

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

POLÍTICA DE CERTIFICACIÓN

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

Índice

ÍNDICE.....	2
1. INTRODUCCIÓN	5
1.1. PRESENTACIÓN.....	5
1.2. DESCRIPCIÓN DE LA POLITICA	6
1.3. PARTICIPANTES EN LOS SERVICIOS DE CERTIFICACIÓN	6
1.3.1. <i>Entidad de Certificación Acreditada</i>	7
1.3.1.1. DIGIFIRMA CA RAÍZ.....	7
1.3.1.2. DIGIFIRMA CA SUBORDINADA 1	8
1.3.2. <i>Unidad de Registro</i>	8
1.3.3. <i>Entidades finales</i>	9
1.3.3.1. Suscriptores del servicio de certificación.....	9
1.3.3.2. Firmantes.....	9
1.3.3.3. Partes usuarias.....	10
1.3.4. <i>Proveedor de Servicios de Infraestructura de Clave Pública</i>	10
1.4. USO DE LOS CERTIFICADOS.....	11
1.4.1. <i>Usos permitidos para los certificados</i>	12
1.4.1.1. Certificado cualificado de persona física en P12	12
1.4.1.2. Certificado cualificado de persona física en QSCD	13
1.4.1.3. Certificado cualificado de persona física con Vinculo Institucional en P12	14
1.4.1.4. Certificado cualificado de persona física con Vinculo Institucional en QSCD.....	15
1.4.1.5. Certificado cualificado de persona física para Procedimientos Tributarios en P12	16
1.4.1.6. Certificado cualificado de persona física para Procedimientos Tributarios en QSCD.....	17
1.4.1.7. Certificado cualificado de persona física representante en p12	18
1.4.1.8. Certificado cualificado persona física representante en QSCD	19
1.4.1.9. Certificado cualificado de Sello Electrónico en p12.....	20
1.4.1.10. Certificado cualificado de Sello Electrónico en QSCD	20
1.4.2. <i>Límites y prohibiciones de uso de los certificados</i>	21
2. IDENTIFICACIÓN Y AUTENTICACIÓN	24
2.1. REGISTRO INICIAL.....	24
2.1.1. <i>Tipos de nombres</i>	24
2.1.1.1. Certificado cualificado de Persona Física ciudadano en p12	24
2.1.1.2. Certificado cualificado de Persona Física en QSCD	24
2.1.1.3. Certificado cualificado de Persona Física con Vinculo Institucional en p12	25

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2.1.1.4.	Certificado cualificado de Persona Física con Vínculo Institucional en QSCD	25
2.1.1.5.	Certificado cualificado de Persona Física para Procedimientos Tributarios en p12	26
2.1.1.6.	Certificado cualificado de Persona Física para Procedimientos Tributarios en QSCD	26
2.1.1.7.	Certificado cualificado de Persona Física Representante en p12	26
2.1.1.8.	Certificado cualificado de firma de Persona Física Representante en QSCD	27
2.1.1.9.	Certificado cualificado de Sello Electrónico en p12	27
2.1.1.10.	Certificado cualificado de Sello Electrónico en QSCD	27
2.1.2.	<i>Significado de los nombres</i>	28
2.1.3.	<i>Emisión de certificados del set de pruebas y certificados de pruebas en general</i>	28
2.1.4.	<i>Empleo de anónimos y seudónimos</i>	29
2.1.5.	<i>Interpretación de formatos de nombres</i>	29
2.2.	VALIDACIÓN INICIAL DE LA IDENTIDAD	29
2.2.1.	<i>Autenticación de la identidad de una organización, empresa o entidad mediante representante</i>	30
2.2.2.	<i>Autenticación de la identidad de una persona física</i>	33
2.2.2.1.	En los certificados	34
2.2.2.2.	Validación de la Identidad	35
2.2.2.3.	Vinculación de la persona física	36
2.3.	IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN	37
2.3.1.	<i>Validación para la renovación rutinaria de certificados</i>	37
2.3.2.	<i>Identificación y autenticación de la solicitud de renovación</i>	37
2.4.	IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN	38
3.	REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS	40
3.1.	SOLICITUD DE EMISIÓN DE CERTIFICADO	40
3.1.1.	<i>Legitimación para solicitar la emisión</i>	40
3.1.2.	<i>Procedimiento de alta y responsabilidades</i>	40
3.2.	PROCESAMIENTO DE LA SOLICITUD DE CERTIFICACIÓN	41
3.2.1.	<i>Ejecución de las funciones de identificación y autenticación</i>	41
3.2.2.	<i>Aprobación o rechazo de la solicitud</i>	41
3.3.	EMISIÓN DEL CERTIFICADO	42
3.4.	ENTREGA Y ACEPTACIÓN DEL CERTIFICADO	42
3.5.	USO DEL PAR DE CLAVES Y DEL CERTIFICADO	43
3.5.1.	<i>Uso por el firmante</i>	43
3.5.2.	<i>Uso por el suscriptor</i>	44
3.5.2.1.	Obligaciones del suscriptor del certificado	44
3.5.2.2.	Responsabilidad civil del suscriptor de certificado	45
3.5.3.	<i>Uso por el tercero que confía en certificados</i>	46

