, se indican los datos de identificación de la ECD PKI SERVICES S.A.S. y de sus proveedores:

1.3.3. IDENTIFICACIÓN DE LA ECD - AC PKI SERVICES S.A.S.


Nombre Razón Social: PKI SERVICES S.A.S.

N.I.T.: 901301044-4

Nº matrícula de Cámara de Comercio: 03136692

Certificado de existencia y representación legal de la Cámara de Comercio y Registro Único Tributario (RUT) se pueden consultar en la sección INF. CORPORATIVA de la página web de PKI SERVICES:

<https://pkiservices.co/>

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 12 de 61

Estado activo en Cámara de Comercio: consultar con NIT 901301044-4 en:

- CONFECAMARAS: <https://www.rues.org.co/> consultar
- DIAN: <https://muisca.dian.gov.co/WebRutMuisca/DefConsultaEstadoRUT.faces>
- Domicilio social y de correspondencia comercial: Calle 127B Bis No. 46-63, Bogotá D.C., Colombia
- Domicilio de correspondencia física notificaciones judiciales: Calle 127B Bis No. 46-63, Bogotá D.C., Colombia.
- Móvil: +57 3506202222
- Dirección de correo electrónico: info@pkiservices.co
- Atención PQRS: Puede consultarse en la sección SERVICIO AL CLIENTE opción SOPORTE PQRS de la página web de PKI SERVICES <https://pkiservices.co/>
- Página Web: www.pkiservices.co
- Certificados Root CA y Subca: Puede consultarse en la sección SERVICIO AL CLIENTE de la página web de PKI SERVICES <https://pkiservices.co/>
- OID: 1.3.6.1.4.1.54689.1

1.3.4. SOLICITANTE

Solicitante; es la persona natural o jurídica que solicita a la ECD PKI SERVICES S.A.S. la emisión de un certificado digital o servicio de certificación digital.

1.3.5. SUSCRIPTOR

Suscriptor: es la persona natural o jurídica a cuyo nombre la ECD PKI SERVICES S.A.S. utiliza un certificado digital y, por tanto, actúa como responsable de este, y que, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en esta DPC y en la PC correspondiente y habiendo firmado el respectivo Contrato de Suscripción con PKI SERVICES S.A.S., acepta las condiciones del servicio de emisión de certificados prestado por éste.

El Suscriptor es el responsable del uso de la clave privada asociada al certificado expedido a su nombre por la ECD PKI SERVICES S.A.S., a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando dicha clave privada.

1.3.6. TERCERO QUE CONFÍA

Tercero que confía (o Tercero aceptante) son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en un certificado digital emitido por la ECD PKI SERVICES S.A.S.

1.3.7. ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL SUSCRIPTOR

Entidad a la cual se encuentra vinculado el Suscriptor es, en su caso, la persona jurídica o persona natural (ya sea ésta una empresa, una organización pública o privada, un colegio profesional o la propia persona natural en el caso de que desempeñe una actividad económica sea ésta del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario) a la que el Suscriptor se encuentra relacionado mediante la vinculación acreditada en el certificado.

1.3.8. ESTAMPA DE TIEMPO (TIME STAMPING)

La estampa de tiempo o time stamping o es el complemento ideal a la seguridad que ofrecen los certificados digitales de identidad. Mediante la aplicación del estampado de tiempo se garantiza el momento exacto en el que se produjo la firma de un documento. El Servicio de Estampado de Tiempo de PKI SERVICES S.A.S. está basado en la especificación del estándar RCF 3161– Internet X509 Public Key Infraestructure. se detalla en el documento Políticas de Certificados – PC.

1.3.9. AUTORIDAD DE LAS POLÍTICAS

Para las jerarquías descritas en este documento la Autoridad de las Políticas (PA) es el comité de políticas y seguridad. Este constituye por lo tanto la Autoridad de las Políticas (PA) de las Jerarquías y Autoridades de Certificación descritas anteriormente siendo responsable de la administración de la DPC el Gerente General y de la aprobación el Comité de Políticas.

Para contactar con la autoridad de las políticas (PA)	
Administrador de la política	Gerente General
Aprobación de políticas	COMITÉ DE POLÍTICAS Y SEGURIDAD
Dirección e-mail	info@pkiservices.co
Dirección	calle 127B bis #46-63
Teléfono	(+57) 350 620 22 22
URL	http://pkiservices.co

1.3.10. PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (ECD)

Esta DPC define al Prestador de Servicios de Certificación (Entidad de Certificación Digital - ECD) como aquella entidad que presta los servicios concretos relativos al ciclo de vida de los certificados digitales y servicios asociados como la emisión de sellos de tiempo (estampado cronológico), provisión de dispositivos de firma o servicios de validación.

Nombre o Razón Social de la ECD - AC	PKI SERVICES S.A.S.
NIT	901301044-4
Nº Matrícula de Cámara Comercio	03136692
Estado Activo en Cámara Comercio	Activo - https://www.rues.org.co/
Domicilio Social y de correspondencia	Calle 127B Bis #46-63 of.102
Teléfono	(+57) 350 620 22 22
Email	info@pkiservices.co
Web	http://pkiservices.co
Oficina Responsable de peticiones, consultas y quejas de los suscriptores y usuarios	http://pkiservices.co sección Servicio al cliente, Soporte PQRS

1.3.11. AUTORIDAD DE REGISTRO (RA)

Una Autoridad de Registro (RA) es la responsable de la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado y cualquier responsabilidad específica establecida en esta DPC y las Políticas de Certificación. Las RA son autoridades delegadas por la ECD, aunque la ECD es en última instancia el responsable del servicio. La ECD puede ejercer en cualquier momento las labores de RA.

1.3.12. OFICIAL DE DECISIÓN

El Oficia de Decisión OD es el funcionario(s) de la ECD responsable de la toma la decisión de emitir o revocar un certificado digital, o de prestar o modificar los servicios de certificación.

1.4.1 SERVICIOS DE CERTIFICACIÓN DIGITAL

1.4.1.1 TIPOS DE CERTIFICADOS DIGITALES

La información de los tipos de certificados digitales que son ofrecidos por PKI SERVICES se encuentra en GE-PO-018 POLITICA DE CERTIFICADOS Puede consultarse en la sección INF. DISPONIBLE de la página web de PKI SERVICES <https://pkiservices.co/>

1.4.1.2 OTROS SERVICIOS DE CERTIFICACIÓN DIGITAL

La información de los tipos de certificados digitales que son ofrecidos por PKI SERVICES se encuentra en GE-PO-018 POLITICA DE CERTIFICADOS Puede consultarse en la sección INF. DISPONIBLE de la página web de PKI SERVICES <https://pkiservices.co/>

1.4.2 USOS APROPIADOS DE LOS CERTIFICADOS

En la descripción de cada tipo de certificado en la presente DPC y en la PC correspondiente se indican los respectivos usos apropiados de los certificados.

En el caso del uso de los certificados para la firma centralizada, los formatos de firmas digitales construidos por servicios ofrecidos por PKI SERVICES S.A.S. siguen los siguientes estándares técnicos:

1.4.3. USOS NO AUTORIZADOS DE LOS CERTIFICADOS

No se permite el uso que sea contrario a la normativa colombiana, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en esta DPC y en la PC correspondiente.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones áreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar a la muerte, lesiones personales o daños medioambientales severos.

Los certificados emitidos a los Suscriptores no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados.

La ECD PKI SERVICES S.A.S. no ofrece el servicio de recuperación de la clave privada, no siendo posible recuperar los datos cifrados con la correspondiente clave pública en caso de pérdida o inutilización de la clave privada o del dispositivo que la custodia por parte del Suscriptor. El Suscriptor que decida cifrar información lo hará en todo caso bajo su propia y única responsabilidad, sin que, en consecuencia, PKI SERVICES S.A.S. tenga responsabilidad alguna por pérdida de información derivada de la pérdida de las claves de cifrado. Por ello, PKI SERVICES S.A.S. no recomienda el uso de los certificados digitales para el cifrado de la información.

1.5. ADMINISTRACIÓN DE LA DPC Y LAS PC

1.5.1 ORGANIZACIÓN RESPONSABLE

Esta Declaración de Prácticas y las Políticas de Certificación son propiedad de PKI SERVICES S.A.S., la administración es responsabilidad de la Gerencia de PKI SERVICES S.A.S

1.5.2 DATOS DE CONTACTO


Para consultas o comentarios relacionados con la presente DPC o las PC asociadas, el interesado podrá dirigirse a PKI SERVICES S.A.S. a través de alguno de los medios siguientes: domicilio social y de correspondencia – comercial, teléfono, fax, direcciones de correo electrónico comercial o PQRS de la Entidad de Certificación Digital indicados en la sección 1.3.3.

se encuentra disponible en nuestra página web, sección SERVICIO AL CLIENTE, opción CONTACTO de la página web de PKI SERVICES <https://pkiservices.co/>

se encuentra disponible en nuestra página web, sección SERVICIO AL CLIENTE, opción SOPORTE PQRS de la página web de PKI SERVICES <https://pkiservices.co/>

1.5.3 PROCEDIMIENTO DE APROBACIÓN

Esta DPC y las PC asociadas son aprobadas por el Comité de Políticas de PKI SERVICES S.A.S.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 15 de 61

antes de ser publicadas, controlando las versiones de estas, a fin de evitar modificaciones y suplantaciones no autorizadas y el uso de documentación obsoleta.

Las nuevas versiones aprobadas de esta DPC y de las PC asociadas son enviadas a ONAC y publicadas en la página web de PKI SERVICES S.A.S. <https://pkiservices.co/> sección INF. DISPONIBLE.

Los cambios en cada nueva versión estarán indicados en la tabla inicial de historial de versiones.

1.6. DEFINICIONES Y ABREVIACIONES

1.6.1 DEFINICIONES

Algoritmo: conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien deba realizar dicha actividad. Dados un estado inicial y siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.

Apelación (PQRS): solicitud presentada por un cliente para reconsiderar cualquier decisión adversa tomada por la ECD con relación a los servicios prestados.

Autoridad de Certificación: Certification Authority (CA). Es una entidad de confianza, responsable de emitir y revocar los certificados digitales, publicación de certificados, publicación de listas de certificados revocados, etc. Nombrada dentro de la normativa colombiana como Entidad de Certificación Digital – ECD.

Autoridad de Registro: persona jurídica, con excepción de los notarios públicos, o parte interna de las ECD necesariamente independiente de su CA, que acorde con la normatividad vigente, es la encargada de recibir las solicitudes relacionadas con certificación digital, para:

- Registrar las peticiones que hagan los solicitantes para obtener un certificado.
- Comprobar la veracidad y corrección de los datos que aportan los usuarios en las peticiones.
- Enviar las peticiones que cumplen los requisitos a una CA para que sean procesadas.

Autoridad de sellado de tiempo (TSA): entidad de confianza que emite sellos de tiempo mediante una o más TSU. Nombrada dentro de la normativa colombiana como Entidad de Certificación Digital – ECD. Los sellos de tiempo emitidos por la ECD, conforme a la regulación establecida por la ONAC, incluyen la fecha y hora referenciada por la fuente de tiempo legal colombiana.

CA Raíz: Autoridad de Certificación de primer nivel, base de confianza.

CA Subordinada: Autoridad de Certificación de segundo nivel o más niveles.

Clave privada: ver Datos de Creación de Firma. **Clave pública:** ver Datos Verificación de Firma

Certificado digital: mensaje de datos electrónico firmado por la ECD, el cual identifica tanto a la ECD que lo expide, como al suscriptor y contiene la clave pública de este último.

Cliente: en los servicios de certificación digital, el término “cliente” identifica a la persona natural o jurídica con la cual la ECD establece una relación comercial.

Corporación (Entidad): persona jurídica o persona natural, ya sea ésta una empresa, una organización pública o privada, un colegio profesional o la propia persona natural en el caso de que desempeñe una actividad económica sea ésta del tipo que sea y para cuyo ejercicio esté obligada a inscribirse en un registro de carácter fiscal o tributario.

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

Datos de Verificación de Firma (Clave pública): datos que son utilizados para verificar que una firma digital fue generada con la clave privada del suscriptor.

Declaración de Prácticas de Certificación (DPC): documento en el que constan de manera detallada los procedimientos que aplica la ECD para la prestación de sus servicios. Una declaración de las prácticas que la ECD emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.

Entidad: ver Corporación

Entidad de Certificación : de acuerdo con lo indicado en la Ley 527 de 1999, Artículo 2, Literal d, aquella persona natural o jurídica que, autorizada conforme a dicha Ley, está facultada para emitir certificados digitales en relación con las firmas digitales de las personas, 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.

Entidades de Certificación Digital – ECD: denominación que se establece con el fin de particularizar y diferenciar este tipo de organizaciones como Entidades de Certificación de los demás Organismos de Certificación que ONAC acredita. Entidad de Certificación que presta el servicio de emisión de certificados, incluyendo otras gestiones propias de certificados digitales, de acuerdo con la regulación establecida por ONAC.

Estampado cronológico (Estampa cronológica, Sello de tiempo o Sellado de tiempo, Time stamp o Time stamping en inglés): mensaje de datos firmado digitalmente y con sello de tiempo por una TSA que vincula a otro mensaje de datos con un momento de tiempo concreto, el cual permite establecer con una prueba que estos datos existan en ese momento y que no sufrieron ninguna modificación a partir del momento en que se realiza el estampado.

Firma Centralizada: se llama “firma centralizada” a la gestión centralizada de los certificados digitales, de manera que estos certificados operen desde un repositorio único, controlado y seguro. De manera práctica esto implica que los certificados digitales son generados y almacenados en el servidor, lo que permite que puedan ser usados desde cualquier ordenador o dispositivo móvil.

Firma Digital: se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático reconocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Función Hash: operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

HSM Centralizado: dispositivo criptográfico en el cual se genera, almacenan y protegen las claves criptográficas de los suscriptores de una forma segura, permitiendo la firma centralizada o firma en la nube.

Lista de Certificados Digitales Revocados (CRL): aquella relación que debe incluir todos los certificados revocados por la ECD.

Log: servicio de registro de eventos del sistema de información, dejando la información anterior y la actual, identifica quién y cuándo se realizó el evento.

Niveles de seguridad: diversos niveles de garantía que ofrecen las variables de firma electrónica cuyos beneficios y riesgos deben ser evaluados por la persona, empresa o institución que piensa optar por una modalidad de firma electrónica para enviar o recibir mensajes de datos o documentos electrónicos.

OID: identificador único de objeto (object identifier). OID. Acrónimo del término en idioma inglés “Object Identifier”, que consiste en un número único de identificación asignado en base a estándares internacionales y comúnmente utilizado para identificar documentos, sistemas, equipos, etc., con la finalidad, entre otras cosas, de conocer el origen, la titularidad y la antigüedad del objeto identificado.

Persona natural individual: persona natural que no sea una Corporación o Entidad.

Petición (PQRS): solicitud presentada por un cliente o parte interesada respecto a los servicios prestados por la ECD.

PKI: Infraestructura de clave pública (Public Key Infrastructure). Es el conjunto de hardware, software, políticas, procedimientos y elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que sólo posee el suscriptor del servicio y una pública, que se incluye en el certificado digital, logran:

- Identificar al emisor de un mensaje de datos electrónico.

- Impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos.
- Impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos.
- Evitar que el suscriptor del servicio de Certificación digital que envió un mensaje electrónico pueda después negar dicho envío.

Política de Certificados (PC): conjunto de reglas que indica los requisitos de un certificado en una comunidad y/o clase en particular, en el marco de los requisitos legales, reglamentarios, y con requisitos de seguridad comunes.

Proveedor: el término “proveedor” incluye a organizaciones, personas, fabricantes, distribuidores, ensambladores de tecnología y otros que suministran productos, bienes y servicios. Entre los proveedores de las ECD están: Entidades recíprocas, empresas de tecnología que prestan servicios en sus diferentes modalidades como son: hosting, colocation, repositorio documental (electrónico o físico), proveedor de dispositivos, proveedor de telecomunicaciones, etc.

Queja (PQRS): expresión de una insatisfacción presentada por un cliente o parte interesada respecto a los servicios prestados por la ECD o al propio proceso de tratamiento de las quejas.

Reclamo (PQRS): expresión de una insatisfacción presentada por un cliente o parte interesada respecto a los servicios prestados por la ECD, por la que se pretende algún tipo de compensación

Revocación: proceso por el cual se inhabilita el certificado digital emitido y se da por terminado su periodo de validez de uso a partir de la fecha de revocación, al presentarse alguna de las causas establecidas en la Declaración de Revocación de Certificación.

Servicio de certificación digital: conjunto de actividades certificación que ofrece la ECD para certificar el origen e integridad de mensajes de datos, basados en las firmas digitales o electrónicas, estampado de tiempo, así como en la aplicabilidad de estándares técnicos admitidos y vigentes en infraestructura de llave pública – PKI.

Sello de tiempo: ver Estampado cronológico.

