CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN	ELABORÓ	REVISÓ	APROBÓ
1	05/02/2020	DOCUMENTO NUEVO	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS
2	15/11/2021	1. Se definieron y se documentaron los derechos y deberes de Solicitante y/o Suscriptor en el documento GE-PO-018 POLÍTICA DE CERTIFICADOS. 2. Se Definieron y documentar en los derechos de los suscriptores, las condiciones para el uso del nombre de PKI SERVICES y de su marca, en el documento GE-PO-018 POLÍTICA DE CERTIFICADOS. 3. Se incluyó información relativa a Firma Electrónicas.	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS
3	21-11-2022	Se incluyo el servicio de emisión de certificado digital para persona Jurídica	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS
4	29-11-2022	Se revisa y se ajusta la descripción de los servicios de certificación digital acreditados en el Alcance, por las indicaciones dadas por el evaluador según directriz de la coordinación sectorial ECD	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS
5	01-03-2023	Se adiciono los servicios de: 1. Emisión de certificados en dispositivo local 2. Notificación Electrónica en	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS

		3. Correo Electrónico o Mensaje SMS Registro, Custodia y Anotación de documentos electrónicos transferibles e-Titulo Valor			
6	07-07-2023	4. Se realizan los ajustes que solicita el comité de acreditación.	COORDINADOR SGI	COMITÉ DE POLÍTICAS	COMITÉ DE POLÍTICAS

Contenido

1. OBJETIVO

Este documento constituye la Política de Certificados (PC) para la emisión de certificados digitales y servicios de certificación digital que PKI SERVICES ofrece, en el marco del cumplimiento de los Criterios Específicos de Acreditación Entidades de Certificación Digital vigente establecidos por el Organismo Nacional de Acreditación de Colombia – ONAC, conforme a la legislación colombiana y las disposiciones de los entes reguladores.

2. ÁMBITO DE APLICACIÓN

La presente Política será de cumplimiento obligatorio para todo el personal de PKI SERVICES S.A.S. interno, externos y proveedores, en todos los procesos que requieran hacer unapresentación a nivel interno o externo (para clientes) y uso de Certificados digitales.

3. DOCUMENTACIÓN RELACIONADA

Este documento es parte integral de la Declaración de Prácticas de Certificación (GE-DPC- 001 Declaración de prácticas de certificación DPC) y viceversa.

4. GENERALIDADES

Buscando satisfacer las diferentes necesidades que surgen en el contexto del uso creciente de las tecnologías de la información y Comunicaciones, PKI SERVICES expide diversos servicios de certificación y tipos de certificados digitales, los cuales se emiten con una vigencia de 1 o 2 años, con vigencia máxima de 2 años, de acuerdo con lo establecido en el CEA-3.0-07 v2

El procedimiento de expedición de los certificados se encuentra detallado en el documento GO-PR-005 CICLO DE VIDA DE LA EMISIÓN DE CERTIFICADOS DIGITALES que se encuentra publicado en página web de PKI SERVICES https://pkiservices.co/

El medio disponible para generar los certificados digitales para los suscriptores en las políticasque se detallan a continuación se encuentra expuesto en internet en la sección de SERVICIOS de la página web de PKI SERVICES https://pkiservices.co/

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

Para la emisión de este tipo de certificado a un menor de edad, deberá adjuntar el permiso expedido por el ministerio de trabajo en virtud de los artículos 35 y 113 de la ley 1098 de 2006.

El Gerente General administra y revisará anualmente La Política de Certificados, el Comité de políticas aprueba la Política de Certificados, con el fin de que la misma cumpla con los Criterios Específicos de Acreditación. Esta revisión debe hacerse con suficiente anticipacióna la renovación anual de la póliza.

5. DECLARCIONES DE PKI SERVICES S.A.S.

a. PKI SERVICES declara que los servicios de certificación digital que ofrece, los prestadetame con su propia infraestructura de llave pública PKI y NO son contratados externamente con terceros o entidades reciprocas.

b. PKI SERVICES declara que NO actualiza datos del certificado, NO suspende temporalmente certificados. Si el suscriptor solicita estas acciones, debe solicitar la expedición de otro nuevocertificado con los costos establecidos y el mismo suscriptor decide si revoca o no su certificado actual.

c. PKI SERVICES declara que ha planeado, gestionado e implementado un entorno Ciberseguro, mediante la implementación de las mejores prácticas, tecnologías y contrataciónde terceros con entornos de ciberseguridad seguros.