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

3.5.3.1.	Obligaciones del tercero que confía en certificados	46
3.5.3.2.	Responsabilidad civil del tercero que confía en certificados	47
3.6.	RENOVACIÓN DE CERTIFICADOS.....	47
3.7.	REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN DE CERTIFICADOS.....	47
3.7.1.	<i>Procedimientos de solicitud de revocación, suspensión o reactivación.....</i>	48
3.7.2.	<i>Obligación de consulta de información de revocación o suspensión de certificados</i>	49
3.7.3.	<i>Obligación de consulta de servicios de comprobación de estado de certificados.....</i>	50
4.	PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS.....	51
4.1.	PERFIL DE CERTIFICADO.....	51
4.1.1.	<i>Número de versión</i>	51
4.1.2.	<i>Identificadores de objeto (OID) de los algoritmos.....</i>	51
4.2.	PERFIL DE LA LISTA DE REVOCACIÓN DE CERTIFICADOS.....	51
4.2.1.	<i>Número de versión</i>	51
4.2.2.	<i>Perfil de OCSP.....</i>	52
5.	ANEXO I – ACRÓNIMOS	53
6.	CONTROL DE CAMBIOS Y APROBACIÓN	54

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

1. Introducción

1.1. Presentación

Este documento declara la política de certificación de firma electrónica Cámara de Comercio y Producción de Santo Domingo, en adelante CCPSD, dando cumplimiento a los requisitos dispuestos en la Ley n° 126-02 sobre comercio electrónico, documentos y firmas digitales, su reglamento general de aplicación, junto con las normas complementarias aplicables, así como las normas técnicas del ETSI aplicables a la expedición y gestión de certificados, principalmente EN 319 411-1 y EN 319 411-2, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Los certificados que se emiten son los siguientes:

De Persona Física

- Certificado cualificado de Persona Física en p12
- Certificado cualificado de Persona Física en QSCD
- Certificado cualificado de Persona Física con Vínculo Institucional en p12
- Certificado cualificado de Persona Física con Vínculo Institucional en QSCD
- Certificado cualificado de Persona Física para Procedimientos Tributarios en p12
- Certificado cualificado de Persona Física para Procedimientos Tributarios en QSCD

De Persona Física Representante

- Certificado cualificado de Persona Física Representante en p12
- Certificado cualificado de Persona Física Representante en QSCD

De Sello de Empresa

- Certificado cualificado de Sello Electrónico en p12

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- Certificado cualificado de Sello Electrónico en QSCD

1.2. Descripción de la Política

CCPSD ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

Número OID	Tipo de certificados
	Persona Física
1.3.6.1.4.1.26236.1.1.1	<i>Certificado cualificado de Persona Física en p12</i>
1.3.6.1.4.1.26236.1.1.2	<i>Certificado cualificado de Persona Física en QSCD</i>
1.3.6.1.4.1.26236.1.2.1	<i>Certificado cualificado de Persona Física con Vínculo Institucional en p12</i>
1.3.6.1.4.1.26236.1.2.2	<i>Certificado cualificado de Persona Física con Vínculo Institucional en QSCD</i>
1.3.6.1.4.1.26236.1.3.1	<i>Certificado cualificado de Persona Física para Procedimientos Tributarios en p12</i>
1.3.6.1.4.1.26236.1.3.2	<i>Certificado cualificado de Persona Física para Procedimientos Tributarios en QSCD</i>
	Representante de entidad
1.3.6.1.4.1.26236.1.4.1	<i>de Persona Física de firma Representante en p12</i>
1.3.6.1.4.1.26236.1.4.2	<i>de Persona Física de firma Representante en QSCD</i>
	Sello Electrónico
1.3.6.1.4.1.26236.1.5.1	<i>de Sello Electrónico en p12</i>
1.3.6.1.4.1.26236.1.5.2	<i>de Sello Electrónico en QSCD</i>