Servicio del estado del certificado en línea OCSP: actividad de consulta en tiempo real al sistema de la ECD, sobre el estado de un certificado digital a través del protocolo OCSP.

Solicitante: persona natural o jurídica que, con el propósito de obtener servicios de Certificación digital de una ECD, demuestra el cumplimiento de los requisitos establecidos en la DPC y la PC correspondiente para acceder al servicio de Certificación digital. Persona natural o jurídica que solicita a la ECD la emisión de un certificado.

Sugerencia (PQRS): recomendación que propone un cliente o parte interesada para la mejora de los servicios prestados por la ECD.

Suscriptor: persona natural o jurídica a cuyo nombre se expide un certificado digital. Persona natural o jurídica que, habiendo firmado el respectivo Contrato de Suscripción, acepta las condiciones del servicio de emisión de certificados prestado por la ECD.

Tercero que confía (Tercero aceptante): persona natural o jurídica que recibe un documento, log, notificación o cualquier otro dato firmado digitalmente, y que confía en la validez del correspondiente certificado digital emitido por la ECD.

Token: dispositivo hardware criptográfico suministrado por una ECD, el cual contiene el certificado digital y la llave privada del suscriptor.

Unidad de sellado de tiempo (TSU): conjunto de hardware y software que es gestionado como una unidad y tiene una única clave de firma de sellos de tiempo activa en un instante de tiempo.

1.6.2 SIGLAS

CA Certification Authority (Autoridad de Certificación)

CRL Certificate Revocation List (Lista de Certificados Revocados)

DN Distinguished Name (Nombre distinguido)

DPC Declaración de Prácticas de Certificación

ECD Entidad de Certificación Digital que prestan servicios de Certificación digital y equivale a una Entidad Certificadora definida en la ley 527 de 1999. También se debe entender como un Organismo de Evaluación de la Conformidad – OEC de acuerdo con lo definido en la ISO/IEC 17000.

FIPS Federal Information Processing Standards (FIPS, en español Estándares Federales de Procesamiento de la Información). Son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno. Muchos estándares FIPS son versiones modificadas de los estándares usados en las comunidades más amplias (ANSA, IEEE, ISO, etc).

HSM Hardware Security Module

IEC International Electrotechnical commission

ISO International Organization for Standardization

ITU International Telecommunication Union

NIF Número de Identificación Tributaria

NIT Número de Identificación Tributaria

NOC Network Operation Center

OCSP Online Certificate Status Protocol (Servicio del estado del certificado en línea)

ONAC Organismo Nacional de Acreditación de Colombia

PC Política de Certificados

PKCS Public-Key Cryptography Standards. Estándares de criptografía de llave pública concebidos y publicados por los laboratorios de RSA.

PKI Public Key Infrastructure (Infraestructura de clave pública)

PQRS Peticiones, Quejas, Reclamos, Sugerencias y Apelaciones

RA Registration Authority (Autoridad de Registro)

RFC Request for Comments. Son una serie de publicaciones del Internet Engineering Task Force (IETF) que describen diversos aspectos del funcionamiento del Internet y otras redes de computadoras, como protocolos, procedimientos, etc.

RSA Rivset, Shamir y Adleman. Es un sistema criptográfico de llave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

RUES Registro Único Empresarial y Social

SHA Secure Hash Algorithm (Algoritmo de seguridad HASH)

SOC Security Operation Center

TSA Time Stamping Authority (Autoridad de sellado de tiempo)

TSU Time Stamping Unit (Unidad de sellado de tiempo)

2. RESPONSABILIDADES SOBRE REPOSITORIOS Y PUBLICACIÓN DE INFORMACIÓN

2.1. REPOSITORIOS

La siguiente información puede ser consultada en sección INF. DISPONIBLE de la página web de PKI SERVICES <https://pkiservices.co/>

- Certificado CA Raíz de PKI SERVICES S.A.S.

- Certificado CA Subordinada de PKI SERVICES S.A.S.
- Lista de Certificados Revocados (CRL)

2.2. PUBLICACIÓN DE LA INFORMACIÓN DE CERTIFICACIÓN

El Comité de Políticas de PKI SERVICES S.A.S. se encarga de la aprobación de la DPC, las PC las políticas y el Contrato de Suscripción. Puede consultarse en la sección INF. DISPONIBLE de la página web de PKI SERVICES <https://pkiservices.co/>

2.3. PLAZO O FRECUENCIA DE LA PUBLICACIÓN

Certificados de CA Raíz y CA Subordinada

Los certificados de la CA Raíz y la CA Subordinada se publicarán y permanecerán en la página web de PKI SERVICES S.A.S. durante todo el tiempo en que la ECD esté prestando servicios de certificación digital.

Lista de Certificados Revocados (CRL)

PKI SERVICES S.A.S. publicará en su página web las CRL de la CA Raíz y la CA Subordinada en los eventos y con la periodicidad definidas en la sección 4.9.6.

Declaración de Prácticas de Certificación (DPC), Políticas de Certificados (PC) y Contrato de Suscripción

PKI SERVICES S.A.S publicará en su página web cada nueva versión aprobada de la DPC, las PC y el Contrato de Suscripción, sustituyendo a la anterior versión que no se mantendrá en la página web.

2.4 CONTROLES DE ACCESO A LOS REPOSITORIOS

Los repositorios disponibles antes mencionados son de libre acceso para su consulta al público en general. La integridad y disponibilidad de la información publicada es responsabilidad de PKI SERVICES S.A.S.

La organización cuenta con los recursos y procedimientos necesarios para restringir el acceso a estos repositorios con otros fines diferentes a la consulta por parte de personas ajenas a PKI SERVICES S.A.S.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1.1 CUMPLIMIENTO AL PRINCIPIO CONSTITUCIONAL DE LA BUENA FE

PKI SERVICES S.A.S. debe dar cumplimiento al artículo 83 de la constitución política colombiana, sobre el principio de la buena fe: “Las actuaciones de los particulares y de las autoridades públicas deberán ceñirse a los postulados de buena fe, la cual se presumirá en todas las gestiones que aquéllos adelanten ante éstas.”

3.1.2 FALSEDAD EN DOCUMENTO PRIVADO.

Los solicitantes y/o suscriptores deben dar cumplimiento a la LEY 599 DE 2000, por la cual se expide el Código Penal Artículo 289. “Falsedad en documento privado. El que falsifique documento privado que pueda servir de prueba, incurrirá, si lo usa, en prisión de uno (1) a seis (6) años.”


PKI SERVICES S.A.S. se reserva el derecho de no emitir el certificado si considera que la COMPROBACIÓN Biométrica facial no corresponde, o si el documento de identificación no corresponde, o si el solicitante se encuentra en una de las listas de lavado de activos o si documentación aportada no es suficiente.

3.2. NOMBRES

3.2.1. TIPOS DE NOMBRES

Todos los certificados requieren un nombre distinguido (DN o distinguished name) del titular conforme al estándar X.500.

Adicionalmente, los DN de los titulares de los certificados son coherentes con lo dispuesto

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 20 de 61

en los siguientes estándares:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

3.2.2 NECESIDAD DE QUE LOS NOMBRES TENGAN SIGNIFICADO

Los campos del DN del titular del certificado referentes a Nombres y apellidos y/o a Nombre o Razón social se corresponderán con los datos registrados legalmente del Suscriptor, expresados exactamente en el formato que consten en la Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte y/o en el Certificado de Cámara de Comercio y/o Registro Único Tributario (o documentos equivalentes).

En el caso de que los datos consignados en el DN del titular del certificado fueran ficticios o se indique expresamente su invalidez en dicho DN (ej. mediante la palabra “PRUEBA” o “INVALIDO”), se considerará al certificado sin validez legal, únicamente válido para realizar pruebas técnicas de interoperabilidad.

3.2.3. ANONIMATO Y SEUDOANONIMATO DE LOS SUSCRIPTORES

No se admiten anónimos ni seudónimos para identificar a los suscriptores.

3.2.4. UNICIDAD DE LOS NOMBRES

El nombre distinguido (DN) de los titulares de los certificados emitidos será único para cada Suscriptor.

Los atributos del DN del titular del certificado que contienen el tipo y el número del documento de identidad y/o el número de identificación fiscal se usan para distinguir entre dos identidades cuando exista algún problema de duplicidad de nombres.

3.2.5. RECONOCIMIENTO, AUTENTICACIÓN Y PAPEL DE LAS MARCAS REGISTRADAS

La ECD no asume compromisos en la emisión de certificados respecto al uso por los Suscriptores de una marca comercial.

PKI SERVICES S.A.S. no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del Suscriptor. Sin embargo, la ECD no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

3.3 VALIDACIÓN DE LA IDENTIDAD

3.3.1 MÉTODO DE PRUEBA DE POSESIÓN DE LA CLAVE PRIVADA

En la PC de cada tipo de certificado se especifica el método de prueba de posesión de la clave privada para cada uno de los tipos de soporte en los que se pueden emitir los correspondientes certificados.

3.3.2 AUTENTICACIÓN DE LA IDENTIDAD DE UNA PERSONA NATURA

La RA verificara de forma fehaciente la identidad de la Persona Natural solicitante contra su documento de identidad en línea. Para ello, la Persona Natural deberá escanear su cara y enviar un documento reconocido en derecho que le identifique y mostrar el documento original durante la videoconferencia. Este mecanismo de autenticación se denomina reconocimiento biométrico facial vivo.

La RA validará que el documento de identidad presentado sea aparentemente legítimo y que los datos contenidos en el mismo (país de expedición, tipo y número del documento de identidad, nombres y apellidos) son conformes a los correspondientes datos ingresados en el formulario de solicitud del certificado. Asimismo, valida que la cara corresponda al documento de identidad presentado.

La RA guardará la documentación relativa al sustento de la validación de la identidad de la persona natural individual Suscriptor y/o Solicitante del certificado.

3.3.3. AUTENTICACIÓN DE LA IDENTIDAD DE UNA ENTIDAD

Para expedir los certificados digitales, la RA pide al solicitante los siguientes datos para poder autenticar la identidad de la Persona Jurídica o Persona Natural:

- Los datos relativos al nombre o razón social de la Entidad (Persona Jurídica o Persona Natural).
- Los datos relativos a la constitución y personalidad jurídica de la Entidad (Persona Jurídica).
- Los datos relativos a la extensión y vigencia de las facultades de representación del representante legal de la Entidad (Persona Jurídica).
- Los datos relativos al número de identificación tributaria de la Corporación o Entidad (Persona Jurídica o Persona Natural).
- Los datos relativos a la dirección completa de la Entidad (Persona Jurídica o Persona Natural).

La RA verificará los datos anteriores mediante:

- Solicitud de la cédula de ciudadanía o documento reconocido en derecho que lo identifique
- Solicitud de Certificado de la Cámara del Comercio o documento equivalente, en los casos que sea aplicable; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.
- Solicitud de Registro Único Tributario o documento equivalente, en todos los casos; expedido en Colombia (por defecto) o en otro país.
- Solicitud de un documento oficial adicional en el que sustente el alcance del certificado digital solicitado.
- El mecanismo de identificación es en línea, por medio de identificación biométrica facial viva, se compara contra documento de identidad reconocido en derecho que lo identifique, y el certificado de existencia y representación contra Registro único empresarial. RUES de Confecámaras, para verificar la existencia de la Entidad y que se encuentra activa.

PKI SERVICES S.A.S. se reserva el derecho de no emitir el certificado si considera que la documentación aportada no es suficiente o para la comprobación de los datos anteriormente citados.

La RA guardará la documentación relativa al sustento de la validación de la identidad de la Corporación o Entidad identificada en el certificado.

3.3.4. INFORMACIÓN DE SUSCRIPTOR Y SOLICITANTE NO VERIFICADA

Bajo ninguna circunstancia la RA omitirá las labores de verificación de información que conduzcan a la identificación del Suscriptor y del Solicitante según lo especificado en las secciones 3.2.

3.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN DE CAMBIO DE CLAVES


PKI SERVICES S.A.S. no atiende requerimientos de renovación de certificados digitales con cambio de claves.

Los casos en los que se requiera un nuevo certificado digital con cambio de claves, por expiración, próxima expiración o revocación de un certificado, se tratan como una nueva emisión de certificado, realizándose la misma validación de identidad que se hizo inicialmente para el primer certificado digital, según lo especificado en la sección 3.2.

3.5. IDENTIFICACIÓN Y AUTENTICACIÓN PARA PETICIONES DE REVOCACIÓN

La identificación y autenticación del Suscriptor o Solicitante para una petición de revocación de un certificado podrá ser realizada por:

- **ONLINE:** El propio Suscriptor o Solicitante, en el caso de que éste utilice el procedimiento de revocación online. En la PC de cada tipo de certificado se especifica el método por el que se identifica y autentica al Suscriptor o Solicitante para una petición de revocación online, dependiendo del tipo de certificado que haya sido emitido.
- **SOLICITUD EN PQRS:** En el caso de que el Suscriptor o Solicitante utilice el procedimiento de revocación mediante solicitud PQRS, debe estar previamente registrado en nuestra página web <https://pkiservices.co> seguido a esto se efectuara por medio en una comunicación enviada por solicitud de Revocación en el sistema PQRS. canal que recibe y gestiona PQRS, paso posterior reenvía al Oficial

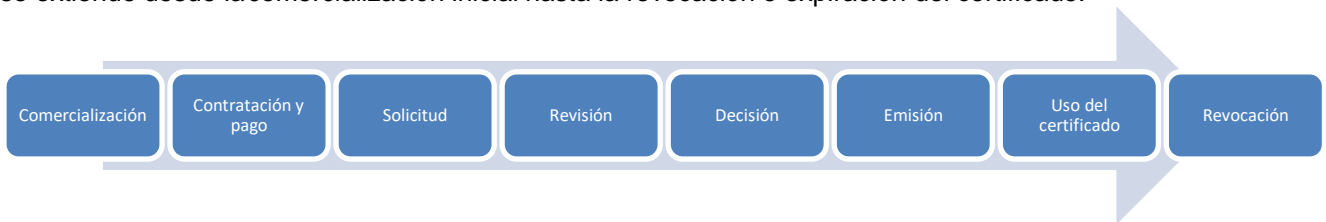
	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 22 de 61

de Decisión.

– SOLICITUD INTERNA: En el caso de que una solicitud de revocación se produce al interior de PKI SERVICES, el solicitante debe usar el procedimiento de revocación mediante solicitud PQRS, debe estar previamente registrado en nuestra página web <https://pkiservices.co> seguido a esto se efectuara por medio en una comunicación enviada por solicitud de Revocación en el sistema PQRS. canal que recibe y gestiona PQRS, paso posterior reenvía al Oficial de Decisión.

4.REQUISITOS OPERACIONALES PARA EL CICLO DE VIDA DE CERTIFICADOS

El ciclo de vida de los certificados digitales emitidos por PKI SERVICES S.A.S. PKI SERVICES S.A.S. se extiende desde la comercialización inicial hasta la revocación o expiración del certificado.



4.1. SOLICITUD DE CERTIFICADOS

4.1.1. QUIÉN PUEDE SOLICITAR UN CERTIFICADO

- 1) El futuro Suscriptor que sea Persona Natural y que sustente correctamente la información requerida por la RA, según lo especificado en la sección 4.1.4 y en la PC respectiva.
- 2) Una Persona Natural individual (no Corporación o Entidad) vinculada a la Corporación o Entidad futuro Suscriptor (Persona Jurídica o persona Natural), incluyendo un representante legal, apoderado, empleado o persona autorizada por un representante legal de la Persona Jurídica Suscriptor o por la propia Persona Natural Suscriptor a solicitar y obtener un certificado para sistemas de firma digital para la actuación administrativa automatizada, que pueda sustentar correctamente la información requerida por la RA, según lo especificado en la sección 4.1.4 y en la PC respectiva.
- 3) Una Corporación o Entidad (Persona Jurídica o Persona Natural) distinta a la Corporación o Entidad futuro Suscriptor, que haya sido autorizada por el representante legal de la Persona Jurídica Suscriptor o por la propia Persona Natural Suscriptor a solicitar y obtener un certificado para sistemas de firma digital para la actuación administrativa automatizada, que pueda sustentar correctamente la información requerida por la RA, según lo especificado en la sección 4.1.4 y en la PC respectiva.

4.1.2 COMERCIALIZACIÓN

El Solicitante y/o, en los casos que sea aplicable, el Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor podrán recibir información acerca del proceso de certificación digital de las siguientes maneras:

- Consultando la página web <https://pkiservices.co>
- Mediante correo electrónico informativo desde la dirección comercial
- El trato directo con Agentes comerciales.
- Por medio de una PQRS dispuesta en la página web <https://pkiservices.co> sección SERVICIO AL CLIENTE, opción SOPORTEPQRS.

Por cualquiera de estos medios, se les brindará información acerca de dicho proceso, requisitos necesarios, tarifas u otros relativos.