d. PKI SERVICES declara que emplea sistemas seguros que protegen la información que se recopila con el fin de expedir los certificados.

e. PKI SERVICES hace extensivo el cumplimiento de los requisitos de acreditación CEA-3.0-07,con el siguiente alcance:
Data Center: Mantener la Certificación ISO/IEC 27001 y TIER III

6. PINCIPIOS DE CUMPLIMIENTO LEGAL.

6.1. 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.”*

6.2. FALSEDAD EN DOCUMENTO PRIVADO.

Los solicitantes 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 la documentación aportada no es suficiente

7. DEBERES Y DERECHOS DE LOS SOLICITANTES

Los deberes y derechos de los solicitantes se encuentran listados en GE-DPC-001 Declaración de prácticas de certificación DPC que se encuentra publicado en la página web de PKI SERVICES **https://pkiservices.co/**

8. DEBERES Y DERECHOS DE LOS SUSCRIPTORES

Los deberes y derechos de los suscriptores se encuentran listados en GE-DPC-001 Declaración de prácticas de certificación DPC que se encuentra publicado en la página web de PKI SERVICES **https://pkiservices.co/**

9. USO DE MARCA

Las siguientes son las restricciones o limitaciones del uso del nombre de PKI SERVICES y de la marca de acreditación y certificación, y sobre la manera de hacer referencia a la certificación digital otorgada.

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 información Disponible- Políticas corporativas.

10. TIPOS DE CERTIFICADOS DIGITALES

Los siguientes tipos de certificados digitales que son ofrecidos por PKI SERVICES:

10.1 CERTIFICADO DE REPRESENTACIÓN DE EMPRESA/ENTIDAD EN DISPOSITIVOS LOCALES O CENTRALIZADOS

Se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante PKI SERVICES con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Colombia, o

con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero, vinculándose con la calidad de representante legal de una persona jurídica o Entidad del Estado.

Los Certificados de Representación de Empresa/Entidad certifican la identidad de una persona natural vinculándola con la representación legal de una persona jurídica, una Entidad del Estado,o como comerciante persona natural en el ámbito de su actividad profesional o mercantil.

Los Certificados de Representación de Empresa/Entidad tienen como suscriptor tanto a lapersona natural que actúa en nombre y representación legal de una persona jurídica, como a la persona jurídica representada que figura igualmente en el certificado digital.

Requisitos:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente
- Certificado de Cámara de comercio no mayor a 30 días
- Registro único tributario – RUT del año vigente
- Certificado de representación firmado por representante legal. no mayor a 30 días

Perfil del certificado:
"UsuarioFinal":
"correo", "Clave":
"XXXXX",
"Nombre": "NOMBRE SUSCRIPTOR",
"Apellido": "APELLIDO SUSCRIPTOR",
"NombreComun": "NOMBRE COMPLETO SUSCRIPTOR",
"Organizacion" : "EMPRESA SUSCRIPTOR", "Localidad":
"CIUDAD",
"Titulo": "RE",
"Pais" : "PAIS",
"Estado": "ESTADO / DEPARTAMENTO", "Calle":
"DIRECCION ENTIDAD",
"Correo": "CORREO",
"OrganizacionId": "NIT",
"SERIALNUMBER": "NUMERO CEDULA",
"TipoCertificado": "Representacion Empresa", "DuracionCertificado":
"X", "LongitudRsaKey": "2048"
“Valido_desde”
“Valido_hasta”

Certificado digital en Dispositivo Local
Corresponde a un estándar de generación de llaves públicas y privadas desde la infraestructura tecnológica del firmante y por responsabilidad del mismo, con el

propósito de obtener certificados digitales acreditados por una entidad de certificación digital.

Características:

- Llave pública de 2048 bits RSA o 256 bits ECDSA
- Algoritmo de firma de certificado con hash SHA 256
- Llave pública firmada en formato *.CER conforme a la cadena de confianza de PKI SERVICES.
- Emisión haciendo uso del estándar PKCS#10 autorizados por ONAC.
- Generar un Certificate Signing Request – CSR – en formato PKCS#10.
- Capacidad de recibir y usar la llave pública en formato .CER.

Cuidados del dispositivo:

- Todos los cuidados físicos y/o digitales relacionados con las claves públicas y privadas del certificado digital emitido bajo este formato son de responsabilidad exclusiva del suscriptor.