1.3. Participantes en los servicios de certificación

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

1.3.1. Entidad de Certificación Acreditada

La Entidad de Certificación acreditada es la persona, física o jurídica, que expide y gestiona certificados para entidades finales, empleando una Autoridad de Certificación, o presta otros servicios relacionados con la firma electrónica.

CCPSD es una Entidad de Certificación acreditada o Prestador de Servicios de Confianza, que actúa de acuerdo con lo dispuesto en la Ley nº 126-02 sobre comercio electrónico, documentos y firmas digitales, su reglamento general de aplicación, junto con las normas complementarias aplicables, así como las normas técnicas del ETSI aplicables a la expedición y gestión de certificados, principalmente EN 319 411-1 y EN 319 411-2, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, CCPSD ha establecido una jerarquía de Autoridades de certificación:



1.3.1.1. DIGIFIRMA CA RAÍZ

Se trata de la Entidad de Certificación raíz de la jerarquía que emite certificados a otras Autoridades de certificación, y cuyo certificado de clave pública ha sido auto firmado.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

Datos de identificación:

CN: digifirma CA Raíz
Huella digital: d6ea339754cf4b6f41526a8e2a65a273575fe8fa
Válido desde: martes, 20 de julio de 2021
Válido hasta: jueves, 26 de julio de 2046 12:05:26
Longitud de clave RSA: 4.096 bits

1.3.1.2. DIGIFIRMA CA SUBORDINADA 1

Se trata de la Entidad de Certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la DIGIFIRMA CA RAÍZ.

Datos de identificación:

CN: digifirma CA Subordinada 1
Huella digital: 8d42a1098951a508d5ea1daa2a16958d348989cc
Válido desde: martes, 20 de julio de 2021
Válido hasta: domingo, 23 de julio de 2034
Longitud de clave RSA: 4.096 bits

1.3.2. Unidad de Registro

Una Unidad de Registro de CCPSD es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- Gestionar la generación de claves y la emisión del certificado
- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

1.3.3. Entidades finales

Las entidades finales son las personas u organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de autenticación y firma electrónica.

Serán entidades finales de los servicios de certificación de CCPSD las siguientes:

1. Suscriptores del servicio de certificación
2. Firmantes
3. Partes usuarias

1.3.3.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- Las empresas, entidades, corporaciones u organizaciones que los adquieren a CCPSD (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo, y se encuentran identificados en los certificados.
- Las personas físicas que adquieren los certificados para sí mismas, y se encuentran identificados en los certificados.

1.3.3.2. Firmantes

Los firmantes son las personas físicas que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma avanzada o cualificada, de acuerdo con los perfiles de este documento; siendo típicamente los empleados, representantes legales

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

o voluntarios, así como otras personas vinculadas a los suscriptores; incluyendo las personas al servicio de las Administraciones Públicas, en los certificados de empleado público.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre, apellidos, dirección y número de identificación inequívoco, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por el prestador de servicios electrónicos de confianza, por lo que las personas físicas identificadas en los correspondientes certificados son las únicas responsables de su protección y deberían considerar las implicaciones de perder una clave privada.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la autenticación, también se emplea el término más genérico de “persona física identificada en el certificado”, siempre con pleno respeto al cumplimiento de la regulación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.3.3.3. Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas electrónicas y certificados digitales.

1.3.4. Proveedor de Servicios de Infraestructura de Clave Pública

CCPSD y Uanataca, S.A., han suscrito un contrato de prestación de servicios de tecnología mediante el cual la compañía Uanataca, S.A proveerá la infraestructura de clave pública (PKI) que sustenta el servicio de certificación de CCPSD. En este sentido Uanataca, S.A., pone a disposición de CCPSD el personal técnico necesario para correcto desempeño de las funciones fiables propias de un Entidad de Certificación acreditada.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

Dicho lo cual, Uanataca, S.A., se configura como el proveedor de servicios de Infraestructura para servicios de certificación, provee sus servicios tecnológicos a CCPSD para que éste pueda llevar a cabo los servicios inherentes a un Entidad de Certificación acreditada, garantizando en todo momento la continuidad de los servicios en las condiciones y bajo los requisitos exigidos por la normativa.