Luego de ser informado el Solicitante, en los casos que sea aplicable, el Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor indicarán en la página web <https://pkiservices.co> sección SERVICIOS

- 1) El tipo de certificado requerido y, si éste admite varios tipos de soporte, el tipo de soporte requerido.
- 2) La vigencia del certificado requerida.

- 3) El nombre completo del Solicitante.
- 4) El tipo y el número de su documento de identidad del Solicitante.
- 5) La cuenta de correo electrónico del Solicitante que estará asociada al certificado digital y por medio de la cual PKI SERVICES S.A.S. le realizará notificaciones y comunicaciones oficiales. Cabe destacar que, para los certificados personales, se debe indicar la cuenta de correo electrónico personal y para los certificados corporativos, la cuenta de correo electrónico corporativa.

En los casos que sea aplicable:

- 6) El nombre o la razón social del Suscriptor o de la Entidad a la cual se encuentra vinculado el Suscriptor.
- 7) El NIT del Suscriptor o de la Entidad a la cual se encuentra vinculado el Suscriptor.

Si el Solicitante es una Persona Natural individual, el Área Comercial y/o un OD enviarán por correo electrónico al Solicitante y/o, en los casos que sea aplicable, al Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor: la Propuesta Comercial, en los casos que sea aplicable; el Contrato de Suscripción; en los tipos de certificado que lo permiten, un modelo de autorización para la solicitud y obtención del certificado en el caso de que se requiera; opcionalmente, un enlace a la plataforma; y las indicaciones respectivas.

4.1.3 CONTRATACIÓN Y PAGO

Para proceder a prestar los servicios certificación digital o servicios digitales, el Solicitante y/o Suscriptor bien sea persona natural o jurídica en los casos que sea aplicable, deberán:

- Leer y aceptar los términos y condiciones que es el contrato de adhesión con firma electrónica en el marco del decreto 2364 de 2012. La evidencia de este proceso de aceptación de términos y condiciones será la compra del servicio paso posterior a aceptación de términos y condiciones.

Cabe resaltar que, además del contrato de adhesión de Aceptación de Términos y Condiciones, a solicitud del solicitante y/o suscriptor, se podría elevar un Contrato de Prestación de Servicios entre PKI SERVICES S.A.S. y el solicitante y/o suscriptor bien sea persona natural o jurídica.

Las minutas de los contratos que pueden ser ajustados según las partes, son:

- GC-CN-001 CONTRATO DE SUSCRIPTORES Y/O SOLICITANTE
- GC-CN-002 CONTRATO DE SUMINISTRO DE MARCAS DE TIEMPO
- GC-CN-003 CONTRATO DE SUMINISTRO DE NOTIFICACIÓN ELECTRÓNICA
- GC-CN-004 CONTRATO DE REGISTRO, CUSTODIA Y ANOTACIÓN DE DOCUMENTOS ELECTRÓNICOS TRANSFERIBLES

Realizar el pago de la tarifa respectiva por un método válido y dispuesto por PKI SERVICES S.A.S., en los casos que sea aplicable. La evidencia de este proceso será el voucher o comprobante de pago.

4.1.4 SOLICITUD

El proceso de solicitud de emisión dependerá del tipo de certificado requerido. En la PC de cada tipo de certificado se especifica el proceso particular de solicitud de emisión para los correspondientes certificados. A continuación, se describe el proceso general de solicitud de emisión.

Para solicitar la emisión de un certificado digital, el Solicitante y/o, en los casos que sea aplicable, al Suscriptor y/o la Entidad a la cual se encuentra vinculado el Suscriptor deberán ingresar al sistema expuesto en la plataforma web <https://pkiservices.co/>. Dentro de la plataforma, procederán a ingresar los datos requeridos y adjuntar los documentos solicitados, para finalmente guardar su solicitud.

La RA de PKI SERVICES S.A.S. solicita toda la información necesaria para la verificación de identidad del Solicitante y/o del Suscriptor. Los documentos requeridos dependerán del tipo de certificado (especificado en la PC respectiva), los cuales pueden ser y no se limitan a los siguientes:

- Cédula de Ciudadanía, Cédula de Extranjería o Pasaporte del Solicitante (Persona Natural individual); expedido en Colombia (por defecto) o en otro país (documento equivalente).
- Certificado de Cámara del Comercio o documento equivalente del Suscriptor o de la Entidad a la que se encuentra vinculado el Suscriptor; expedido en Colombia (por defecto) o en otro país un máximo de 30 días antes.
- Registro Único Tributario o documento equivalente del Suscriptor o de la Entidad a la que se encuentra vinculado el Suscriptor; expedido en Colombia (por defecto) o en otro país (documento equivalente).
- Autorización firmada por el Representante Legal de la Persona Jurídica, o por la propia Persona Natural, del Suscriptor o de la Entidad a la que se encuentra vinculado el Suscriptor, con los datos de la Persona Natural o de la Persona Jurídica autorizada a solicitar y obtener un certificado digital; expedida un máximo de 30 días antes.
- Documento de identificación: Cédula de Ciudadanía, Cédula de Extranjería o pasaporte del Representante Legal de la Persona Jurídica, o por la propia Persona Natural, que firma la autorización; expedido en Colombia (por defecto) o en otro país (documento equivalente).

Asimismo, la RA de PKI SERVICES S.A.S. PKI SERVICES S.A.S. solicita los siguientes documentos adicionales para la emisión de un certificado:

- Constancia del pago de la tarifa del certificado indicada en la Propuesta Comercial, en los casos que sea aplicable.
- Aceptación de términos y condiciones y/o Contrato de Suscripción firmado según el caso.

PKI SERVICES S.A.S. cuenta con el derecho de solicitar documentos adicionales para garantizar la correcta autenticación del Solicitante y/o del Suscriptor y llevar a cabo un adecuado servicio de certificación digital.

4.2. TRAMITACIÓN DE SOLICITUD DE CERTIFICADOS

4.2.1 REVISIÓN

Es responsabilidad de la RA realizar de forma fehaciente en línea y de manera automática la identificación y autenticación del Solicitante y/o Suscriptor de acuerdo al tipo de certificado solicitado, y según lo especificado en las secciones 3.2.2 y 3.2.3 y en la PC correspondiente, previo pago en línea.

Si hace falta regularizar pagos o documentación, se notificará lo requerido a la dirección de correo electrónico declarada por el Solicitante.

Una vez que el OD ha validado los documentos presentados y los datos ingresados en el formulario de solicitud de certificado y que, en el caso de que el Solicitante sea una Persona Natural individual, ha verificado su identidad, el OD aprobará la solicitud de emisión en la plataforma de la RA.

Si la información o verificación de identidad no fuese correcta, la RA deberá denegar la petición, contactando al Solicitante para comunicarle el motivo.

4.2.2 DECISIÓN

El OD de PKI SERVICES S.A.S. PKI SERVICES S.A.S. es responsable de la decisión tomada con respecto a la certificación digital. Es decir, PKI SERVICES S.A.S. es responsable de aprobar o denegar la certificación digital. En el caso de denegación, PKI SERVICES S.A.S. se encarga de comunicar el motivo del rechazo al Solicitante.

4.3. EMISIÓN DE CERTIFICADOS

4.3.1 ACCIONES DE PKI SERVICES S.A.S. DURANTE LA EMISIÓN DE CERTIFICADOS

Una vez aprobada la solicitud, se procederá a la emisión del certificado, que deberá ser emitido de forma segura al Suscriptor:

- Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Protege la confidencialidad e integridad de los datos de registro.
- Todos los certificados iniciarán su vigencia en el momento que se indica en el propio certificado.

En la PC de cada tipo de certificado se especifican las acciones particulares de PKI SERVICES S.A.S. durante la emisión del certificado para cada uno de los tipos de soporte en los que se pueden emitir los correspondientes certificados.

4.3.2 NOTIFICACIÓN AL SOLICITANTE POR PKI SERVICES S.A.S. DE LA EMISIÓN DEL CERTIFICADO

PKI SERVICES S.A.S. PKI SERVICES S.A.S. notificará al Solicitante la emisión del certificado y le enviará por correo electrónico la documentación de la certificación digital.

En la PC de cada tipo de certificado se especifica cómo notifica PKI SERVICES S.A.S. al Solicitante la emisión del certificado y qué documentación de la certificación digital le envía, para cada uno de los tipos de soporte en los que se pueden emitir los correspondientes certificados.

4.4. ACEPTACIÓN DEL CERTIFICADO

4.4.1 FORMA EN LA QUE SE ACEPTA EL CERTIFICADO

El certificado se considerará aceptado por el Suscriptor y por el Solicitante, una vez que PKI SERVICES S.A.S. ha notificado la misma al Solicitante, según lo especificado en la PC respectiva.

4.4.2 PUBLICACIÓN DEL CERTIFICADO POR PKI SERVICES S.A.S.

PKI SERVICES S.A.S. publica los certificados emitidos en el repositorio.

4.4.3 NOTIFICACIÓN DE LA EMISIÓN DEL CERTIFICADO POR PKI SERVICES S.A.S. A OTRAS ENTIDADES

PKI SERVICES S.A.S. no notifica la emisión de certificados a terceros.

4.5. USOS DE LAS CLAVES Y EL CERTIFICADO

4.5.1 USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR EL SUScriptor

Los certificados podrán ser utilizados según lo estipulado en esta DPC y la PC respectiva.

Las extensiones Key Usage y Extended Key Usage podrán ser utilizadas para establecer límites técnicos a los usos de la clave privada del certificado correspondiente. La aplicación de estos límites dependerá en gran parte de su correcta implementación por aplicaciones informáticas de terceros, quedando su regulación fuera del alcance de este documento.


4.5.2. USO DE LA CLAVE PRIVADA Y DEL CERTIFICADO POR TERCEROS QUE CONFÍAN

Los Terceros que confían en los certificados podrán utilizar los certificados para aquello que establece la presente DPC y la PC respectiva.

Es responsabilidad de los Terceros que confían verificar el estado del certificado mediante los servicios ofrecidos por PKI SERVICES S.A.S. los cuales pueden ser consultados en la sección SERVICIOS de la página web de PKI SERVICES <https://pkiservices.co/> concretamente para ello y especificados en el presente documento.

4.6. RENOVACIÓN DEL CERTIFICADO SIN CAMBIO DE CLAVES

PKI SERVICES S.A.S. PKI SERVICES S.A.S. no atiende requerimientos de renovación de certificados digitales, el suscriptor deberá solicitar un nuevo certificado.

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 26 de 61

Los casos en los que se requiera un nuevo certificado digital, por expiración, próxima expiración o revocación de un certificado, se tratan como una nueva emisión de certificado.

4.7. RENOVACIÓN DEL CERTIFICADO CON CAMBIO DE CLAVES

PKI SERVICES S.A.S. PKI SERVICES S.A.S. no atiende requerimientos de renovación de certificados digitales, el suscriptor deberá solicitar un nuevo certificado.

Los casos en los que se requiera un nuevo certificado digital, por expiración, próxima expiración o revocación de un certificado, se tratan como una nueva emisión de certificado.

4.8. MODIFICACIÓN DE CERTIFICADOS

PKI SERVICES S.A.S. PKI SERVICES S.A.S. no atiende requerimientos de modificación de certificados digitales, se revoca y el suscriptor deberá solicitar un nuevo certificado.

Los casos en los que se requiera modificar algún dato en un certificado digital (actualización de la información contenida en un certificado) se tratan como una revocación de certificado y una nueva emisión de certificado.

4.9. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

La revocación de un certificado supone la pérdida de validez del mismo y es irreversible. Las revocaciones tienen efecto desde el momento en que aparecen publicadas en la CRL, estas pueden ser consultadas en la sección SERVICIO AL CLIENTE de la página web de PKI SERVICES <https://pkiservices.co/> Asimismo, no se permite la suspensión de certificados que no conduzca a un estado de revocación inmediato. La ED PKI SERVICES S.A.S. no realiza suspensiones de certificados.

En caso de que se revoque un certificado con relación a las firmas electrónicas o digitales, posteriormente el mismo NO podrá ser rehabilitado por la ECD.

4.9.1 CIRCUNSTANCIAS O CAUSAS PARA LA REVOCACIÓN DE UN CERTIFICADO

La revocación de un certificado digital podrá darse ya sea por solicitud del suscriptor, o cuando la ECD conoce, tiene indicios o confirmación de alguna de las siguientes situaciones:

- a) Por compromiso de la seguridad en cualquier motivo, modo, situación o circunstancia.
- b) Por muerte o incapacidad sobrevenida del suscriptor.
- c) Por liquidación de la persona jurídica representada que consta en el servicio de certificación digital.
- d) Por la confirmación de que alguna información o hecho contenido en el certificado digital es falso.
- e) Por la ocurrencia de hechos nuevos que provoquen que los datos originales no correspondan a la realidad.
- f) Por orden judicial o de entidad administrativa competente.
- g) Por pérdida, inutilización del certificado digital que haya sido informado a la ECD.
- h) Por la terminación del contrato de suscripción, de conformidad con las causales establecidas en el contrato.
- i) 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 servicio.
- j) Por el manejo indebido por parte del suscriptor del certificado digital.
- k) Por el incumplimiento del suscriptor o de la persona jurídica que representa o a la que está vinculado a través del Contrato del Servicio de Certificación Digital proporcionado por la ECD.

4.9.2 QUIÉN PUEDE SOLICITAR UNA REVOCACIÓN

Pueden solicitar la revocación de un certificado:

- El propio Suscriptor y/o Solicitante, que deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias o causas de revocación establecidas.
- Cualquier persona podrá solicitar la revocación de un certificado en caso de tener conocimiento de alguna de las circunstancias o causas de revocación establecidas.
- Los funcionarios autorizados por PKI SERVICES S.A.S.

4.9.3 PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

Existen dos alternativas a la hora de solicitar la revocación del certificado. En todo caso, en el momento de revocarse el certificado, se enviará un comunicado al Suscriptor, comunicando la hora y la causa de esta.

4.9.3.1 Procedimiento Online

PKI SERVICES S.A.S. brinda a los suscriptores el servicio de revocación del certificado online a través de la sección SERVICIOS de la página web de PKI SERVICES <https://pkiservices.co/> Los Suscriptores que deseen revocar sus certificados deberán citar una de las causas de revocación establecidas.

4.9.3.2 Mediante PQRS

PKI SERVICES S.A.S. brinda el servicio de revocación de un certificado generando un ticket de solicitud de Revocación en PQRS ubicado en la sección SERVICIO AL CLIENTE opción SOPORTE PQRS de la página web de PKI SERVICES <https://pkiservices.co/>, citando una de las causas de revocación establecidas. Esta solicitud será transferida al Oficial de Decisión para que valide la identidad y la causa de revocación, y tome la decisión de revocar o no.

Unilateralmente PKI SERVICES puede revocar un certificado siempre y cuando atienda a una de las causas establecidas para revocar un certificado de la siguiente forma:

– SOLICITUD INTERNA: En el caso de que una solicitud de revocación se produzca al interior de PKI SERVICES, el solicitante debe usar el procedimiento de revocación mediante solicitud PQRS, debe estar previamente registrado en nuestra página web <https://pkiservices.co> seguido a esto se efectuara por medio en una comunicación enviada por solicitud de Revocación en el sistema PQRS. canal que recibe y gestiona PQRS, paso posterior reenvía al Oficial de Decisión para que tome la decisión de revocar o no.

4.9.4 PLAZO EN EL QUE PKI SERVICES S.A.S. DEBE RESOLVER LA SOLICITUD DE REVOCACIÓN

PKI SERVICES establece como tiempo máximo de 5 días hábiles para tramitar una revocación.

4.9.5 OBLIGACIÓN DE VERIFICACIÓN DE LAS REVOCACIONES POR LOS TERCEROS QUE CONFÍAN

La verificación del estado de los certificados es obligatoria para cada uso de los certificados, ya sea mediante la consulta de la lista de revocaciones (CRL) o del servicio OCSP.

4.9.6 FRECUENCIA DE EMISIÓN DE LAS CRLS

La CRL de PKI SERVICES Root (CA Raíz) se emite antes de que hayan transcurrido 180 días desde la emisión de la anterior CRL (antes de su fin de validez) o cuando se produzca una revocación.

La CRL de PKI SERVICES S.A.S. PKI SERVICES (CA Subordinada) se emite al menos cada 4 días (antes del fin de validez de la anterior CRL); en condiciones normales, la CRL se emite cada 24 horas.

4.9.7 TIEMPO MÁXIMO ENTRE LA GENERACIÓN Y LA PUBLICACIÓN DELAS CRLS

Una vez emitida la CRL de PKI SERVICES Root (CA Raíz), ésta se publica al menos antes del fin de validez de la anterior CRL (180 días después de su emisión); en condiciones normales, la CRL se publica

el mismo día de su emisión.

Una vez emitida la CRL de PKI SERVICES S.A.S. PKI SERVICES (CA Subordinada), ésta se publica al menos antes del fin de validez de la anterior CRL (4 días después de su emisión); en condiciones normales, la CRL se publica en el momento de la generación de esta, por lo que se considera cero o nulo el tiempo transcurrido.