Riesgos asociados:

- Para el certificado en PKCS#10 los riesgos a los cuales se encuentra expuesto el HSM de producción que se encuentra en data center con certificado TIER III e ISO 27001.
- En temas lógicos, los riesgos asociados se encuentran definidos por ataques cibernéticos que impidan el acceso y/o disponibilidad respectiva para la firma del certificado.
- Por parte del suscriptor, tendrá los riesgos asociados al dispositivo el cual posea las claves públicas y privadas asociadas al certificado digital emitido bajo este protocolo

10.2 CERTIFICADO DE PERTENENCIA A EMPRESA/ENTIDAD EN DISPOSITIVOS LOCALES O CENTRALIZADOS

Se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante PKI SERVICES con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero, y permite identificarla como persona natural vinculándola como perteneciente a una determinada organización empresarial o entidad del Estado, pero sin que tenga la representación legal de la misma o facultad de comprometerla jurídicamente.

Los suscriptores de este tipo de certificados digitales son: 1) La persona natural que logre acreditar suficientemente, a juicio de PKI SERVICES, que existe una relación jurídica, laboral o de cualquier otra índole, con la persona jurídica o entidad del Estado que vaya a aparecer en el certificado digital. 2) La persona jurídica que figura en el certificado digital.

Requisitos:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente
- Certificado de Cámara de comercio no mayor a 30 días
- Registro único tributario – RUT del año vigente
- Certificado Laboral no mayor a 30 días

Perfil del certificado:

"UsuarioFinal
": "correo",
"Clave":
"XXXXX",
"Nombre": "NOMBRE
SUSCRIPTOR",
"Apellido": "APELLIDO
SUSCRIPTOR",
"NombreComun": "NOMBRE COMPLETO SUSCRIPTOR",
"Organizacion" : "EMPRESA
SUSCRIPTOR", "Localidad":
"CIUDAD",
"Titulo": "PE",
"Pais" : "CO",
"Estado": "ESTADO /
DEPARTAMENTO", "Calle":
"DIRECCION ENTIDAD",
"Correo": "CORREO",
"OrganizacionId": "NIT",
"SERIALNUMBER":
"NUMERO CEDULA",
"TipoCertificado": "Pertenencia Empresa",

"DuracionCertif
icado": "X",
"LongitudRsaK
ey": "2048"
“Valido_desde”
“Valido_hasta”

Certificado digital en Dispositivo Local

Corresponde a un estándar de generación de llaves públicas y privadas desde la infraestructura tecnológica del firmante y por responsabilidad del mismo, con el propósito de obtener certificados digitales acreditados por una entidad de certificación digital.

Características:

- Llave pública de 2048 bits RSA o 256 bits ECDSA
- Algoritmo de firma de certificado con hash SHA 256
- Llave pública firmada en formato *.CER conforme a la cadena de confianza de PKI SERVICES.
- Emisión haciendo uso del estándar PKCS#10 autorizados por ONAC.
- Generar un Certificate Signing Request – CSR – en formato PKCS#10.
- Capacidad de recibir y usar la llave pública en formato .CER.

Cuidados del dispositivo:

- Todos los cuidados físicos y/o digitales relacionados con las claves públicas y privadas del certificado digital emitido bajo este formato son de responsabilidad exclusiva del suscriptor.

Riesgos asociados:

- Para el certificado en PKCS#10 los riesgos a los cuales se encuentra expuesto el HSM de producción que se encuentra en data center con certificado TIER III e ISO 27001.
- En temas lógicos, los riesgos asociados se encuentran definidos por ataques

cibernéticos que impidan el acceso y/o disponibilidad respectiva para la firma del certificado.
- Por parte del suscriptor, tendrá los riesgos asociados al dispositivo el cual posea las claves públicas y privadas asociadas al certificado digital emitido bajo este protocolo

10.3 CERTIFICADO DE TITULAR DE FUNCIÓN PÚBLICA EN DISPOSITIVOS LOCALES O CENTRALIZADOS

Se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante PKI SERVICES con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero, permitiendo identificar como persona natural y vinculándola como funcionario público perteneciente a una entidad del Estado en la República de Colombia.

Los suscriptores de este tipo de certificados digitales son las personas naturales que logren acreditar suficientemente, a juicio de PKI SERVICES, que han obtenido el nombramiento o son titulares legales del cargo de notario, cónsul, juez de la república, magistrado, registrador o servidor público en la República de Colombia y que se encuentran en ejercicio del mismo.