La PKI de Uanataca, S.A., se somete a auditorías anuales para la evaluación de la conformidad de prestadores cualificados de servicios de confianza de acuerdo con la normativa aplicable, bajo las normas:

- a. ISO/IEC 17065:2012
- b. ETSI EN 319 403
- c. ETSI EN 319 421
- d. ETSI EN 319 401
- e. ETSI EN 319 411-2
- f. ETSI EN 319 411-1

Asimismo, la PKI de Uanataca, S.A., se somete a auditorías anuales bajo los estándares de seguridad:

- a. ISO 9001:2015
- b. ISO/IEC 27001:2014

1.4. Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

1.4.1. Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, disponibles en el web <https://www.camarasantodomingo.do/digifirma/>

1.4.1.1. Certificado cualificado de persona física en P12

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.1.1. Es un certificado cualificado que se emite para la firma electrónica avanzada y autenticación, de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0. Este certificado de persona física se emite en archivo p12, de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de persona física emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma.

Garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

- a) Autenticación en sistemas de control de acceso.
- b) Firma de correo electrónico seguro.
- c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación).
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.2. Certificado cualificado de persona física en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.1.2. Es un certificado cualificado que se emite para la firma electrónica cualificada y autenticación, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de persona física emitido en QSCD de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Funciona con dispositivos cualificados de creación de firma, dando cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de confianza, y permite la generación de la “firma electrónica cualificada”; por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación).
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.3. Certificado cualificado de persona física con Vinculo Institucional en P12

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.2.1. Es un certificado cualificado que se emite para la firma electrónica avanzada y autenticación, de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0. Este certificado de persona física con Vinculo Institucional se emite en archivo p12, de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de persona física con Vinculo Institucional emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma.

Garantizan la identidad del suscriptor y del firmante, y una relación entre el firmante y una entidad, empresa u organización descrita en el campo “O” (Organization), y permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

- a) Autenticación en sistemas de control de acceso.
- b) Firma de correo electrónico seguro.
- c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación).
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.4. Certificado cualificado de persona física con Vinculo Institucional en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.2.2. Es un certificado cualificado que se emite para la firma electrónica cualificada y autenticación, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de persona física con Vinculo Institucional se emite en QSCD de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Funciona con dispositivos cualificados de creación de firma, dando cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantizan la identidad del suscriptor y del firmante, y una relación entre el firmante y una entidad, empresa u organización descrita en el campo “O” (Organization), y permite la generación de la “firma electrónica cualificada”; por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma electrónica.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación).
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.5. Certificado cualificado de persona física para Procedimientos Tributarios en P12

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.3.1. Es un certificado cualificado que se emite para la firma electrónica avanzada y autenticación, de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0. Este certificado de persona física para Procedimientos Tributarios se emite en archivo p12, de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de persona física emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma.

Garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

Este certificado solo podrá ser utilizado para procedimientos tributarios del suscriptor identificado en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- a. Firma digital (Digital Signature, para realizar la función de autenticación).
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.6. Certificado cualificado de persona física para Procedimientos Tributarios en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.3.2. Es un certificado cualificado que se emite para la firma electrónica cualificada y autenticación, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de persona física para Procedimientos Tributarios se emite en QSCD de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Funciona con dispositivos cualificados de creación de firma, dando cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de confianza, y permite la generación de la "firma electrónica cualificada"; por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Este certificado solo podrá ser utilizado para procedimientos tributarios del suscriptor identificado en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación).

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.7. Certificado cualificado de persona física representante en p12

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.4.1. Es un certificado cualificado que se emite para la firma electrónica avanzada y autenticación, de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0. Este certificado de representante se emite en archivo p12, de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de persona física emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma.