4.9.8 DISPONIBILIDAD DEL SISTEMA EN LÍNEA DE VERIFICACIÓN DEL ESTADO DE LOS CERTIFICADOS

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana a través de la página web de PKI SERVICES <https://pkiservices.co/> sección INF. DISPONIBLE. En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de PKI SERVICES S.A.S. ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 8 horas.

4.9.9 REQUISITOS DE COMPROBACIÓN DE REVOCACIÓN EN LÍNEA

Para el uso del servicio de CRLs, de libre acceso, deberá considerarse lo siguiente:

- Se deberá comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión CRL Distribution Points.
- Se deberá comprobar adicionalmente la(s) CRL(s) pertinentes de la cadena de Certificación de la jerarquía.
- Se deberá comprobar que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.
- Los certificados revocados que expiren podrán ser retirados de la CRL.

También se puede comprobar la revocación en línea por medio del servicio OCSP, de libre acceso, en la dirección URL contenida en el propio certificado en la extensión Authority Information Access.

4.10. SERVICIOS DE INFORMACIÓN DEL ESTADO DE CERTIFICADOS

4.10.1 CARACTERÍSTICAS OPERACIONALES

Con el fin de proporcionar información sobre la validez de un certificado electrónico, y por consiguiente de la fiabilidad de la firma electrónica de un documento, PKI SERVICES S.A.S., ofrece un servicio gratuito de publicación en Web de Listas de Certificados Revocados (CRL) sin restricciones de acceso.

PKI SERVICES S.A.S. ofrece un servicio gratuito de acceso a validación de certificados en línea por medio del protocolo OCSP.

Adicionalmente, PKI SERVICES S.A.S. puede ofrecer servicios comerciales de validación de certificados.

4.10.2 DISPONIBILIDAD DEL SERVICIO

La información relativa al estado de los certificados estará disponible en línea las 24 horas del día, los 7 días de la semana.

En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de PKI SERVICES S.A.S., ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 8 horas

4.10.3 CARACTERÍSTICAS ADICIONALES

PKI SERVICES S.A.S. puede disponer de servicios avanzados de validación de certificados que requieran de una licencia específica.

4.11. FINALIZACIÓN DE LA SUSCRIPCIÓN

La suscripción del certificado finalizará en el momento de expiración o revocación del certificado.

4.12. CUSTODIA Y RECUPERACIÓN DE CLAVES (KEY ESCROW AND RECOVERY)

PKI SERVICES S.A.S. no ofrece un servicio de custodia de copias de respaldo y recuperación de claves privadas de los suscriptores (key escow).

5. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

Los sistemas y equipamientos empleados para las operaciones del servicio de certificación digital se encuentran administrados en el Centro de Datos subcontratado, el cual tiene certificado ISO 9001, ISO 27001 y TIER III

Los controles de seguridad abarcan el ambiente físico, las redes, los sistemas, entre otros; los cuales se enumeran a continuación.

5.1. CONTROLES FÍSICOS

PKI SERVICES S.A.S. tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas y los equipamientos empleados para las operaciones.

La seguridad física y ambiental aplicable a los servicios de generación de certificados ofrece protección frente:

- Accesos físicos no autorizados.
- Desastres naturales.
- Incendios.
- Fallo de los sistemas de apoyo (energía eléctrica, telecomunicaciones, etc.)
- Inundaciones.
- Robo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios de PKI SERVICES S.A.S.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso. La localización de las instalaciones garantiza la presencia de fuerzas de seguridad en un plazo no superior a 30 minutos.

5.1.1 UBICACIÓN FÍSICA Y CONSTRUCCIÓN

Las instalaciones de la data center están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta, y ubicadas en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas posee falso suelo, detección y extinción de incendios, sistemas anti-humedad, sistema de refrigeración y sistema de suministro eléctrico.

5.1.2 ACCESO FÍSICO

El acceso físico a las dependencias donde se llevan a cabo procesos de Certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por circuito cerrado de televisión.


El acceso a las salas se realiza con lectores de tarjeta de identificación

5.1.3 ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

Las instalaciones de la data center disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado mediante un grupo electrógeno redundante con depósitos de combustible que pueden ser rellenados desde el exterior.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4 EXPOSICIÓN AL AGUA

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 30 de 61

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 PREVENCIÓN Y PROTECCIÓN DE INCENDIOS

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

5.1.6 SISTEMA DE ALMACENAMIENTO

Los sistemas del servidor se ejecutan mediante el despliegue de un entorno virtualizado en alta disponibilidad, soportado sobre dispositivos redundantes de computación, almacenamiento de alto rendimiento y redes independientes de producción, gestión y almacenamiento.

5.1.7. ELIMINACIÓN DEL MATERIAL DE ALMACENAMIENTO DE LA INFORMACIÓN

Cuando haya dejado de ser útil, la información sensible, es destruida en la forma más adecuada al soporte que la contenga:

- Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.
- Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado, mediante su destrucción física o haciendo ilegible la información contenida.

5.1.8. COPIAS DE SEGURIDAD FUERA DE LA INSTALACIÓN

PKI SERVICES S.A.S. mantiene un almacén externo seguro para la custodia de documentos en papel, y de dispositivos y documentos electrónicos independiente del Centro de Datos.

Se requieren al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2. CONTROLES DE PROCEDIMIENTO

5.2.1 ROLES DE CONFIANZA

Se cuenta con roles de confianza distintos para la administración y operación de las plataformas de la CA Raíz y la CA Subordinada de PKI SERVICES S.A.S., destinadas a la generación y administración de las claves y a la administración de los perfiles de certificados y CRL de la CA Raíz y la CA Subordinada de PKI SERVICES S.A.S., y para la administración y operación de las plataformas de la RA de PKI SERVICES S.A.S. (plataformas WEB, de la RA y del HSM Centralizado), destinadas a la administración y operación de la Autoridad de Registro de PKI SERVICES S.A.S.

De esta forma, se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de Certificación y registro.

Los roles de confianza establecidos en los documentos del Sistema de Gestión integrado Diagrama Organizacional para la administración de estas plataformas.

5.2.2. NÚMERO DE PERSONAS REQUERIDAS POR TAREA

PKI SERVICES S.A.S. garantiza al menos dos de tres personas para realizar las tareas que requieren control multipersona, para el acceso al Sistema de la CA, y que se detallan a continuación:

- La generación de la clave de las CA.
- La recuperación y back-up de la clave privada de las CA.
- La emisión de certificados de las CA.
- La revocación de certificados de las CA.
- Activación de la clave privada de las CA.

5.2.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA CADA ROL

Cada rol de confianza de la CA Raíz, CA Subordinada y RA se autentica mediante la utilización de mecanismos de autenticación seguros. La autenticación dentro de las plataformas previamente mencionadas permite el acceso a determinados activos de información de PKI SERVICES S.A.S.

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

5.2.4. ROLES QUE REQUIEREN SEGREGACIÓN DE FUNCIONES

La segregación de funciones e incompatibilidades se determinan en el Diagrama Organizacional.

Los roles de la CA (Auditor de la CA, Administrador de la CA) son incompatibles con los de roles de la RA (Administrador de la RA, Agente de la RA, Auditor de la RA).

Los roles de la RA (Administrador de la RA, Agente de la RA, Auditor de la RA) son incompatibles entre ellos.

5.3. CONTROLES DE PERSONAL

5.3.1. REQUISITOS SOBRE LA CUALIFICACIÓN, EXPERIENCIA Y CONOCIMIENTO PROFESIONALES

Todo el personal que realiza tareas calificadas como confiables sin supervisión lleva al menos dos meses trabajando en el centro de operación técnica y tiene contrato laboral fijo.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

PKI SERVICES S.A.S. se asegura que el personal de la RA es personal confiable para realizar las tareas de registro. A tal efecto se exige una Autorización para su rol dentro de PKI SERVICES S.A.S.

PKI SERVICES S.A.S. retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

En el sistema de gestión integrado, existe un procedimiento para la selección de personal que define todos los requisitos para la selección de personal para los roles profesionales.

5.3.2. PROCEDIMIENTO DE COMPROBACIÓN DE ANTECEDENTES

Para el ingreso y con frecuencia anual, se realizan investigaciones pertinentes antes de la contratación de cualquier persona.

5.3.3. REQUISITOS DE FORMACIÓN

Se llevan a cabo los cursos necesarios al personal para asegurar la correcta realización de las tareas asignadas a sus respectivos roles, y en función de los conocimientos personales de cada persona.

Como política de contratación de personal, se busca y contrata personal que sean expertos y con experiencia en los Roles definidos.

5.3.4. REQUISITOS Y FRECUENCIA DE ACTUALIZACIÓN DE FORMACIÓN

Se realizarán actualizaciones de formación al personal cuando se realicen modificaciones en las tareas asignadas a un rol que así lo requieran, o cuando lo solicite alguna persona.

5.3.5. SANCIONES POR ACTUACIONES NO AUTORIZADAS

Se dispone del reglamento interno de trabajo el cual permite sancionar a los empleados de PKI SERVICES por la realización de acciones no autorizadas pudiéndose llegar al cese del trabajador.

5.3.6. REQUISITOS DE CONTRATACIÓN DE TERCEROS

Los empleados de las empresas proveedores de infraestructura tecnológica y de servicios locales de PKI SERVICES S.A.S. que tengan un rol asignado dentro de la actividad de PKI SERVICES S.A.S para realizar tareas confiables deberán firmar anteriormente el acuerdo bilateral de confidencialidad y los requerimientos operacionales empleados por PKI SERVICES S.A.S. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar al cese del contrato laboral.

5.3.7. DOCUMENTACIÓN PROPORCIONADA AL PERSONAL

PKI SERVICES S.A.S. pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas, las políticas y Prácticas que rigen dichos procesos y la documentación de seguridad.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

5.4. PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

5.4.1. TIPOS DE EVENTOS REGISTRADOS

PKI SERVICES S.A.S. registra y guarda los logs de todos los eventos relativos al sistema de seguridad de PKI SERVICES S.A.S. Estos incluyen los siguientes eventos:

- Encendido y apagado del sistema.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados a los sistemas de PKI SERVICES S.A.S. a través de la red.
- Registros de las aplicaciones de PKI SERVICES S.A.S.
- Encendido y apagado de las aplicaciones de PKI SERVICES S.A.S.
- Cambios en la configuración de PKI SERVICES S.A.S. y/o sus claves.
- Cambios en la creación de perfiles de certificados.
- Generación de claves propias.
- Eventos del ciclo de vida de los certificados.
- Eventos asociados al módulo criptográfico.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Adicionalmente, PKI SERVICES S.A.S. conserva, ya sea manual o electrónicamente, la siguiente información
- Las ceremonias de creación de claves de las CA.
- Cambios en el personal que realiza tareas de confianza.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de Suscriptor, si se gestiona esa información.
- Posesión de datos de activación, para operaciones con las claves privadas de PKI SERVICES S.A.S.


5.4.2. FRECUENCIA DE PROCESADO DE REGISTROS DE AUDITORÍA(LOG)

Se revisarán los logs de auditoría anualmente y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

5.4.3. PERIODO DE RETENCIÓN DE LOS REGISTROS DE AUDITORÍA

Se almacenará la información de los logs de auditoría por un periodo de tres (03) años para garantizar la seguridad del sistema en función de la importancia de cada log en concreto.

5.4.4. PROTECCIÓN DE LOS REGISTROS DE AUDITORÍA

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 33 de 61

Los logs de los sistemas son protegidos de su manipulación mediante mecanismos que aseguran su integridad.

Los dispositivos son manejados en todo momento por personal autorizado.

5.4.5. PROCEDIMIENTOS DE RESPALDO DE LOS REGISTROS DE AUDITORÍA

PKI SERVICES S.A.S. dispone de un procedimiento adecuado de backup, de manera que, en caso de Pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

Se realizan copias diarias incrementales y completas semanales.

5.4.6. SISTEMA DE RECOGIDA DE INFORMACIÓN DE AUDITORÍA (INTERNA O EXTERNA)

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo.

5.4.7. ANÁLISIS DE VULNERABILIDADES

PKI SERVICES S.A.S. realiza anualmente una revisión de vulnerabilidades y test de intrusión para analizar la infraestructura de PKI SERVICES S.A.S. Después se analizarán y se corregirán las vulnerabilidades que PKI SERVICES S.A.S. que crea son un riesgo para ella.

5.4.8. SUPERVISIÓN

PKI SERVICES S.A.S. dispone de un NOC (Network Operation Center) y un SOC (Security Operation Center) y para monitorizar todas las tareas de supervisión de la seguridad y las comunicaciones de los servicios ofrecidos.

5.5. ARCHIVO DE REGISTROS

5.5.1. TIPOS DE EVENTOS ARCHIVADOS

PKI SERVICES S.A.S. conservará los eventos que tengan lugar durante el ciclo de vida del certificado. Se almacenarán por la CA o, por delegación de ésta, en la RA:

- Todos los datos de la auditoría,
- Todos los datos relativos a los certificados, incluyendo los contratos con los Suscriptores y/o Solicitantes y los datos relativos a su identificación,
- solicitudes de emisión y revocación de certificados,
- todos los certificados emitidos o publicados,
- CRL's emitidas o registros del estado de los certificados generados,
- la documentación requerida por los auditores y
- las comunicaciones entre los elementos de la PKI

PKI SERVICES S.A.S. es responsable del correcto archivo de todo este material y documentación.

5.5.2. PERIODO DE CONSERVACIÓN DE REGISTROS

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservarán durante el periodo que establezca la legislación vigente cuando sea aplicable. Los certificados se conservarán durante al menos un año desde su expiración. Los contratos con los Suscriptores y/o Solicitantes y cualquier información relativa a la identificación y autenticación del Suscriptor y/o Solicitante serán conservados durante al menos tres (03) años desde su finalización o el periodo que establezca la legislación vigente.

5.5.3. PROTECCIÓN DEL ARCHIVO

PKI SERVICES S.A.S. asegura la correcta protección de los archivos, incluyendo, entre otros, la información que se recopila con el fin de expedir los certificados, mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones externas al Centro de Datos de PKI SERVICES S.A.S. en los casos en que así se requiera.

Además, se disponen de documentos técnicos y de configuración donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

5.5.4. PROCEDIMIENTOS DE COPIA DE SEGURIDAD DEL ARCHIVO

PKI SERVICES S.A.S. dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias de máquinas virtuales. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

5.5.5. REQUISITOS PARA EL SELLADO DE TIEMPO DE LOS REGISTROS

Los registros están fechados con la fuente fiable del Instituto Nacional de Metrología (INM) de Colombia, mediante sincronización a través del protocolo NTP v4, conforme al estándar RFC 3161 Time-Stamp Protocol.

Existe dentro de la documentación técnica y de configuración de PKI SERVICES S.A.S. un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

5.5.6. SISTEMA DE ARCHIVO DE LA INFORMACIÓN DE AUDITORÍA (INTERNO O EXTERNO)

El sistema de archivo de la información de auditoría de PKI SERVICES S.A.S. es interno, si bien se dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos

5.5.7. PROCEDIMIENTOS PARA OBTENER Y VERIFICAR INFORMACIÓN ARCHIVADA

Los eventos registrados están protegidos contra manipulaciones no autorizadas.

Sólo el personal autorizado para ello tiene acceso a los archivos físicos de soportes y archivos informáticos, para obtener y llevar a cabo verificaciones de integridad de dichos archivos.

5.6. CAMBIO DE CLAVES

El procedimiento para proporcionar, en caso de cambio de claves de la CA Raíz o de la CA Subordinada, la nueva clave pública de la CA a los Suscriptores, Solicitantes y Terceros aceptantes de los certificados emitidos con las nuevas claves es el mismo que para proporcionar la actual clave pública de la CA Raíz y de la CA Subordinada.

En consecuencia, el nuevo certificado de la CA conteniendo su nueva clave pública se publicará en la página web de PKI SERVICES S.A.S.

5.7. PROCEDIMIENTOS DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

PKI SERVICES S.A.S. tiene establecido y probado el plan de continuidad y contingencia encaminado a garantizar la continuidad del servicio de certificación, en caso de que ocurra algún evento que comprometa la prestación del servicio.

Cualquier fallo en la consecución de las metas marcadas por este plan de continuidad y contingencia será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de PKI SERVICES S.A.S. para implementar dichos procesos.

En el sistema de gestión integrado, se encuentra el procedimiento de seguridad para el manejo de incidentes, cumple con el anexo A de la norma ISO 27001.

Como parte de los incidentes de seguridad que son registrados por PKI SERVICES S.A.S., se encuentran:

- Cuando la seguridad de una llave privada de PKI SERVICES S.A.S. se ha visto comprometida.
- Cuando el sistema de seguridad de PKI SERVICES S.A.S. ha sido vulnerado.