El Certificado de Titular de Función Pública no garantiza la calidad, idoneidad o cumplimiento efectivo de las funciones a cargo de su titular. PKI SERVICES no garantiza que el suscriptor del certificado de Titular de Función Pública haya sido sujeto de sanciones disciplinarias, administrativas, penales o de cualquier otra clase en la República de Colombia o en el exterior. Para la emisión de Certificado de Titular de Función Pública PKI SERVICES se basa en la documentación exhibida y las declaraciones efectuadas por el suscriptor. Mientras la ley o las normas aplicables no establezcan lo contrario, la solicitud de Emisión del Certificado de Función Pública no es obligatoria para los Titulares de Función Pública. La emisión del Certificado de Función Pública no limita al suscriptor para solicitar otros certificados digitales.

Requisitos:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente
- Certificado de Cámara de comercio o su equivalente no mayor a 30 días
- Registro único tributario – RUT del año vigente
- Resolución o acta de nombramiento, o contrato de servicios vigente, o de Certificado Laboral queindique el cargo no mayor a 30 días, con membrete de la institución.

Perfil del certificado:

"UsuarioFinal
": "correo",
"Clave":
"XXXXX",
"Nombre": "NOMBRE

SUSCRIPTOR",
"Apellido": "APELLIDO
SUSCRIPTOR",
"NombreComun": "NOMBRE COMPLETO SUSCRIPTOR - RESOLUCIÓN",
"Organizacion" :
"EMPRESA PUBLICA",
"Localidad": "CIUDAD",
"Titulo": "FP",
"Pais" : "PAIS",
"Estado": "ESTADO /
DEPARTAMENTO", "Calle":
"DIRECCION ENTIDAD",
"Correo": "CORREO",
"OrganizacionId": "NIT",
"SERIALNUMBER":
"NUMERO CEDULA",
"TipoCertificado":
"Funcion Publica",
"DuracionCertificado":
"X", "LongitudRsaKey":
"2048"
“Valido_desde”
“Valido_hasta”

Certificado digital en Dispositivo Local

Corresponde a un estándar de generación de llaves públicas y privadas desde la infraestructura tecnológica del firmante y por responsabilidad del mismo, con el propósito de obtener certificados digitales acreditados por una entidad de certificación digital.

Características:

- Llave pública de 2048 bits RSA o 256 bits ECDSA
- Algoritmo de firma de certificado con hash SHA 256
- Llave pública firmada en formato *.CER conforme a la cadena de confianza de PKI SERVICES.
- Emisión haciendo uso del estándar PKCS#10 autorizados por ONAC.
- Generar un Certificate Signing Request – CSR – en formato PKCS#10.
- Capacidad de recibir y usar la llave pública en formato .CER.

Cuidados del dispositivo:

- Todos los cuidados físicos y/o digitales relacionados con las claves públicas y privadas del certificado digital emitido bajo este formato son de responsabilidad exclusiva del suscriptor.

Riesgos asociados:

- Para el certificado en PKCS#10 los riesgos a los cuales se encuentra expuesto el HSM de producción que se encuentra en data center con certificado TIER III e ISO 27001.
- En temas lógicos, los riesgos asociados se encuentran definidos por ataques cibernéticos que impidan el acceso y/o disponibilidad respectiva para la firma del certificado.
- Por parte del suscriptor, tendrá los riesgos asociados al dispositivo el cual posea las claves públicas y privadas asociadas al certificado digital emitido bajo este protocolo

10.4 CERTIFICADO DIGITAL PERSONA NATURAL / PERSONA JURIDICA EN DISPOSITIVOS LOCALES O CENTRALIZADOS

Se expide a personas naturales nacionales o extranjeras que se han identificado plenamente ante PKI SERVICES con documento(s) de identidad válido(s) y vigente(s) expedidos por la autoridad competente de la República de Colombia, o con documento(s) equivalente(s) expedido(s) por la autoridad competente de cualquier Estado Extranjero.

Los Certificados de Persona Natural / Persona Jurídica tienen como suscriptor a la persona natural que actuando en nombre propio logre acreditar suficientemente a juicio de PKI SERVICES su vinculación con la representación legal de una persona jurídica o con la representación legal de sí mismo en el ámbito de su actividad profesional o mercantil para persona natural.

PERSONA NATURAL

Requisitos:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte
- Registro único Tributario – RUT del año vigente
- Un Recibo de servicios públicos.