Garantizan la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

Por otra parte, los certificados de representante emitido en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.8. Certificado cualificado persona física representante en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.4.2. Es un certificado cualificado que se emite para la firma electrónica cualificada y autenticación, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de representante se emite en QSCD de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Funciona con dispositivos cualificados de creación de firma, dando cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la "firma electrónica cualificada", por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.9. Certificado cualificado de Sello Electrónico en p12

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.5.1, y es un certificado que se emite de acuerdo con la política de certificación QCP-I con el OID 0.4.0.194112.1.1. Los certificados de sello electrónico son certificados cualificados emitidos de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de persona física emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:

El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación)
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- c. Key Encipherment

1.4.1.10. Certificado cualificado de Sello Electrónico en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.26236.1.5.2, y es un certificado cualificado que se emite de acuerdo con la política de certificación QCP-I-qscd con el OID

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

0.4.0.194112.1.3. Los certificados de sello electrónico son cualificados y emitidos de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Funciona con dispositivos cualificados de creación de firma, dando cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación)
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- c. Key Encipherment

1.4.2. Límites y prohibiciones de uso de los certificados

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la regulación aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

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 aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, disponibles en la web de CCPSD.

El empleo de los certificados digitales en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos con las Unidades de Registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a CCPSD, en función de la legislación vigente, de responsabilidades que provengan del uso indebido de los certificados ya sea realizado el uso por el firmante o por tercero.

CCPSD no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, y por ello no es posible emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las Unidades de Registro o con sus suscriptores, así como de cualquier

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2. Identificación y autenticación

2.1. Registro inicial

2.1.1. Tipos de nombres

Todos los certificados contienen un nombre distintivo (DN o *distinguished name*) conforme al estándar X.509 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la persona física identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

2.1.1.1. Certificado cualificado de Persona Física ciudadano en p12

Country Name	Estado
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCDO-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del firmante

2.1.1.2. Certificado cualificado de Persona Física en QSCD

Country Name	Estado
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCDO-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del firmante

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2.1.1.3. Certificado cualificado de Persona Física con Vínculo Institucional en p12

Country Name	Estado
Organization Name	Organización a la que pertenece el firmante
Organizational Unit Name	Departamento al que pertenece el firmante o el tipo de vinculación con la organización
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATDO-Q0000000J")
Title	Nombre del título o puesto que la persona ocupa en la Empresa o Entidad.
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCDO-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización

2.1.1.4. Certificado cualificado de Persona Física con Vínculo Institucional en QSCD

Country Name	Estado
Organization Name	Organización a la que pertenece el firmante
Organizational Unit Name	Departamento al que pertenece el firmante o el tipo de vinculación con la organización
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATDO-Q0000000J")
Title	Nombre del título o puesto que la persona ocupa en la Empresa o Entidad.
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCDO-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2.1.1.5. Certificado cualificado de Persona Física para Procedimientos Tributarios en p12

Country Name	Estado
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCDO-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del firmante

2.1.1.6. Certificado cualificado de Persona Física para Procedimientos Tributarios en QSCD

Country Name	Estado
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCDO-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del firmante

2.1.1.7. Certificado cualificado de Persona Física Representante en p12

Country Name	Estado
Organization Name	Organización de la que el firmante es representante
Organizational Unit Name	Departamento al que pertenece representante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATDO-Q0000000J")
Title	Nombre del título o puesto del Representante
Surname	Apellidos del representante (como consta en el documento oficial)
Given Name	Nombre del representante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCDO-12345678Z")
Common Name	00000000T NOMBRE APELLIDOS DEL REPRESENTANTE (R: Q0000000J)
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2.1.1.8. Certificado cualificado de firma de Persona Física Representante en QSCD

Country Name	Estado
Organization Name	Organización de la que el firmante es representante
Organizational Unit Name	Departamento al que pertenece representante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATDO-Q0000000J")
Title	Nombre del título o puesto del Representante
Surname	Apellidos del representante (como consta en el documento oficial)
Given Name	Nombre del representante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319412-1 ("IDCDO-12345678Z")
Common Name	00000000T NOMBRE APELLIDOS DEL REPRESENTANTE (R: Q0000000J)
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización

2.1.1.9. Certificado cualificado de Sello Electrónico en p12

Country Name	Estado
Organization Name	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)
Organizational Unit Name	Denominación de la unidad
Organization Identifier	Número oficial de identificación de la Persona Jurídica a la que está vinculado el sello en formato ETSI EN 319412-1 (Ejemplo: "VATDO-Q0000000J")
Surname	Apellidos del responsable del sello (como consta en el documento oficial)
Given Name	Nombre del responsable del sello (como consta en el documento oficial)
Serial Number	Número oficial de identificación de la Persona Jurídica
Common Name	Nombre descriptivo del creador del sello. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la entidad