- Cuando se presenten fallas en el sistema de PKI SERVICES S.A.S. que comprometan la prestación del servicio.
- Cuando los sistemas de cifrado pierdan vigencia por no ofrecer el nivel de seguridad contratado por el suscriptor.
- Cuando se presente cualquier otro evento o incidente de seguridad de la información.

5.7.1. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE

El plan de contingencia de la jerarquía de PKI SERVICES S.A.S. trata el compromiso de una clave privada de PKI SERVICES S.A.S. como un desastre.

En caso de compromiso de la clave privada de la CA Raíz o de la CA Subordinada, la seguridad del servicio de emisión de certificados se verá afectada gravemente, y se procederá según el procedimiento Gestión de claves a:

- Informar a todos los suscriptores, usuarios y otras ECD con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web de PKI SERVICES S.A.S.
- Indicar que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

5.7.2. CONTINUIDAD DEL NEGOCIO DESPUÉS DE UN DESASTRE

PKI SERVICES S.A.S. en su sistema de gestión integrado, ha desarrollado el plan de continuidad para recuperar todos los sistemas después de un desastre. El plan de continuidad tiene dos frentes, uno que es el plan de continuidad del data center para asegurar el cumplimiento del 99.9% uptime, y desde el frente de componentes PKI.

5.8. CESE DEL SERVICIO DE EMISIÓN DE CERTIFICADOS

Ante el cese del servicio de emisión de certificados de PKI SERVICES S.A.S. se procederá según el Procedimiento de Cesación de servicios de la siguiente forma:

- Informar en primera instancia a la Superintendencia de Industria y Comercio y a ONAC acerca del cese de actividades con una anticipación de treinta (30) días y solicitar su autorización.
- Luego de haber sido autorizado, informar por medio de dos avisos publicados en diarios de amplia difusión y por el correo electrónico declarado, a todos los Suscriptores con un intervalo de quince (15) días sobre la terminación de su actividad o actividades, la fecha precisa de cesación y las consecuencias jurídicas de ésta respecto de los certificados expedidos.

En cualquier caso, se garantiza la continuidad del servicio a los usuarios quienes ya hayan contratado los servicios de PKI SERVICES S.A.S. PKI SERVICES S.A.S., directamente o por medio de terceros, sin ningún costo adicional a los servicios que contrató.

6. CONTROLES TÉCNICOS DE SEGURIDAD

6.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

6.1.1. GENERACIÓN DEL PAR DE CLAVES

La generación de las claves de la CA y SUBCA se realiza, de acuerdo con el proceso documentado de ceremonia de claves, en dispositivos criptográficos hardware certificados (HSM) FIPS 140-2 nivel 3, por personal adecuado según los roles de confianza y, al menos con un control dual y testigos de PKI SERVICES S.A.S., de la organización titular de PKI SERVICES S.A.S. y de un auditor externo.

Para los certificados de entidad final, la generación de claves se realizará en dispositivos que aseguren razonablemente que la clave privada únicamente puede ser utilizada por el Suscriptor, bien por medios físicos, bien estableciendo el Suscriptor los controles y medidas de seguridad adecuadas.

En los casos en que PKI SERVICES S.A.S. pueda garantizar que las claves criptográficas del Suscriptor han sido creadas en un dispositivo criptográfico que cumpla con los requisitos mínimos (si el tipo de

soporte es Tarjeta/Token o HSM Centralizado), se indicará en el propio certificado mediante la inclusión del identificador OID correspondiente en la extensión Certificate Policies.

En cualquier otro caso (si el tipo de soporte es Otros Dispositivos), los certificados se emitirán con un identificador OID diferente en la extensión Certificate Policies.

6.1.2. ENTREGA DE LA CLAVE PRIVADA A LOS SUSCRIPTORES

La RA será responsable de garantizar la entrega del certificado al Suscriptor y/o Solicitante, ya sea entregándole el dispositivo de firma o habilitándole los mecanismos para su descarga y/o instalación y posterior uso, tal y como se especifica en la PC respectiva. De esta forma, se asegura que el Suscriptor y/o Solicitante utiliza, con un alto nivel de confianza, bajo su control exclusivo los datos de creación de firma correspondientes a los de verificación que constan en el certificado.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

El envío de la clave pública a PKI SERVICES S.A.S. para la generación del certificado se realiza mediante un formato estándar preferiblemente en formato PKCS #10 o equivalente auto firmado, utilizando un canal seguro para la transmisión.

6.1.4. ENTREGA DE LA CLAVE PÚBLICA DE PKI SERVICES S.A.S. A TERCEROS QUE CONFÍAN

Los Terceros que confían podrán consultar los certificados de la CA Raíz y la CA Subordinada, verificar la cadena de Certificación y su fingerprint (huella digital). Dichos certificados se encuentran a disposición de los usuarios en la página web de PKI SERVICES S.A.S.

6.1.5. TAMAÑO DE LAS CLAVES Y PERIODO DE VALIDEZ


Certificado	Tamaño claves RSA (bits)	Periodo validez
CA Raíz	4096	20 años Desde: 14/03/2018 13:50:35, tiempo UTC Hasta 14/03/2038 13:50:35, tiempo UTC
CA Subordinada	4096	Desde: 14/03/2018 13:59:37, tiempo UTC Hasta: 14/03/2038 00:00:00, tiempo UTC
OCSP CA Subordinada	2048	Desde: 05/04/2018 10:53:48, tiempo UTC Hasta: 14/03/2038 00:00:00, tiempo UTC
Suscriptores	2048	Como máximo, lo establecido en la legislación y normativas vigentes

6.1.6. PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA Y VERIFICACIÓN DE LA CALIDAD

Se utilizan los parámetros recomendados en el documento de especificaciones técnicas ETSI TS 119 312.

Concretamente los parámetros utilizados son los siguientes:

Signature suite	Hash function	Signature algorithm
-----------------	---------------	---------------------

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 37 de 61

sha256-with-rsa	SHA-256	RSA-PKCSv1_5
-----------------	---------	--------------

6.1.7 USOS PERMITIDOS DE LA CLAVE (SEGÚN EL CAMPO KEY USAGE DE LA X.509)

Todos los certificados incluyen las extensiones Key Usage y Extended Key Usage, indicando los usos habilitados de las claves.

Los usos admitidos para los certificados de la CA Raíz y la CA Subordinada son firma de certificados y firma de CRLs.

En cuanto a los usos admitidos de la clave para cada certificado de usuario final, se encuentran definidos en la Política de Certificación correspondiente.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA Y CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

6.2.1. CONTROLES Y ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Los módulos criptográficos empleados para generar y almacenar las claves de PKI SERVICES S.A.S. están certificados con la norma FIPS 140-2 nivel 3.

Las claves de los Suscriptores de certificados HSM Centralizado y de los certificados de operadores y administradores de la RA en Tarjeta/Token son generadas de forma segura utilizando un dispositivo criptográfico con FIPS 140-2 nivel 3, dando lugar a un nivel de aseguramiento alto para proteger las claves privadas frente a riesgos como:

- Ataques de código malicioso
- Exportación no autorizada de claves
- Suplantación de identidad por descuido del Suscriptor en la custodia de dispositivos criptográficos
- Daño físico del módulo criptográfico

6.2.2. CONTROL MULTIPERSONA (N DE M) DE LA CLAVE PRIVADA

El acceso a las claves privadas de la CA Raíz y la CA Subordinada se encuentra bajo control multipersona. Es decir, se requiere más de una persona para el acceso y activación de la mencionada clave privada, en el caso de PKI SERVICES se requieren como mínimo 2 de 3 llaves.

Dicho control garantiza que una persona no posea el control individual, descentralizando la responsabilidad de activar y usar las claves privadas de la CA Raíz y la CA Subordinada.

6.2.3. CUSTODIA DE LA CLAVE PRIVADA

La clave privada de la CA Raíz está custodiada por un dispositivo criptográfico hardware certificado con la norma FIPS 140-2 nivel 3, en estado off line totalmente desconectado de red y corriente, garantizando que la clave privada nunca está fuera del dispositivo criptográfico. La activación y posterior uso de la clave privada requiere el control multipersona detallado anteriormente. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

La clave privada de la CA Subordinada está custodiada en un dispositivo criptográfico seguro certificado con la norma FIPS 140-2 nivel 3, garantizando que la clave privada nunca está fuera del dispositivo criptográfico. La activación de la clave privada requiere el control multipersona detallado anteriormente.

PKI SERVICES S.A.S. no custodia copias de respaldo de las claves privadas de los Suscriptores de certificados (key escrow).

6.2.4. COPIA DE SEGURIDAD DE LA CLAVE PRIVADA

La copia de la clave privada de la CA raíz se realizó en otro HSM igual, éste se encuentra en sobre de

seguridad en cajilla de seguridad, a la cual solamente tiene acceso el gerente con control dual.

La clave de la SUBCA se encuentra en HA en el data center alterno.

Las claves de la CA Raíz y la CA Subordinada se pueden restaurar por un proceso multipersona que requiere la utilización 2 de 3 llaves.

6.2.5. ARCHIVO DE LA CLAVE PRIVADA

PKI SERVICES S.A.S. archivará las claves privadas de firma de certificados de la CA Raíz y la CA Subordinada después de la expiración del periodo de validez de esta, o de su revocación.

6.2.6. ALMACENAMIENTO DE LAS CLAVES PRIVADAS EN UN MÓDULOCRIPTOGRÁFICO

Existe un documento de ceremonia de claves de PKI SERVICES S.A.S., donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

6.2.7. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

Las claves de la CA Raíz y la CA Subordinada se activan por un proceso multipersona que requiere la utilización 2 de 3 llaves.

6.2.8. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Cada vez que se reinicie la aplicación las claves privadas de la CA Raíz y de la CA Subordinada se desactivarán por un proceso multipersona que requiere la utilización 2 de 3 llaves.

6.2.9 MÉTODO PARA DESTRUIR LA CLAVE PRIVADA

Se destruirán físicamente o reinicializarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de la clave privada de firma de certificados de la CA Raíz y de la CA Subordinada, o de los datos de activación de estas, incluyendo también los dispositivos que contengan copias de dichas claves o de sus datos de activación

6.3. OTROS ASPECTOS DE LA GESTIÓN DEL PAR DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

PKI SERVICES S.A.S. conservará todas las claves públicas durante el periodo exigido por la legislación vigente, cuando sea aplicable, o mientras el servicio de Certificación este activo y 6 meses más como mínimo, en otro caso.

6.3.2. PERIODOS OPERATIVOS DE LOS CERTIFICADOS Y PERIODO DE USO DEL PAR DE CLAVES

El periodo de uso de un certificado será determinado por la validez temporal del mismo.

Un certificado no debe ser usado después del periodo de validez del mismo, aunque la parte confiante pueda usarlo para verificar datos históricos teniendo en cuenta que no se garantiza un servicio de verificación en línea válido para ese certificado.


6.4. DATOS DE ACTIVACIÓN

6.4.1. GENERACIÓN E INSTALACIÓN DE LOS DATOS DE ACTIVACIÓN

Los datos de activación de las claves de la CA Raíz y la CA Subordinada fueron generados de forma segura durante la ceremonia de creación de claves de las CA.

En el caso de certificados de operadores y administradores de la RA en Tarjeta/Token, los datos de activación (PIN y PUK) son generados en el momento de inicialización del dispositivo criptográfico.

En el caso de certificados de Suscriptores generados en HSM Centralizado, los datos de activación serán generados al mismo tiempo que las claves en el HSM Centralizado, en el instante previo a la

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 39 de 61

emisión del certificado (contraseña), o cada vez que se accede a una clave en el HSM Centralizado (código recibido en el teléfono celular).

6.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

Sólo el personal autorizado tiene conocimiento de los datos de activación de las claves privadas de la CA Raíz y la CA Subordinada.

Para los certificados de entidad final, una vez se ha hecho entrega del dispositivo y/o de los datos de activación, es responsabilidad del Suscriptor de mantener la confidencialidad de estos datos.

6.4.3. OTROS ASPECTOS DE LOS DATOS DE ACTIVACIÓN

N/A.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

PKI SERVICES S.A.S. emplea sistemas fiables y productos comerciales para ofrecer sus servicios de Certificación, conforme a la norma internacional ISO/IEC 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de PKI SERVICES S.A.S., 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.
- Requerimientos de tráfico de red.
- La seguridad perimetral es definida por PKI SERVICES, pero es administrada por el data center.

La documentación técnica y de configuración de PKI SERVICES S.A.S. detalla la arquitectura de los equipos que ofrecen el servicio de Certificación tanto en su seguridad física como lógica.

6.5.1. REQUISITOS TÉCNICOS DE SEGURIDAD ESPECÍFICOS

Cada servidor de PKI SERVICES S.A.S. incluye las siguientes funcionalidades:

- Control de acceso a los servicios de PKI SERVICES S.A.S. y gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Auditoría de eventos relativos a la seguridad.
- Autodiagnóstico de seguridad relacionado con los servicios de PKI SERVICES S.A.S.
- Mecanismos de recuperación de claves y del sistema de PKI SERVICES S.A.S.

Las funcionalidades expuestas son provistas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2. CONTROLES DE SEGURIDAD DE LA RED

PKI SERVICES S.A.S. protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos firewall, una VLAN exclusiva para la PKI y VPN para acceso remoto controlado y que son administrados por el data center siguiendo las indicaciones de PKI SERVICES

6.5.3. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

6.5.3.1 CONTROLES DE DESARROLLO DE SISTEMAS

PKI SERVICES S.A.S. no hace desarrollo de software, sin embargo, posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

6.5.3.2 CONTROLES DE GESTIÓN DE SEGURIDAD

6.5.3.2.1 Gestión de seguridad

PKI SERVICES S.A.S. desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad.

6.5.3.2.2 Clasificación y gestión de información y bienes

PKI SERVICES S.A.S. mantiene un inventario de activos y documentación.

Cada una de las Políticas y procedimiento indica su nivel de confidencialidad. Los documentos están catalogados en tres niveles: PÚBLICO, INTERNO y CONFIDENCIAL.

6.5.3.3 Operaciones de gestión

PKI SERVICES S.A.S. dispone de procedimientos de gestión de incidencias y de la continuidad del negocio.

PKI SERVICES S.A.S. dispone de cajillas de seguridad ignífugas con control dual para el almacenamiento de soportes físicos.

PKI SERVICES S.A.S. tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el proceso de Certificación.

6.5.3.4 Tratamiento de los soportes y seguridad

Todos los soportes serán tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

6.5.3.5 Planning del sistema

El departamento de Sistemas de PKI SERVICES S.A.S. mantiene un registro de las capacidades de los equipos.


Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

6.5.3.6 Gestión del sistema de acceso

PKI SERVICES S.A.S. realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el acceso al sistema está limitado a las personas autorizadas. En particular:

6.5.3.7 Gestión general de PKI SERVICES S.A.S:

- Se dispone de controles basados en firewalls de alta disponibilidad y seguridad perimetral ambos administrados por el data center
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con autenticación fuerte.
- Se dispone de un procedimiento de cambio de titulares y cambio de custodios de las cajas fuertes.
- Se dispone de un procedimiento para asegurar que las operaciones se realizan respetando el Diagrama Organizacional.
- Cada persona tiene asociado su identificador para realizar las operaciones de Certificación según su

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 41 de 61

rol.

- El personal de PKI SERVICES S.A.S. será responsable de sus actos, por ejemplo, por retener logs de eventos.

• **Generación del certificado:**

- Las instalaciones de PKI SERVICES S.A.S. están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar ante un intento de acceso a sus recursos no autorizado y / o irregular.

- La autenticación para realizar el proceso de emisión de certificados se realiza mediante un sistema m de n operadores para la activación de la clave privada de la CA Raíz y de la CA Subordinada de PKI SERVICES S.A.S.

• **Gestión de la revocación:**

- Las instalaciones de PKI SERVICES S.A.S. están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar ante un intento de acceso a sus recursos no autorizado y / o irregular al sistema de revocaciones.

- La revocación se refiere a la pérdida de efectividad de un certificado digital de forma permanente. La revocación se realizará mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de log generaran las pruebas que garantizan el no repudio de la acción realizada por el operador de PKI SERVICES S.A.S.

• **Estado de la revocación**

- La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

• **Gestión del ciclo de vida del hardware criptográfico**

- PKI SERVICES S.A.S. se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.

- El Hardware criptográfico está construido sobre soportes preparados para evitar cualquier manipulación.

- PKI SERVICES S.A.S. registra toda la información pertinente del dispositivo para añadir al catálogo de activos de PKI SERVICES S.A.S.

- El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

- El dispositivo criptográfico solo es manipulado por personal confiable.

- La configuración del sistema de PKI SERVICES S.A.S. así como sus modificaciones y actualizaciones son documentadas y controladas.

- Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.5.4. EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA

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.

La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal es fácil debido al reducido número de personas que realizan sus trabajos en el Centro de Datos subcontratado.