Perfil del certificado:

"UsuarioFinal
": "correo",
"Clave":
"XXXXX",
"NombreComun": "NOMBRE COMPLETO SUSCRIPTOR",
"Localidad":
"CIUDAD",
"Titulo":
"PN",
"Pais" : "PAIS",
"Estado": "ESTADO /
DEPARTAMENTO", "Calle":
"DIRECCION",
"Correo": "CORREO",
"SERIALNUMBER": "NUMERO CEDULA",
"TipoCertificado":
Persona Natural",
"DuracionCertificado":
"X", "LongitudRsaKey":
"2048"
“Valido_desde”
“Valido_hasta”

Certificado digital en Dispositivo Local

Corresponde a un estándar de generación de llaves públicas y privadas desde la infraestructura tecnológica del firmante y por responsabilidad del mismo, con el propósito de obtener certificados digitales acreditados por una entidad de certificación digital.

Características:

- Llave pública de 2048 bits RSA o 256 bits ECDSA
- Algoritmo de firma de certificado con hash SHA 256
- Llave pública firmada en formato *.CER conforme a la cadena de confianza de PKI SERVICES.
- Emisión haciendo uso del estándar PKCS#10 autorizados por ONAC.
- Generar un Certificate Signing Request – CSR – en formato PKCS#10.
- Capacidad de recibir y usar la llave pública en formato .CER.

Cuidados del dispositivo:

- Todos los cuidados físicos y/o digitales relacionados con las claves públicas y privadas del certificado digital emitido bajo este formato son de responsabilidad exclusiva del suscriptor.

Riesgos asociados:

- Para el certificado en PKCS#10 los riesgos a los cuales se encuentra expuesto el HSM de producción que se encuentra en data center con certificado TIER III e ISO 27001.
- En temas lógicos, los riesgos asociados se encuentran definidos por ataques cibernéticos que impidan el acceso y/o disponibilidad respectiva para la firma del certificado.
- Por parte del suscriptor, tendrá los riesgos asociados al dispositivo el cual posea las claves públicas y privadas asociadas al certificado digital emitido bajo este protocolo

PERSONA JURIDICA

Requisitos:

- Documento de identificación del representante legal: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte
- Certificado de Cámara de Comercio no mayor a 30 días
- Registro único Tributario – RUT del año vigente

Perfil del certificado:

"UsuarioFinal
": "correo",
"Clave":
"XXXXX",
"NombreComun": "NOMBRE COMPLETO ENTIDAD",
"Organización": "NOMBRE DE LA ENTIDAD",
"Localidad": "CIUDAD",
"Titulo": "PERSONA JURIDICA X AÑOS", donde X corresponde a 1 o 2 años
"Pais" : "PAIS",
"Estado": "ESTADO / DEPARTAMENTO", abreviaturas de país y departamento que utiliza wordpress y que equivale a la lista de los dominios de Internet.
"Calle": "DIRECCION",
"Correo": "CORREO",

"SERIALNUMBER": "NUMERO CEDULA",
"TipoCertificado": Persona
Juridica", "DuracionCertificado":
"X",
"LongitudRsaKey": "2048"
“Valido_desde”
“Valido_hasta”

Certificado digital en Dispositivo Local
Corresponde a un estándar de generación de llaves públicas y privadas desde la infraestructura tecnológica del firmante y por responsabilidad del mismo, con el propósito de obtener certificados digitales acreditados por una entidad de certificación digital.
Características:

- Llave pública de 2048 bits RSA o 256 bits ECDSA
- Algoritmo de firma de certificado con hash SHA 256
- Llave pública firmada en formato *.CER conforme a la cadena de confianza de PKI SERVICES.
- Emisión haciendo uso del estándar PKCS#10 autorizados por ONAC.
- Generar un Certificate Signing Request – CSR – en formato PKCS#10.
- Capacidad de recibir y usar la llave pública en formato .CER.

Cuidados del dispositivo:

- Todos los cuidados físicos y/o digitales relacionados con las claves públicas y privadas del certificado digital emitido bajo este formato son de responsabilidad exclusiva del suscriptor.