2.1.1.10. Certificado cualificado de Sello Electrónico en QSCD

Country Name	Estado
---------------------	--------

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

Organization Name	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)
Organizational Unit Name	Denominación de la unidad
Organization Identifier	Número oficial de identificación de la Persona Jurídica a la que está vinculado el sello en formato ETSI EN 319412-1 (Ejemplo: "VATDO-Q000000J")
Surname	Apellidos del responsable del sello (como consta en el documento oficial)
Given Name	Nombre del responsable del sello (como consta en el documento oficial)
Serial Number	Número oficial de identificación de la Persona Jurídica
Common Name	Nombre descriptivo del creador del sello. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la entidad

2.1.2. Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

2.1.3. Emisión de certificados del set de pruebas y certificados de pruebas en general

En el caso que los datos indicados en el DN o Subject fueran ficticios (ej. "Test Organization", "Test Nombre", "Apellido1") o se indique expresamente palabras que denoten su invalidez (ej. "TEST", "PRUEBA" o "INVALIDO"), se considerará al certificado sin validez legal y por lo tanto sin responsabilidad alguna sobre CCPSD. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y permitir al ente regulador su evaluación.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2.1.4. Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad, empresa u organización, ni a un firmante. Así mismo, en ningún caso se emiten certificados anónimos.

2.1.5. Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” o “estado” será el del suscriptor del certificado.

Los certificados cuyos suscriptores sean personas jurídicas, entidades u organismos de la administración pública, muestran la relación entre estas y una persona física, con independencia de la nacionalidad de la persona física.

En el campo “número de serie” se incluye el número del documento oficial de identidad, de acuerdo con un documento de identidad reconocido en derecho.

2.2. Validación inicial de la identidad

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre CCPSD y el suscriptor, previa verificación de la existencia del suscriptor a través de los procedimientos de reconocimiento establecidos y mediante la comprobación de su documento oficial de identidad o las escrituras correspondientes, al igual que los poderes de actuación de la persona que presente como representante si fuese el caso. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

En el caso de personas naturales identificadas en certificados cuyo suscriptor sea una persona jurídica, sus identidades se validarán mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a CCPSD, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

2.2.1. Autenticación de la identidad de una organización, empresa o entidad mediante representante

Las personas físicas con capacidad de actuar en nombre de las personas jurídicas o entidades sin personalidad jurídica, públicas o privadas, que sean suscriptoras de certificados, podrán actuar como representantes de estas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona física y la organización de la que se trate, que exige su reconocimiento por CCPSD, la cual se realizará mediante el siguiente procedimiento:

- El representante y/o suscriptor deberá acreditar su identidad por uno de los siguientes métodos:(i) Identificándose presencialmente ante un operador o persona autorizada de una Unidad de Registro de CCPSD:
 - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
 - Acreditando el carácter y facultades que alegue poseer.
- (ii) Identificándose electrónicamente a través del sistema de video identificación remota de CCPSD:
 - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.
 - Proveyendo prueba de vida través de un video grabado de al menos 30 segundos, y en algunos casos, para una segunda validación, se procederá a tener una sesión virtual en vivo con el suscriptor.
 - Acreditando el carácter y facultades que alegue poseer.

- 2. El representante y/o suscriptor proporcionará la siguiente información y sus correspondientes soportes acreditativos:
 - Sus datos de identificación:
 - Nombre y apellidos
 - Lugar y fecha de nacimiento
 - Documento de identidad reconocido en derecho para la identificación del representante,
 - Correo electrónico
 - No. De contacto
 - Domicilio o dirección del firmante.
 - Los datos de identificación del suscriptor al que representa:
 - Denominación o razón social.
 - Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.
 - Documento de Identificación o documento acreditativo de la identificación fiscal de la entidad.
 - Documento: Documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

- Área o Departamento al cual pertenece.
 - Los datos relativos a la representación o la capacidad de actuación que ostenta:
 - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin) si resulta aplicable.
 - El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:
 - TOTAL. Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.
 - PARCIAL. Representación o capacidad parcial. Esta comprobación se podrá realizar mediante copia auténtica electrónica de la escritura notarial de apoderamiento, en los términos de la normativa notarial.
3. El operador o personal autorizado de la Unidad de Registro de CCPSD comprobará la identidad del representante actuando del siguiente modo:
- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
 - Documento de identidad aportado.
 - Documentación que acredite su representación.
 - Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de CCPSD mediante:

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
- Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota.
- Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
- Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.
- Revisión manual del video de prueba de vida recibido por el suscriptor.
- Documentación que acredite su representación.