6.6. SELLADO DE TIEMPO

El tiempo para los servicios de PKI SERVICES S.A.S. se obtienen mediante consulta de la hora legal colombiana al Instituto Nacional de Metrología (INM) de Colombia, de acuerdo con lo establecido en el artículo 14 del Decreto 4175 de 2011,

Los servidores se mantienen actualizados con la hora UTC, mediante sincronización a través del protocolo NTP v4, conforme al estándar RFC 3161 Time-Stamp Protocol.

7. PERFILES DE CERTIFICADO, CRL Y OCSP

7.1. PERFIL DE CERTIFICADO

7.1.1. FORMATO DEL CERTIFICADO

Los certificados emitidos por PKI SERVICES S.A.S. PKI SERVICES S.A.S. son certificados X.509 v3, conforme a los siguientes estándares:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

Adicionalmente, los certificados emitidos por PKI SERVICES S.A.S. son coherentes con lo dispuesto en los siguientes estándares:

En la tabla siguiente se especifica el perfil común de los certificados emitidos por la CA Raíz y la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

PERFIL COMÚN DE LOS CERTIFICADOS		
Campo del certificado	Descripción	Valor
versión	Nº de versión	v3
Serial Number	Nº de serie	Número entero positivo único con respecto a la CA que emite el certificado ¹
signature	Algoritmo de firma	OID ² y parámetros del algoritmo de firma
Issuer	Emisor (DN)	DN de la CA que emite el certificado ³
Validity notBefore	válido desde	Fecha y hora de inicio de validez del certificado, tiempo UTC ⁴
Validity notAfter	válido hasta	Fecha y hora de fin de validez del certificado, tiempo UTC ⁵
subject	Asunto (DN)	DN del titular del certificado ⁶
subjectPublicKeyInfo	Clave pública	OID ⁷ y parámetros del algoritmo y valor ⁸ de la clave pública
extensions	Extensiones del certificado	Extensiones del certificado ⁹

1. Valor aleatorio de 20 bytes

2. sha256WithRSAEncryption (ver OID en la sección 7.1.3)

3. certificados de CA Raíz, CA Subordinada y TSU TSA de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver DN de la CA Raíz en la sección 7.1.4; Certificados de OCSP CA Subordinada y de Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver DN de la CA Subordinada en la sección 7.1.4

4. fecha y hora de emisión del certificado.

5. certificados de CA Raíz, CA Subordinada y OCSP CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver periodo de validez en la sección 6.1.5; Certificado de TSU TSA de

PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver periodo de validez en la DPC para el estampado cronológico de PKI SERVICES S.A.S.; Certificados de Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver periodo de validez en la PC correspondiente al tipo de certificado.

6. Certificados de CA Raíz y CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver DN en la sección 7.1.4; Certificado de OCSP CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver DN en la sección 7.4.4; Certificado de TSU TSA de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver DN en la DPC para el estampado cronológico de PKI SERVICES S.A.S.; Certificados de Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver DN del titular en la PC correspondiente al tipo de certificado.

7. rsaEncryption (ver OID en la sección 7.1.3)

8. Certificados de CA Raíz, CA Subordinada, OCSP CA Subordinada y Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver tamaños claves RSA en la sección 6.1.5; Certificado de TSU TSA de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver tamaños claves RSA en la DPC para el estampado cronológico de PKI SERVICES S.A.S.

9. Certificados de CA Raíz y CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver extensiones en la sección 7.1.2; Certificado de OCSP CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver extensiones en la sección 7.4.2; Certificado de TSU TSA de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver extensiones en la DPC para el estampado cronológico de PKI SERVICES S.A.S.; Certificados de Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S: ver extensiones en la PC correspondiente al tipo de certificado.

7.1.2. EXTENSIONES DEL CERTIFICADO

En las tablas siguientes se especifican las extensiones de los certificados de la CA Raíz y de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

EXTENSIONES DEL CERTIFICADO DE CA RAÍZ – PKI SERVICES ROOT		
Extensión	Crítica	Valor
Subject Key Identifier	-	Identificador de la clave pública del certificado, obtenido a partir del hash SHA-1 de la misma
Key Usage	Sí	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Certificate Policies	-	OID 1.3.6.1.4.1.54689.1 URL de la DPC: en la página web de PKI SERVICES https://pkiservices.co/ sección INF. DIOSPONIBLE
Basic Constraints	Sí	CA: NONE

EXTENSIONES DEL CERTIFICADO DE CA SUBORDINADA – ECD PKI SERVICES COLOMBIA		
Extensión	Crítica	Valor
Authority Key Identifier	-	Identificador de la clave pública del certificado de la CA Raíz, obtenido a partir del hash SHA-1 de la misma
Subject Key Identifier	-	Identificador de la clave pública del certificado, obtenido a partir del hash SHA-1 de la misma
Key Usage	Sí	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

Certificate Policies	-	OID 1.3.6.1.4.1.54689.1 URL de la DPC: en la página web de PKI SERVICES https://pkiservices.co/ sección INF. DIOSPONIBLE
Basic Constraints	Sí	CA: TRUE pathLenConstraint: 0
CRL Distribution Points	-	URI de la CRL: en la página web de PKI SERVICES https://pkiservices.co/ sección INF. DIOSPONIBLE
Authority Information Access	-	URI del certificado de la CA Raíz: en la página web de PKI SERVICES https://pkiservices.co/ sección INF. DIOSPONIBLE

En la sección 7.4.2 se especifican las extensiones del certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

En la PC de cada tipo de certificado se especifican las extensiones de los correspondientes certificados de Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

En la DPC para el estampado cronológico de PKI SERVICES S.A.S se especifican las extensiones del certificado de TSU de la TSA de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

7.1.3. IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

Nombre	OID	Descripción
Sha512WithECDSAEncryption	1.3.6.1.4.1.54689.1	Algoritmo de firma de certificados y CRL en CA Raiz
Sha384WithECDSAEncryption	1.3.6.1.4.1.54689.1	Algoritmo de firma de certificados y CRL en CA subordinada
SHA256WithRSAEncryption	1.3.6.1.4.1.54689.1	Algoritmo de firma en perfil común de certificados.

7.1.4. FORMATOS DE NOMBRES

En las tablas siguientes se especifican los correspondientes atributos del DN de la CA Raíz y de la CA Subordinada PKI SERVICES S.A.S. PKI SERVICES S.A.S.

DN DE LA CA RAÍZ – PKI SERVICES ROOT		
Atributo del DN	Descripción	Valor
Country Name (C)	País	CO 1
State OD Province Name (ST)	Estado/Provincia	Bogota DC 2
Locality Name (L)	Localidad	Bogota DC 2
Street Address (STREET)	Dirección	see current address at https://pkiservices.co/

Organization Identifier (2.5.4.97)	Identificador de Organización	901301044 2
Organization Name (O)	Nombre de Organización	PKI SERVICES SAS 2
Common Name (CN)	Nombre	PKI SERVICES Root CA 2

- 1 Codificado en PrintableString
- 2 Codificado en UTF8String

DN DE LA CA SUBORDINADA – ECD PKI SERVICES COLOMBIA		
Atributo del DN	Descripción	Valor
Country Name (C)	País	CO
State OD Province Name (ST)	Estado/Provincia	Bogota DC
Locality Name (L)	Localidad	Bogota DC
Street Address (STREET)	Dirección	https://pkiservices.co/contacto
Organization Identifier (2.5.4.97)	Identificador de Organización	901301044
Organization Name (O)	Nombre de Organización	PKI SERVICES SAS
Common Name (CN)	Nombre	ECD PKI SERVICES

En la sección 7.4.4 se especifica el DN del certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

En la PC de cada tipo de certificado se especifican el DN del titular de los correspondientes certificados de Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

En la DPC para el estampado cronológico de PKI SERVICES S.A.S. se especifica el DN del certificado de TSU de la TSA de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

7.1.5. RESTRICCIONES DE LOS NOMBRES

Según lo especificado en las secciones 3.1 y 7.1.4 y en la PC de cada tipo de certificado.

7.1.6. IDENTIFICADORES DE OBJETO (OID) DE LA POLÍTICA DE CERTIFICADOS

El OID de la política del certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S se encuentra especificado en la sección 7.4.2 y también a continuación: 1.3.6.1.4.1.54689.1

Los OID de la Política de Certificados de cada tipo de certificados de Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S. se encuentran especificados en la sección 1.4 y en la PC correspondiente.

El OID de la política del certificado de TSU de la TSA de PKI SERVICES S.A.S. PKI SERVICES S.A.S. se encuentra especificado en la DPC para el estampado cronológico de PKI SERVICES S.A.S.

- 1 Codificado en PrintableString
- 2 Codificado en UTF8String

7.1.7. USO DE LA EXTENSIÓN POLICY CONSTRAINTS

Los certificados emitidos por la CA Raíz de PKI SERVICES S.A.S. PKI SERVICES S.A.S. definen dicha extensión con un valor de cero (0). Lo que indica que la entidad subordinada a la CA Raíz no puede generar nuevas subordinadas a partir de sí misma.

7.1.8. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

La extensión Certificate Policies de los certificados emitidos por la CA Raíz y la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S. contiene los siguientes Policy Qualifiers:

- id-qt-cps (URI de la DPC): contiene la URI donde se puede encontrar la última versión de la presente DPC, así como, en el caso de los certificados de Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S., la PC correspondiente al tipo de certificado.

7.1.9. TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATEPOLICY

La extensión Certificate Policies de los certificados emitidos por la CA Raíz y la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S. permite identificar la política que PKI SERVICES S.A.S. PKI SERVICES S.A.S. asocia al tipo de certificado y dónde se puede encontrar la presente DPC, así como, en el caso de los certificados de Suscriptores de PKI SERVICES S.A.S. PKI SERVICES S.A.S., la PC correspondiente al tipo de certificado.

7.2. PERFIL DE CRL

7.2.1. FORMATO Y PERIODO DE VALIDEZ DE LA CRL

Las CRL emitidas por PKI SERVICES S.A.S. PKI SERVICES S.A.S. son CRL X.509 v2, conforme a los siguientes estándares:

- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

En la tabla siguiente se especifica el perfil común de las CRL emitidas por la CA Raíz y la CA Subordinada de PKI SERVICES S.A.S.

PERFIL DE CRL		
Campo de la CRL	Descripción	Valor
versión	Nº de versión	v2
signatura	Algoritmo de firma	OID ¹ y parámetros del algoritmo de firma
Issuer	Emisor (DN)	DN de la CA que emite la CRL ²
ThisUpdate	Fecha y hora de emisión de esta CRL	Fecha y hora de emisión de la CRL, tiempo UTC
NextUpdate	Fecha y hora de emisión de la próxima CRL	Fecha de fin de validez de la CRL, tiempo UTC ³
Revoked Certificates user Certificate	Nº de serie del certificado revocado	Nº de serie del Certificado revocado
Revoked Certificates revocationDate	Fecha y hora de revocación del certificado	Fecha y hora de revocación del certificado, tiempo UTC

Revoked Certificates crlEntryExtensions	Extensiones de entrada de CRL	Extensiones de entrada de CRL
CrlExtensions	Extensiones de la CRL	Extensiones de la CRL

7.2.2. EXTENSIONES DE LA CRL Y DE ENTRADA DE CRL

EXTENSIONES DE LA CRL		
Extensión	Crítica	Valor
Authority Key Identifier	-	Identificador de la clave pública del certificado de la CA que emite la CRL, obtenido a partir del hash SHA-1 de la misma
CRL Number	-	Número incremental, con respecto a la CA que emite la CRL

EXTENSIONES DE ENTRADA DE CRL		
Extensión	Crítica	Valor
Reason Code	-	Código del motivo de revocación del certificado

- 1 sha256WithRSAEncryption (ver OID en la sección 7.1.3)
- 2 CRL de CA Raíz: ver DN de la CA Raíz en la sección 7.1.4; CRL de CA Subordinada: ver DN de la CA Subordinada en la sección 7.1.4
- 3 CRL de CA Raíz: 180 días; CRL de CA Subordinada: 4 días

7.3. PERFIL DE OCSP

El perfil OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S. es conforme al estándar RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", con las siguientes particularidades:

- Algoritmo de firma de respuestas OCSP: sha256WithRSAEncryption (ver OID en la sección 7.1.3)

7.4. PERFIL DE CERTIFICADO OCSP

7.4.1. FORMATO DEL CERTIFICADO

El formato del certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S. cumple lo especificado en la sección 7.1.1.

Adicionalmente, el certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S. es coherente con lo dispuesto en los siguientes estándares:

- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

El certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S. ha sido emitido por la propia CA Subordinada (PKI SERVICES Colombia).

El tamaño de claves y periodo de validez del certificado se indica en la sección 6.1.6

7.4.2. EXTENSIONES DEL CERTIFICADO

En la tabla siguiente se especifican las extensiones del certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

Extensión	Crítica	Valor
-----------	---------	-------

Authority Identifier	Key	-	Identificador de la clave pública del certificado de la CA Subordinada, obtenido a partir del hash SHA-1 de la misma
Subject Identifier	Key	-	Identificador de la clave pública del certificado, obtenido a partir del hash SHA-1 de la misma
Key Usage		Sí	digitalSignature nonRepudiation
Certificate Policies		-	OID 1.3.6.1.4.1.54689.1 URL de la DPC: https://pkiservices.co/cinfodisponible/
Basic Constraints		Sí	CA: END ENTITY
Extended Key Usage		Sí	OCSPSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points		-	URI de la CRL: http://pkiservices.co/info-disponible/pkiservicesubcac1.crl
Authority Information Access		-	URI del certificado de la CA Subordinada: http://pkiservices.co/infodisponible/pkiservicesrootca.crt

7.4.3. IDENTIFICADORES DE OBJETO (OID) DE LOS ALGORITMOS

Según lo especificado en la sección 7.1.3

7.4.4. FORMATOS DE NOMBRES


En la tabla siguiente se especifican los correspondientes atributos del DN del certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S.

Atributo del DN	Descripción	Valor
Country Name (C)	País	CO 1
State OD Province Name (ST)	Estado/Provincia	Bogotá DC 2
Locality Name (L)	Localidad	Bogotá DC 2
Street Address (STREET)	Dirección	https://pkiservices.co/contacto/
Organization Identifier (2.5.4.97)	Identificador de Organización	901301044-4 2
Organization Name (O)	Nombre de Organización	PKI SERVICES S.A.S. 2
Common Name (CN)	Nombre	PKI SERVICES – OCSP 2

7.4.5. RESTRICCIONES DE LOS NOMBRES

Según lo especificado en las secciones 3.1, 7.1.4 y 7.4.4.

7.4.6. IDENTIFICADORES DE OBJETO (OID) DE LAS POLÍTICAS DECERTIFICADOS

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 49 de 61

El OID de la política del certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S se encuentra especificado en la sección 7.4.2 y también a continuación: 1.3.6.1.4.1.51362.0.2.0.1

7.4.7. USO DE LA EXTENSIÓN POLICY CONSTRAINTS

El certificado OCSP de la CA Subordinada de PKI SERVICES S.A.S. PKI SERVICES S.A.S no contiene la extensión Policy Constraints.

1 Codificado en PrintableString

2 Codificado en UTF8String

7.4.8. SINTAXIS Y SEMÁNTICA DE LOS POLICY QUALIFIERS

Según lo especificado en la sección 7.1.8.

7.4.9. TRATAMIENTO SEMÁNTICO PARA LA EXTENSIÓN CERTIFICATEPOLICY

Según lo especificado en la sección 7.1.9.

8. AUDITORÍA DE CONFORMIDAD Y OTROS CONTROLES

PKI SERVICES S.A.S. se somete a las auditorías de acreditación que realiza ONAC de conformidad con lo dispuesto en el artículo 162 del Decreto-ley 19 de 2012. Asimismo, de acuerdo con lo exigido en los Criterios Específicos de Acreditación de ONAC, PKI SERVICES S.A.S. se somete a auditoría interna y auditoría de tercera parte en los términos previstos en dicho documento.

En caso de requerirse, PKI SERVICES S.A.S. permite y facilita la realización de auditorías por parte de la Superintendencia de Industria y Comercio de Colombia.

8.1. FRECUENCIA DE LAS AUDITORÍAS

Las auditorías se realizarán con carácter anual

8.2. IDENTIDAD/CUALIFICACIÓN DEL AUDITOR

Las auditorías de acreditación que competen a PKI SERVICES S.A.S. son realizadas por auditores designados por ONAC.

Las auditorías internas y de tercera parte se realizan por auditores que cumplan con lo establecido en los Criterios Específicos de ONAC vigentes y siguiendo el procedimiento interno Auditoría.

8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

Las empresas que realizan las auditorías externas nunca representan ningún conflicto de intereses que pueda desvirtuar su actuación en su relación con PKI SERVICES S.A.S.