Riesgos asociados:

- Para el certificado en PKCS#10 los riesgos a los cuales se encuentra expuesto el HSM de producción que se encuentra en data center con certificado TIER III e ISO 27001.
- En temas lógicos, los riesgos asociados se encuentran definidos por ataques cibernéticos que impidan el acceso y/o disponibilidad respectiva para la firma del certificado.
- Por parte del suscriptor, tendrá los riesgos asociados al dispositivo el cual posea las claves públicas y privadas asociadas al certificado digital emitido bajo este protocolo

NOTA: El certificado contempla OCSP para admitir LTV

11. OTROS SERVICIOS DE CERTIFICACIÓN DIGITAL

11.1. Estampado Cronológico (TSA)

Mecanismo de seguridad y validez jurídica que da la fecha y hora exacta en la generación, envíoy recepción de información electrónica. Además, a través de un sello de tiempo certificado se garantiza la integridad de la información durante su ciclo de vida.

Se expide a personas naturales o jurídicas, nacionales o extranjeras que solicitan el servicio por medio de la página web de PKI SERVICES https://pkiservices.co/ sección servicios.

Un agente comercial se contactará con el solicitante por medio del correo registrado para llegar aacuerdos comerciales del servicio.

Requisitos:

Para persona natural:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente

Para persona jurídica:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente
- Certificado de Cámara de comercio no mayor a 30 días
- Registro único tributario – RUT del año vigente

Contrato del servicio

11.2. Notificación Electrónica en Correo Electrónico.

La Notificación Electrónica acreditada, es el servicio de registro, generación, transmisión y recepción de mensajes de datos electrónicos, mediante correo electrónico, los cuales cuentan con mecanismo de seguridad, tales que permiten verificar su trazabilidad de los momentos de envío y recepción y por lo tanto tener validez jurídica

La Notificación Electrónica acreditada, hace que las comunicaciones adquieran la misma credibilidad y misma validez legal del correo certificado tradicional físico de una carta certificada con acuse de recibo.

Se expide a personas naturales o jurídicas, nacionales o extranjeras que solicitan el servicio por medio de la página web de PKI SERVICES https://pkiservices.co/ sección servicios.

Un agente comercial se contactará con el solicitante por medio del correo registrado para llegar aacuerdos comerciales del servicio.

Requisitos:

Para persona natural:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente

Para persona jurídica:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente
- Certificado de Cámara de comercio no mayor a 30 días
- Registro único tributario – RUT del año vigente

Contrato del servicio

Correo y número de celular o móvil activos y válidos, es decir que se encuentren en

correcto funcionamiento al momento de usar los servicios de notificación electrónica.

11.3. Notificación Electrónica en Mensaje SMS

La Notificación Electrónica acreditada, es el servicio de registro, generación, transmisión y recepción de mensajes de datos electrónicos, mediante SMS, los cuales cuentan con mecanismo de seguridad, tales que permiten verificar su trazabilidad de los momentos de envío y recepción y por lo tanto tener validez jurídica

La Notificación Electrónica acreditada, hace que las comunicaciones adquieran la misma credibilidad y misma validez legal del correo certificado tradicional físico de una carta certificada con acuse de recibo.

Se expide a personas naturales o jurídicas, nacionales o extranjeras que solicitan el servicio por medio de la página web de PKI SERVICES https://pkiservices.co/ sección servicios.

Un agente comercial se contactará con el solicitante por medio del correo registrado para llegar aacuerdos comerciales del servicio.

Requisitos:

Para persona natural:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente

Para persona jurídica:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente
- Certificado de Cámara de comercio no mayor a 30 días
- Registro único tributario – RUT del año vigente

Contrato del servicio

Correo y número de celular o móvil activos y válidos, es decir que se encuentren en correcto funcionamiento al momento de usar los servicios de notificación electrónica.

11.4. Archivo y conservación de documentos electrónicos transferibles y mensajes de datos.

Mediante la solución tecnológica e–Título Valor prestamos el servicio Archivo y conservación de documentos electrónicos transferibles y documentos electrónicos transferibles con los más altos estándares de seguridad, diseñada para asegurar su ciclo de vida y anotaciones, permitiendo que los Títulos Valores electrónicos nazcan a la vida jurídica de forma inmaterial cumpliendo y garantizando todos los elementos de integridad, validez y confiabilidad jurídica, como lo es la autenticidad y el no repudio de cada anotación que conforman la trazabilidad almacenada en el mismo Título Valor.

Se expide a personas naturales o jurídicas, nacionales o extranjeras que solicitan el servicio por medio de la página web de PKI SERVICES https://pkiservices.co/ sección servicios.

Es necesario que los operadores de los Títulos valores designados por el cliente, tengan un certificado digital de pertenencia a empresa para que puedan registrar las anotaciones.

Un agente comercial se contactará con el solicitante por medio del correo registrado para llegar aacuerdos comerciales del servicio.

Requisitos:

Para persona natural:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente

Para persona jurídica:

- Documento de identificación: Cédula de ciudadanía, Cédula de extranjería, o Pasaporte vigente
- Certificado de Cámara de comercio no mayor a 30 días
- Registro único tributario – RUT del año vigente

Contrato

Seriales de Certificados de pertenencia a empresa

11.5. Firmas electrónicas

Las firmas electrónicas, tienen como suscriptor a la persona natural o jurídica que actuando en nombre propio logre acreditar suficientemente su identidad a través de los métodos de validación de identidad dispuestos por PKI SERVICES, como son tecnologías de biometría, video, voz, registro fotográfico, código único, entre otras tecnologías bajo el principio de neutralidad tecnológica, previsto en el numeral 6 del artículo 2 de la Ley 1341 de 2009 (decreto 2364 de 2012).

La evidencia de identificación que a juicio de PKI SERVICES considere suficiente, quedara incrustada en el documento PDF.

El SUSCRIPTOR, entienden que la Firma Electrónica es apropiada y confiable para los fines propios del uso que se le dará en los sistemas informáticos, de conformidad con el artículo 3 del Decreto 2364 de 2012.

Para efectos de lo dispuesto en el artículo 7 del Decreto 2364 del 2012 y el artículo 3 de la Resolución 70 del 03 de noviembre de 2016 o de la norma que la modifique, adicione o sustituya; el SUSCRIPTOR con el presente acuerdo, acepta que las técnicas de identificación acordadas cumplen los requisitos de firma electrónica, además conoce las medidas de seguridad para su utilización y los límites de responsabilidad conforme lo establecido en el presente documento.

Salvo que se incluya expresamente dentro del servicio, se entenderá que el SUSCRIPTOR tiene el deber de validar la identidad de los firmantes o las personas asociadas al certificado de firma electrónica, entregando a PKI SERVICES los datos completos de dichas personas para que se pueda emitir la firma electrónica.

PKI SERVICES no responderá por errores en la validación de identidad por parte del SUSCRIPTOR ni por la autenticidad de los documentos.

La firma electrónica no garantiza la calidad, idoneidad o cumplimiento efectivo para elcual se está usando. Para la emisión de firma electrónica PKI SERVICES se basa en la documentación exhibida y las declaraciones efectuadas por el suscriptor. Y no limita al suscriptor para solicitar otros certificados digitales o servicios de certificación digital ofrecidos por PKI SERVICES.

12. REQUISITOS TÉCNICOS

SERVICIOS DE CERTIFICACION DIGITAL (1)	**ACTIVIDADES DE CERTIFICACIÓN Artículo 161 del Decreto Ley 0019 de 2012 (2)**	**DOCUMENTOS NORMATIVOS O TÉCNICOS Anexos CEA-3.0-07 Versión 2 (3)**
Emisión de certificados digitales para Representación de Empresa/Entidad en dispositivos Locales o Centralizados	1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales ojurídicas 2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles. 3. Emitir certificados en relación con la personaque posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la ley 527 de 1999	ECDSA 521 bits para la CA Raíz ECDSA 384 bits para la Subordinada ECDSA 256 bits para entidad final RSA 2048 SHA-256 tamaño de clave mínimo 2048 bits agosto 2002 RFC 3647 noviembre 2003 RFC 5280 mayo 2008 RFC 6960 junio 2013 RFC 6979 agosto 2013 FIPS 140-2 Nivel 3 mayo 2001

Emisión de certificados digitales para Pertenencia a Empresa/Entidad en dispositivos Locales o Centralizados	1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales ojurídicas 2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles. 3. Emitir certificados en relación con la personaque posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la ley 527 de1999	ECDSA 521 bits para la CA Raíz ECDSA 384 bits para la Subordinada ECDSA 256 bits para entidad final RSA 2048 SHA-256 tamaño de clave mínimo 2048 bitsagosto 2002 RFC 3647 noviembre 2003 RFC 5280 mayo 2008 RFC 6960 junio 2013 RFC 6979 agosto 2013 FIPS 140-2 Nivel 3 mayo 2001
Emisión de certificados digitales para Titular de Función Pública en dispositivos Locales o Centralizados	1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales ojurídicas 2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles. 3. Emitir certificados en relación con la personaque posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la ley 527 de 1999	ECDSA 521 bits para la CA Raíz ECDSA 384 bits para la Subordinada ECDSA 256 bits para entidad final RSA 2048 SHA-256 tamaño de clave mínimo 2048 bitsagosto 2002 RFC 3647 noviembre 2003 RFC 5280 mayo 2008 RFC 6960 junio 2013 RFC 6979 agosto 2013 FIPS 140-2 Nivel 3 mayo 2001
Emisión de certificados digitales para Persona natural / Persona Jurídica en dispositivos Locales o Centralizados	1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales ojurídicas 2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles. 3. Emitir certificados en relación con la personaque posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la ley 527 de 1999	ECDSA 521 bits para la CA Raíz ECDSA 384 bits para la Subordinada ECDSA 256 bits para entidad final RSA 2048 SHA-256 tamaño de clave mínimo 2048 bitsa gosto 2002 RFC 3647 noviembre 2003 RFC 5280 mayo 2008 RFC 6960 junio 2013 RFC 6979 agosto 2013 FIPS 140-2 Nivel 3 mayo 2001