8.4. ASPECTOS CUBIERTOS POR LOS CONTROLES

Las auditorías verifican de forma general que se cumple con los principios establecidos en los requisitos de acreditación (Criterios Específicos de ONAC vigentes), la legislación vigente aplicable y la documentación establecida en el sistema de gestión de PKI SERVICES S.A.S.. Dichos aspectos de deben identificar y controlar siguiendo el procedimiento interno Auditoría.

8.5. ACCIONES PARA TOMAR COMO RESULTADO DE LA DETECCIÓN DE DEFICIENCIAS

En caso de que sean detectadas incidencias o no-conformidades se tratarán las medidas oportunas para su resolución en el menor tiempo posible siguiendo el procedimiento interno de Auditoría.

8.6. COMUNICACIÓN DE RESULTADOS

El organismo auditor se comunicará con PKI SERVICES S.A.S. a través del interlocutor establecido en cada caso.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1. TARIFAS

9.1.1. TARIFAS DE EMISIÓN DE CERTIFICADOS

Las tarifas especificadas en las PC son referenciales, por lo que pueden variar de acuerdo al tipo de certificado y al contrato con cada cliente.

Las mismas tarifas se encuentran publicadas en la página web de PKI SERVICES S.A.S.

En la propuesta comercial se indicará el precio final con IVA para el certificado solicitado.

9.1.2. TARIFAS DE ACCESO A LOS CERTIFICADOS

El acceso a la consulta del estado de los certificados emitidos es libre y gratuito.

9.1.3. TARIFAS DE REVOCACIÓN O ACCESO A LA INFORMACIÓN DE ESTADO

No se establece ninguna tarifa para la revocación de certificados, ni para el acceso a la información de estado de los certificados.

9.1.4. TARIFAS DE OTROS SERVICIOS

Las tarifas aplicables a otros posibles servicios se negociarán entre PKI SERVICES S.A.S y los clientes de los servicios ofrecidos.

9.1.5. POLÍTICA DE REEMBOLSO

PKI SERVICES S.A.S. dispone de la devolución correspondiente al tiempo faltante del tiempo para la revocación sobre el costo del certificado sin incluir el costo del dispositivo. Esto si existe una de las causas de revocación.

9.2. RESPONSABILIDADES FINANCIERAS

9.2.1. COBERTURA DEL SEGURO

PKI SERVICES S.A.S. dispone de recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, garantizando sus responsabilidades en su actividad como ECD tal como se define en la legislación colombiana vigente (ART. 9 Decreto 333 de 2014)

La garantía citada se establece mediante un Seguro de Responsabilidad Civil con una cobertura igual o superior a la exigida por la legislación colombiana vigente.


Las características de dicho seguro son las siguientes:

- Es expedido por una entidad aseguradora vigilada por la Superintendencia Financiera de Colombia.
- Cubre riesgos y perjuicios contractuales y extracontractuales de suscriptores y terceros de buena fe.
- Cubrir los anteriores riesgos por una cuantía asegurada por evento igual o superior al mayor entre:
7.500 salarios mínimos mensuales legales por evento;
- La entidad aseguradora se encarga de informar previamente a ONAC la terminación del contrato de seguro o si se realizan modificaciones que reducen el alcance o monto de la cobertura pactada.

El seguro se hará cargo de todas las cantidades que PKI SERVICES S.A.S. resulte legalmente obligado a pagar, hasta el límite de cobertura contratado, como resultado de cualquier procedimiento judicial en el que pueda declararse su responsabilidad, derivada de cualquier acto negligente, error u incumplimiento no intencionado de la legislación vigente entre otros.

9.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

PKI SERVICES S.A.S. considera confidencial toda la información que no esté catalogada expresamente como pública. No se difundirá información declarada como confidencial sin el consentimiento expreso

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 51 de 61

por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

9.3.1. INFORMACIÓN CONFIDENCIAL

En particular, la siguiente información será considerada confidencial:

- Las claves privadas de la CA Raíz y la CA Subordinada de PKI SERVICES S.A.S.
- Acta de Ceremonia de generación de las claves de la CA Raíz y la CA Subordinada.
- Procedimiento de Ceremonia de generación de las claves de la CA Raíz y la CA Subordinada.
- La información de negocio suministrada y/o elaborada conjuntamente con PKI SERVICES S.A.S. por parte de sus clientes, proveedores u otras personas con las que PKI SERVICES se comprometió a guardar secreto establecido legal o convencionalmente.
- Los resultados de validaciones de identidad de Suscriptores y/o Solicitantes, provistas por fuentes públicas o privadas.
- La información del Suscriptor y/o Solicitante obtenida por fuentes diferentes del Suscriptor y/o Solicitante y que haya sido catalogada como "Confidencial".
- Los datos recogidos durante la certificación digital.

9.3.2. INFORMACIÓN NO CONFIDENCIAL

La siguiente información será considerada no confidencial:

- La contenida en la presente DPC.
- La contenida en las distintas Políticas de Certificados (PC).
- La información contenida en los certificados, puesto que para su emisión el Suscriptor y/o Solicitante otorga previamente su consentimiento, incluyendo los diferentes estados o situaciones del certificado.
- Las listas de revocación de certificados (CRL's), así como las restantes informaciones de estado de revocación.
- Cualquier información cuya publicidad sea impuesta normativamente.

9.4. POLÍTICA DE PROTECCIÓN DE DATOS

PKI SERVICES S.A.S. garantiza la protección de datos personales de los Suscriptores y/o Solicitantes de los servicios de certificación digital, en cumplimiento de la Ley Estatutaria 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 del 2013; de los Decretos 1377 de 2013 y 886 de 2014, ley 1266 de 2008 de demás decretos reglamentarios relacionados, donde se reglamenta lo establecido en la Ley 1581 de 2012, por la cual se expidió el Régimen General de Protección de Datos Personales, cuyo objeto es "(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma" y de los Criterios Específicos de Acreditación Entidades de Certificación Digital - CEA-4.1-10 vigente.

Serán considerados como datos personales, la información de nombres, dirección, correo electrónico, y toda información que pueda vincularse a la identidad de una persona natural o jurídica, contenidos en los contratos y solicitudes de los Suscriptores y/o Solicitantes. Esta información será considerada como confidencial y será de uso exclusivo para las operaciones de certificación digital estipuladas, a excepción que exista un previo consentimiento del usuario final de dichos datos o medie una orden judicial o administrativa que así lo determine.

PKI SERVICES S.A.S. cuenta con una Política de Privacidad de datos personales que detalla los principios, recolección y tratamiento de datos personales y que se encuentra publicada en la página web: <https://pkiservices.co/>

Es responsabilidad de los Suscriptores y/o Solicitantes garantizar que la información provista a PKI

SERVICES S.A.S. sea veraz y vigente. Asimismo, son responsables del perjuicio que pudieran causar por aportar datos falsos, incompletos o inexactos.

Los solicitantes y/o suscriptores deben dar cumplimiento a la LEY 599 DE 2000, por la cual se expide el Código Penal Artículo 289. "Falsedad en documento privado. El que falsifique documento privado que pueda servir de prueba, incurrirá, si lo usa, en prisión de uno (1) a seis (6) años."

9.5. DERECHOS DE PROPIEDAD INTELECTUAL

De conformidad con lo dispuesto por las leyes nacionales y los tratados internacionales, todos los derechos en materia de propiedad intelectual e industrial relacionados con los sistemas, documentos, procedimientos, listas de revocación y cualesquiera otros, relacionados con su actividad como ECD, incluida la presente DPC y las PC asociadas, corresponderán en exclusiva a PKI SERVICES S.A.S."

9.6. OBLIGACIONES

9.6.1. OBLIGACIONES DE PKI SERVICES S.A.S.

PKI SERVICES S.A.S. PKI SERVICES S.A.S. se obliga con lo dispuesto en este documento, principalmente a:

- Respetar lo dispuesto en la presente DPC y en las PC asociadas, así como en el Contrato de Suscripción.
- Publicar esta DPC, las PC asociadas y el Contrato de Suscripción en su página Web, en su versión vigente.
- Informar sobre las modificaciones de esta DPC y de las PC asociadas a los Suscriptores, incluyendo dichas modificaciones en la tabla inicial de historial de versiones.
- Disponer de un seguro de responsabilidad civil que cubra el valor mínimo exigido por la normativa vigente.
- Utilizar sistemas fiables para almacenar certificados que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el Suscriptor y/o Solicitante hayan indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

Por lo que a los certificados respecta:

- Emitir certificados conforme a esta DPC, a las PC correspondientes y a los estándares de aplicación.
- Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
- Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.
- Revocar los certificados según lo dispuesto en esta DPC y en las PC correspondientes y publicar las mencionadas revocaciones en la CRL (Lista de Certificados Revocados).

Sobre custodia de información:

- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente, cuando sea aplicable.
- No almacenar ni copiar los datos de creación de firma del Suscriptor, cuando así lo disponga la normativa vigente.
- Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia si así se contemplase.
- Proteger sus claves privadas de forma segura.
- Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante Pérdida, destrucción o falsificación.

f) Remitir a ONAC, con frecuencia anual, para la realización de la Etapa 1 de cada evaluación de la acreditación:

- Archivo con los certificados emitidos y su respectivo contenido.
- Archivo con totales de control (emitidos, vigentes, revocados y expirados).

Como Autoridad de Registro (RA) también se obliga en los términos definidos en la presente DPC para la emisión de certificados, principalmente a:

- Respetar lo dispuesto en esta DPC y en la PC correspondiente al tipo de certificado que emita.
- Respetar lo dispuesto en los contratos firmados con el Suscriptor. En el ciclo de vida de los certificados:
 - Comprobar la identidad de los Solicitantes de certificados según lo descrito en esta DPC o mediante otro procedimiento que haya sido aprobado por PKI SERVICES S.A.S..
 - Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
 - Informar al Suscriptor, antes de la emisión de un certificado, de las obligaciones que asume, la forma que debe custodiar los datos de creación de firma, el procedimiento que debe seguir para comunicar la Pérdida o utilización indebida de los datos o dispositivos de creación de firma, de su precio, de las condiciones precisas para la utilización del certificado, de sus limitaciones de uso y de la forma en que garantiza su posible responsabilidad patrimonial, y de la página web donde puede consultar cualquier información de PKI SERVICES S.A.S., de la DPC y de la PC correspondiente al certificado.
 - Tramitar y entregar los certificados conforme a lo estipulado en esta DPC y en la PC correspondiente.
 - Tramitar el Contrato de Suscripción según lo establecido por la Política de Certificación aplicable.
 - Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor y/o Solicitante.
 - Informar a la CA Subordinada de las causas de revocación.
 - Realizar las comunicaciones con los Suscriptores, por los medios que consideren adecuados, para la correcta gestión del ciclo de vida de los certificados. Concretamente, realizar las comunicaciones relativas a la proximidad de la caducidad de los certificados y a las revocaciones de los mismos.

9.6.2. OBLIGACIONES DE LOS PROVEEDORES

En caso de que PKI SERVICES utilice servicios de un proveedor de infraestructura de llave pública, éste se encuentra obligado a cumplir con los siguientes requisitos:

- Responsabilidad y financiación
- Confidencialidad
- Requisitos para los recursos
- Requisitos del proceso – Ciclo de vida del certificado digital
- Requisitos del sistema de gestión
- Requisitos de la CA
- Requisitos de la RA
- Requisitos técnicos

9.6.3. OBLIGACIONES DE LOS SOLICITANTES

El Solicitante de un certificado estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- Suministrar a la RA la información real, verdadera necesaria para realizar una correcta identificación.

Los solicitantes y/o suscriptores deben dar cumplimiento a la LEY 599 DE 2000, por la cual se expide el Código Penal Artículo 289. "Falsedad en documento privado. El que falsifique documento privado

que pueda servir de prueba, incurrirá, si lo usa, en prisión de uno (1) a seis (6) años.”

- b) Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.
- c) Respetar lo dispuesto en los documentos contractuales firmados con PKI SERVICES S.A.S.
- d) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- e) Informar a la mayor brevedad posible del conocimiento de alguna causa de revocación.
- f) Aceptar términos y condiciones de servicios.

9.6.4. OBLIGACIONES DE LOS SUSCRIPTORES

El Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- a) Custodiar de manera diligente sus claves privadas y/o los datos de activación de las mismas (tales como contraseñas o códigos secretos definidos o recibidos por algún medio).
- b) Usar el certificado según lo establecido en la presente DPC y en la PC correspondiente.
- c) Respetar lo dispuesto en los instrumentos jurídicos vinculantes con PKI SERVICES S.A.S.
- d) Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- e) Informar a la mayor brevedad posible de la existencia de alguna causa de revocación.
- f) No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por PKI SERVICES S.A.S. o la RA de la revocación de este, o una vez expirado el plazo de validez del certificado.

9.6.5. OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y además:

- a) Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
- b) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confían, y aceptar sujetarse a las mismas.
- c) Notificar a PKI SERVICES S.A.S. cualquier situación irregular con respecto al servicio prestado por PKI SERVICES S.A.S.

9.6.6. OBLIGACIONES DE LA ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL SUSCRIPTOR

En los tipos de certificado que sea aplicable, la Entidad a la cual se encuentra vinculado el Suscriptor estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- a) Suministrar al Solicitante y/o a la RA la información necesaria para realizar una correcta identificación.
- b) Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.
- c) Respetar lo dispuesto en los documentos contractuales firmados con PKI SERVICES S.A.S.
- d) Notificar cualquier cambio en su conocimiento en los datos aportados para la creación del certificado durante su periodo de validez.
- e) Informar a la mayor brevedad posible del conocimiento de alguna causa de revocación.

9.6.7. OBLIGACIONES (DEBERES Y DERECHOS) DEL SOLICITANTE Y/O SUSCRIPTOR

9.6.7.1. USO DE MARCA.

Es deber y derecho de los solicitantes y suscriptores como de todas las partes relacionadas, cumplir con las restricciones o limitaciones del uso del nombre de PKI SERVICES y de la marca de acreditación como la de certificación, y sobre la manera de hacer referencia a la certificación digital otorgada.

1. El uso de la marca ONAC, sólo podrá usarse por PKI SERVICES S.A.S. cumpliendo lo establecido en el RAC-3.0-03 Reglamento de uso de los símbolos de Acreditado y/o Asociado que se puede consultar en <https://onac.org.co/>, es deber de los solicitantes, suscriptores y proveedores no usar la marca ONAC.

2. El uso de la marca PKI SERVICES será autorizado al suscriptor y terceros, como se indica en la Política: GE-PO-017 POLÍTICA DE USO DE SÍMBOLOS que se encuentra disponible en la página web de PKI SERVICES <https://pkiservices.co/> sección INF. DISPONIBLE opción Políticas corporativas.

9.6.7.2. DEBERES DE LOS SOLICITANTES.

El Solicitante de un certificado (ya sea de forma directa o a través de un tercero autorizado) se compromete a cumplir con las disposiciones legales y a:

- 1 Entregar información veraz y real a la RA. (Artículo 289, Ley 599 DE 2000)
- 2 Suministrar toda la información requerida para el registro de la cuenta.
- 3 Suministrar información exacta y verídica y aportar la documentación indicada en cada proceso de Solicitud.
- 4 Aceptar y respetar las disposiciones establecidas en los documentos suscritos con la SubCA y la RA.
- 5 Aceptar la política de términos y condiciones.

9.6.7.3. DERECHOS DE LOS SOLICITANTES.

- 1 El solicitante tiene derecho a solicitar un certificado digital o servicio de certificación digital libre de toda discriminación.
- 2 El solicitante tiene derecho a estar informado sobre el trámite de su solicitud.
- 3 El solicitante tiene derecho a acceder a la página de PKI SERVICES y toda la información disponible.
- 4 Recibir respuesta clara y oportuna a las PQRS o soporte requerido por el Solicitante.

9.6.7.4. DEBERES DE LOS SUSCRIPTORES

Artículo 39, Ley 527 de 1999. Deberes de los suscriptores. Son deberes de los suscriptores:

1. Utilizar el certificado de acuerdo con la presente DPC y las Políticas de Certificación aplicables.
2. Respetar las disposiciones establecidas en los documentos suscritos con la SubCA y la RA.
3. Reportar cualquier causa de suspensión / revocación tan pronto como sea posible.
4. Reporte cualquier cambio en los datos proporcionados para crear el certificado durante su período de validez.
5. No utilizar la clave privada ni el certificado una vez la SubCA solicita o informa de la suspensión o revocación del mismo, o una vez ha expirado el plazo de validez del certificado.
6. Recibir la firma digital por parte de la entidad de certificación o generarla, utilizando un método autorizado por ésta.
7. Suministrar la información que requiera la entidad de certificación.
8. Mantener el control de la firma digital.
9. Solicitar oportunamente la revocación de los certificados.
10. Custodiar y proteger de manera responsable la información del Certificado y la llave privada
11. No utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para la ECD.
12. 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.

9.6.7.5. DERECHOS DE LOS SUSCRIPTORES

- 1 Artículo 40, ley 527 de 1999. Responsabilidad de los suscriptores. Los suscriptores serán responsables por la falsedad, error u omisión en la información suministrada a la entidad de certificación y por el incumplimiento de sus deberes como suscriptor.
- 2 Solicitar la revocación del Certificado Digital en atención a una de las causas de revocación autorizadas.

9.7. RESPONSABILIDADES

9.7.1. RESPONSABILIDADES DE PKI SERVICES S.A.S.

- a) Cumplir con las leyes, normas, estándares técnicos, requisitos para su operación.
- b) Garantizar que los certificados cumplen con todos los requisitos materiales establecidos en la DPC y que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por PKI SERVICES S.A.S. PKI SERVICES S.A.S.
- c) Dar cumplimiento al artículo 83 de la constitución política colombiana, sobre el principio de la buena fe: “Las actuaciones de los particulares y de las autoridades públicas deberán ceñirse a los postulados de buena fe, la cual se presumirá en todas las gestiones que aquéllos adelanten ante éstas.”
- d) Facilitar los documentos necesarios y en su última versión al Suscriptor y al Solicitante.
- e) Brindar al Suscriptor información acerca de cómo validar el certificado, incluyendo el requisito de comprobar el estado de este y las condiciones en las cuales se puede confiar razonablemente en el certificado, lo cual resulta aplicable cuando el Suscriptor actúa como Tercero que confía.
- f) Notificar al Suscriptor acerca de los cambios en las políticas y prácticas de PKI SERVICES S.A.S. PKI SERVICES S.A.S.
- g) Notificar al Suscriptor cualquier cambio en los términos y condiciones básicas (identificadores de políticas, limitaciones de uso, obligaciones de Suscriptor, forma de validación de un certificado, procedimiento de resolución de disputas, periodo dentro del cual los registros de auditoría serán conservados, sistema legal aplicable y conformidad según los requerimientos del ONAC).
- h) El uso de los símbolos que caractericen la acreditación de PKI SERVICES S.A.S. de PKI SERVICES S.A.S. estarán restringidos al alcance acreditado, y no podrán ser transferidos a terceros ni heredados fuera de los servicios de certificación digital, personas, procesos y terceros evaluados por el ONAC; tal como lo describe el documento Política de uso de símbolos de PKI SERVICES S.A.S.
- i) Ejercer control, sobre los servicios de certificación digital acreditados, respecto a la propiedad y el uso de símbolos, certificados, cualquier otro mecanismo para indicar que el servicio de certificación digital está acreditado.
- j) Las referencias al alcance de acreditación otorgado, o el uso engañoso del alcance de acreditación otorgado, los símbolos, los certificados, y cualquier otro mecanismo para indicar que un servicio de certificación digital, o que PKI SERVICES S.A.S. está acreditada, en la documentación o en otra publicidad estarán sujetas al cumplimiento de las Reglas de Acreditación de ONAC.
- k) Atender y dar respuesta a las peticiones, quejas, reclamos y apelaciones de los Suscriptores y partes relacionadas.
- l) En cuanto a sus actividades como RA, notificará al ONAC cuando se establezca una nueva Oficina de Registro, donde se seguirá los mismos procedimientos y cumplirá los mismos requisitos que la Oficina Principal de PKI SERVICES S.A.S.
- m) Actuar de forma imparcial de acuerdo con su Política de Imparcialidad y de No Discriminación.

9.7.2 EXCLUSIÓN DE RESPONSABILIDAD DE PKI SERVICES S.A.S

PKI SERVICES no asume ninguna responsabilidad en caso de pérdida o perjuicio:

1. De los servicios que presta, en caso de guerra, huelgas, paros, golpes de estado, desastres naturales o cualquier otro caso de fuerza mayor.
2. Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos o la Declaración de Prácticas de Certificación (DPC) de PKI SERVICES.
3. Ocasionados por omisión involuntaria de los profesionales o terceros que laboran o prestan un

servicio para PKI SERVICES S.A.S.

4. Ocasionado por el uso indebido o fraudulento de los certificados o CRL'S emitidos por PKI SERVICES S.A.
5. Por la introducción de virus informático o código malicioso en el SSPS por parte del Usuario o de un tercero.
6. Por fallos de conexión a internet, imputables al Usuario o al Proveedor de servicio de Internet del Usuario.
7. Ocasionados a terceros de buena fe si el destinatario de los documentos firmados electrónicamente digitalmente no comprueba ni tiene en cuenta las restricciones que figuren en el certificado en cuanto a sus posibles usos, o cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado publicada en la CRL, o cuando no verifique la firma digital.

9.7.3. RESPONSABILIDADES DEL SUSCRIPTOR

- a) Actuar conforme a lo estipulado en la presente DPC de PKI SERVICES S.A.S. PKI SERVICES S.A.S.
- b) Facilitar información completa, actual y veraz a PKI SERVICES S.A.S. PKI SERVICES S.A.S.
- c) Emplear adecuadamente el certificado respecto a su aplicación, limitaciones y prohibiciones de uso; conforme a lo establecido en la DPC de PKI SERVICES S.A.S.
- d) Cumplir con los requisitos estipulados por PKI SERVICES S.A.S. para el respectivo servicio de certificación digital.
- e) Cumplir con nuevos requisitos, cuando PKI SERVICES S.A.S implemente cambios en los servicios de certificación digital, previa comunicación de dichos cambios por parte de PKI SERVICES S.A.S. al Suscriptor.
- f) Que las declaraciones sobre la certificación son coherentes con el alcance del servicio de certificación digital.
- g) No utilizar su certificación digital de manera que contravenga la ley u ocasione mala reputación para PKI SERVICES S.A.S. PKI SERVICES S.A.S. y no hace ninguna declaración relacionada con su certificación que PKI SERVICES S.A.S. pueda considerar engañosa o no autorizada. Lo que a su vez implica no monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica del ONAC y PKI SERVICES S.A.S. PKI SERVICES S.A.S.; así como comprometer intencionadamente la seguridad de la Jerarquía del ONAC y PKI SERVICES S.A.S. PKI SERVICES S.A.S.
- h) Inmediatamente después de la cancelación o la terminación de la certificación digital, dejar de utilizarla en todo el material publicitario que contenga alguna referencia a ella, y emprender las acciones exigidas por el servicio de certificación digital y cualquier otra medida previamente notificada.
- i) Al hacer referencia al servicio de certificación digital en medios de comunicación, tales como documentos, folletos o publicidad, informar de que cumple con los requisitos especificados en la respectiva PC de PKI SERVICES S.A.S.
- j) Cumplir con los requisitos que pueda prescribir el servicio de certificación digital con relación al uso de las marcas de conformidad y a la información relacionada con el servicio.
- k) Informar a PKI SERVICES S.A.S., sin retraso, acerca de los cambios que puedan afectar a la certificación digital que fue expedida por PKI SERVICES S.A.S.
- l) Ser diligente en la custodia de su clave privada y las contraseñas de acceso que protegen su clave privada, con el fin de evitar usos no autorizados.
- m) En todo momento ser responsable de proteger su clave privada, las contraseñas de acceso y el dispositivo criptográfico donde se encuentra almacenada su clave privada sin poder transferir esta responsabilidad a ningún tercero.
- n) Solicitar la revocación del certificado digital en caso de: pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada; compromiso potencial de la clave privada; pérdida de control sobre su clave privada, debido al compromiso de los datos de activación o por cualquier otra causa; inexactitudes o cambios en el contenido del certificado que conozca o pudiera

conocer.

- o) Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado
- p) No utilizar válidamente el certificado expirado a partir de la fecha en la que expira.
- q) Solicitar la revocación de certificados cuando incumple las obligaciones a las que se encuentra comprometido dentro de los requerimientos de ONAC.
- r) Informar que cumple con lo estipulado en la DPC de PKI SERVICES S.A.S., cuando haga referencia al servicio de certificación digital en medios de comunicación (artículos, documentos, folletos o publicidad).
- s) El Suscriptor debe proteger los dispositivos y claves utilizados para la firma digital y asume las obligaciones y responsabilidades sobre el uso de los certificados que adquiera.

9.8. LIMITACIÓN DE RESPONSABILIDAD


PKI SERVICES S.A.S., no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

- a) Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Suscriptor o por los Terceros, o cualquier otro caso de fuerza mayor.
- b) Por el uso indebido o fraudulento del directorio de certificados y CRL's (Lista de Certificados Revocados) emitidos por la CA.
- c) Por el uso indebido de la información contenida en el Certificado o en la CRL.
- d) Por el contenido de los mensajes o documentos firmados o encriptados mediante los certificados.
- e) En relación con acciones u omisiones del Solicitante y Suscriptor:
 - Falta de veracidad de la información suministrada para emitir el certificado.
 - Retraso en la comunicación de las causas de revocación del certificado.
 - Ausencia de solicitud de revocación del certificado cuando proceda.
 - Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
 - Uso del certificado fuera de su periodo de vigencia, o cuando PKI SERVICES S.A.S. o la RA le notifique la revocación de este.
 - Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y en la DPC de PKI SERVICES S.A.S., en particular, superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al Suscriptor por PKI SERVICES S.A.S.
- f) En relación con acciones u omisiones del Tercero que confía en el certificado:
 - Falta de comprobación de las restricciones que figuren en el certificado electrónico o en la DPC de PKI SERVICES S.A.S. en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.
 - Falta de comprobación de la Pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.

9.9. INDEMNIZACIONES

9.9.1. INDEMNIZACIONES POR DAÑOS OCASIONADOS POR PKI SERVICES S.A.S.

PKI SERVICES, S.A.S asumirá las indemnizaciones correspondientes por daños efectuados a Solicitantes, Suscriptores, Terceros que confían o a cualquier otra parte interesada en base a los términos establecidos en la normativa reguladora de la prestación de los servicios de emisión, revocación

	DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (DPC)	<i>CÓDIGO</i>	GE-DPC-001
		<i>VERSIÓN</i>	5
		<i>FECHA</i>	16-09-2024
		<i>PÁGINA</i>	Página 59 de 61

y distribución de los certificados digitales, así como a la presente DPC y las PC asociadas.

9.9.2. INDEMNIZACIONES POR LOS DAÑOS CAUSADOS POR LOS SOLICITANTES, POR LOS SUSCRIPTORES Y POR LOS TERCEROS QUE CONFÍAN

Tanto los Suscriptores, como los Solicitantes, como los Terceros que confían son responsables por apoderarse, destruir, modificar, adulterar indebidamente los datos de una firma o certificado digital durante o después de la fecha de creación del certificado y estarán sujetos al pago de indemnizaciones por los correspondientes daños causados según lo establecido en la normativa reguladora de la prestación de los servicios de emisión, revocación y distribución de los certificados digitales.

9.10 PERIODO DE VALIDEZ

9.10.1. PLAZO

Esta DPC y las PC asociadas entrarán en vigor desde el momento de su publicación en la página web de PKI SERVICES S.A.S y permanecerán en vigor mientras no se deroguen expresamente por la publicación de una nueva versión.

9.10.2. SUSTITUCIÓN Y DEROGACIÓN DE LA DPC Y LAS PC

Esta DPC y las PC asociadas serán sustituidas por nuevas versiones con independencia de la trascendencia de los cambios efectuados en la misma, de forma que siempre será de aplicación en su totalidad. Cuando la DPC quede derogada se retirará de la página web de PKI SERVICES S.A.S, si bien se conservará durante al menos tres (03) años desde su finalización o el periodo que establezca la legislación vigente.

9.10.3. EFECTOS DE LA FINALIZACIÓN

Las obligaciones y restricciones que establece esta DPC y las PC asociadas, en referencia a auditorías, información confidencial, obligaciones y responsabilidades de PKI SERVICES S.A.S nacidas bajo su vigencia, subsistirán tras su sustitución o derogación por una nueva versión en todo en lo que no se oponga a ésta.

9.11. PQRS

Las peticiones, quejas, reclamos, sugerencias y apelaciones (PQRS) sobre los servicios prestados por PKI SERVICES S.A.S., son recibidas directamente por el responsable de PQRS de PKI SERVICES S.A.S.

Los Solicitantes, Suscriptores, Terceros que confían o el público en general indicarán su PQRS con respecto a los servicios de certificación digital ofrecidos por PKI SERVICES S.A.S. enviando un correo electrónico a la dirección <https://pkiservices.co/> sección SERVICIO AL CLIENTE, opción SOPORTE PQRS, en el que se detalla la situación por la que se presenta.

Los PQRS serán gestionados por el responsable de PQRS de PKI SERVICES S.A.S., quien se encargará de derivar la incidencia al Departamento o rol respectivo. Dicha gestión se llevará a cabo, dando lugar a una solución en un lapso no mayor a quince (15) días. El usuario recibirá un mensaje de correo electrónico confirmando la recepción de la PQRS y cuando esta sea resuelta. PKI SERVICES S.A.S. cuenta con el procedimiento de PQRS para el tratamiento de PQRS que detalla cada uno de los procesos y se encuentra publicado en la página web de PKI SERVICES S.A.S.

9.12. CAMBIOS EN DPC Y PC

Todos los cambios en esta DPC y en las PC asociadas requerirán nuevas versiones de los documentos.

Los cambios en cada nueva versión estarán indicados en la tabla inicial de historial de versiones.

Las nuevas versiones aprobadas de esta DPC y de las PC asociadas son enviadas a ONAC y publicadas en la página web de PKI SERVICES S.A.S.

9.13. RECLAMACIONES Y RESOLUCIÓN DE DISPUTAS

Para la resolución de cualquier conflicto que pudiera surgir con relación a esta DPC o a las PC asociadas,

las partes, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los Tribunales colombianos, con independencia del lugar dónde se hubieran utilizado los certificados emitidos.

9.14. LEY APLICABLE

La legislación aplicable al presente documento, así como a las PC asociadas y a las operaciones que derivan de ellas se registra en el documento de carácter interno, entre ella se encuentra la siguiente, así como los reglamentos que la modifiquen o complementen:

- a) Ley 527 de 1999
- b) Ley Estatutaria 1581 de 2012
- c) Decreto Ley 0019 de 2012
- d) Decreto 1074 de 2015
- e) Decreto 333 de 2014
- f) Decreto 2364 de 2012
- g) Decreto 1471 de 2014

9.15. CONFORMIDAD CON LA LEY APLICABLE

Es responsabilidad de PKI SERVICES S.A.S. asegurar el cumplimiento de la legislación aplicable recogida en el apartado anterior.

9.16. ESTIPULACIONES DIVERSAS

9.16.1. CONTRATO DE SUSCRIPCIÓN

El Contrato de Suscripción (GC-CN-001 Contrato de Suscripción) para el servicio de emisión de certificados vigente se encuentra publicado en la siguiente página web: <https://pkiservices.co/> sección INF. DISPONIBLE

Se usa el mismo modelo de contrato para todos los tipos de certificados. En el contrato se deberán rellenar el tipo de certificado contratado y su vigencia.

9.16.2. CLÁUSULA DE ACEPTACIÓN COMPLETA

Todos los Solicitantes, Suscriptores, Terceros que confían y cualquier otra parte interesada asumen en su totalidad el contenido de la última versión de esta DPC y de las PC asociadas.

9.16.3. INDEPENDENCIA

En el caso de que cualquiera de los apartados recogidos en la presente DPC o en las PC asociadas sea declarado, parcial o totalmente, nulo o ilegal no afectará tal circunstancia al resto del documento.

9.17. OTRAS ESTIPULACIONES

No se contemplan.

10. POLÍTICAS DE LOS CERTIFICADOS DIGITALES QUE EXPIDE PKI SERVICES

El procedimiento de expedición de los certificados se encuentra detallado en el Numeral 4 Ciclo de vida de los certificados de este documento.

El medio disponible para generar los certificados digitales y servicios de certificación digital se encuentra en nuestra página web PKI SERVICES <https://pkiservices.co/> sección SERVICIOS

Es requisito haber sido validada la identidad del solicitante de acuerdo con lo establecido en el numeral 3.2 – Validación de identidad.

La Política de certificados se encuentran en GE-PO-018 POLITICA DE CERTIFICADOS, documento que forma parte integral de esta DPC, publicado en nuestra página web PKI SERVICES <https://pkiservices.co/> sección INFORMACIÓN DISPONIBLE.

10.6. TARIFAS:



**DECLARACIÓN DE PRÁCTICAS DE
CERTIFICACIÓN
(DPC)**

<i>CÓDIGO</i>	GE-DPC-001
<i>VERSIÓN</i>	5
<i>FECHA</i>	16-09-2024
<i>PÁGINA</i>	Página 61 de 61

El valor que fija PKI SERVICES para la prestación de los Servicios de Certificados de firma digital se establece de acuerdo con las condiciones contractuales acordadas con los solicitantes del servicio y serán adecuadamente calculados y liquidados por PKI SERVICES.

La tarifa para la Prestación del servicio de Certificados de firma digital será establecida con base en las necesidades del cliente y de acuerdo con la volumetría de certificados de firma digital que el cliente requiera. Las tarifas se encuentran en GE-PO-018 POLITICA DE CERTIFICADOS