Estampado cronológico	5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.	RSA 2048 SHA-256 tamaño de clave mínimo 2048 bitsagosto 2002 RFC 3161 agosto 2001 RFC 3628 noviembre 2003 RFC 5280 mayo 2008 FIPS 140-2 nivel 3 mayo 2001 RFC 6979 agosto 2013
Correo Electrónico certificado	5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos. 9. Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas.	ECDSA 521 bits para la CA Raíz ECDSA 384 bits para la CA Subordinada ECDSA 256 bits para entidad final RSA 2048 para entidad final SHA 256 con ECDSA Encryption RFC 3161 agosto 2001 RFC 3628 noviembre 2003 RFC 5280 mayo 2008 FIPS 140-2 nivel 3 mayo 2001 RFC 6979 agosto 2013 ETSI 319 142-1 abril 2016
SMS.certificado	5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos. 9. Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas.	ECDSA 521 bits para la CA Raíz ECDSA 384 bits para la CA Subordinada ECDSA 256 bits para entidad final RSA 2048 para entidad final SHA 256 con ECDSA Encryption RFC 3161 agosto 2001 RFC 3628 noviembre 2003 RFC 5280 mayo 2008 FIPS 140-2 nivel 3 mayo 2001 RFC 6979 agosto 2013 ETSI 319 142-1 abril 2016
Archivo y conservación de documentos electrónicos transferibles y mensajes de datos	8. Ofrecer los servicios de archivo y conservación de mensajes de datos y documentos electrónicos transferibles.	NTC-ISO 14641-1 2014

13. TARIFAS

La tarifa para la prestación del servicio de Certificados Digitales y Servicios de Certificación Digital, será establecida con base en las necesidades del cliente y de acuerdo con la volumetría que el cliente requiera. La siguiente tabla, muestra los precios base de venta al público por unidad.

CERTIFICADOS CENTRALIZADOS	PVP 2023 Un Año	PVP 2023 Dos Años
CERTIFICADO DE REPRESENTACIÓN DE EMPRESA/ENTIDAD	$ 130,000.00	$ 200,000.00
CERTIFICADO DE PERTENENCIA A EMPRESA/ENTIDAD	$ 130,000.00	$ 200,000.00
CERTIFICADO DE TITULAR DE FUNCIÓNPÚBLICA	$ 130,000.00	$ 200,000.00
CERTIFICADO DIGITAL PERSONA NATURAL	$ 130,000.00	$ 200,000.00
CERTIFICADO DIGITAL PERSONA JURIDICA	$ 400,000.00	$ 600,000.00
ESTAMPA DE TIEMPO	Negociación	Negociación
NOTIFICACIÓN ELECTRÓNICO EN CORREO ELECTRÓNICO	Negociación	Negociación
NOTIFICACIÓN ELECTRÓNICO EN SMS	Negociación	Negociación
ARCHIVO Y CONSERVACION DE DOCUMENTOS ELECTRÓNICOS TRANSFERIBLES Y MENSAJES DE DATOS	Negociación	Negociación
FIRMA ELECTRÓNICA	Negociación	Negociación

RANGO ESTAMPADO CRONOLÓGICO	VALOR UNITARIO SIN IVA
Hasta 100.000	**$ 85,0**
100.001 – 500.000	**$ 70,0**
500.001 – 1.000.000	**$ 55,0**
1.000.001 – 3.000.000	**$ 42,0**
3.000.001 en adelante	**$ 30,0**

Carlos Andrés Piragauta

Gerente.
Bogotá, 07-07-2023