4. Alternativamente, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar al operador o personal autorizado de la Unidad de Registro por correo postal certificado, en cuyo caso los pasos 3 y 4 anteriores no serán necesarios.

La prestación del servicio de certificación digital se formaliza mediante el oportuno contrato entre CCPSD y el suscriptor, debidamente representado.

2.2.2. Autenticación de la identidad de una persona física

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2.2.2.1. En los certificados

La identidad de las personas naturales firmantes identificados en los certificados, se valida a través de uno de los siguientes métodos:

- (i) Identificándose presencialmente ante un operador o persona autorizada de una Unidad de Registro de CCPSD:
 - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
- (ii) Identificándose electrónicamente a través del sistema de video identificación remota de CCPSD:
 - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
 - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.
 - Proveyendo prueba de a través de un video grabado de al menos 30 segundos, y en algunos casos, para una segunda validación, se procederá a tener una sesión virtual en vivo con el suscriptor.

La información de identificación de las personas naturales identificadas en los certificados (i) cuyo suscriptor sea una entidad con o sin personalidad jurídica o (ii) ya constase la misma en virtud de una relación previa, la información podrá ser validada comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, o bien con la documentación que esta haya suministrado sobre la persona natural que identifica como firmante, asegurando la corrección de la información a certificar.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2.2.2.2. Validación de la Identidad

El operador o personal autorizado de la Entidad de Registro de UANATACA comprobará la identidad de la persona natural identificada en la solicitud del certificado, actuando del siguiente modo:

- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
 - Documento de identidad aportado.
- Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de UANATACA mediante:
 - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
 - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota.
 - Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
 - Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.
 - Revisión manual del video de prueba de vida recibido por el suscriptor

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica no se requiere identificación expresa, debido a la relación ya acreditada entre la persona natural y entidad, empresa u organización de derecho público o privado a la que está vinculada. Sin embargo, antes de la entrega de un certificado, la entidad, empresa u organización de derecho público o privado suscriptora, por medio de su responsable de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la persona natural identificada en el certificado mediante su presencia física o siguiendo el procedimiento de video identificación remota establecido por UANATACA.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2.2.2.3. Vinculación de la persona física

La justificación documental de la vinculación de una persona física identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización...) de cada una de las personas públicas y privadas a las que están vinculadas.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

2.3. Identificación y autenticación de solicitudes de renovación

2.3.1. Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, el operador o personal autorizado de la Unidad de Registro comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son:

- El uso del código "CRE" o "ERC" relativo al certificado anterior, o de otros métodos de autenticación personal, que consiste en información que sólo conoce la persona física identificada en el certificado, y que le permite renovar de forma automática su certificado, siempre que no se haya superado el plazo máximo legalmente establecido.
- El empleo del certificado vigente para su renovación y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 2.2.

2.3.2. Identificación y autenticación de la solicitud de renovación

Antes de renovar un certificado, el operador o personal autorizado de la Unidad de Registro comprobará que la información empleada en su día para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona física identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 2.2.

2.4. Identificación y autenticación de la solicitud de revocación, suspensión o reactivación

CCPSD o un operador o personal autorizado de la Unidad de Registro autentica las peticiones e informes relativos a la revocación, suspensión o reactivación de un certificado, comprobando que provienen de una persona autorizada.

La identificación de los suscriptores y/o firmantes en el proceso de revocación, suspensión o reactivación de certificados podrá ser realizada por:

- El suscriptor y/o firmante:
 - Identificándose y autenticándose mediante el uso del Código de Revocación (ERC o ERC) a través de la página web de CCPSD en horario 24 horas al día 7 días a la semana.
 - Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la suspensión o revocación, a juicio de CCPSD y/o Unidades de Registro.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- Las Unidades de Registro deberán identificar al firmante ante una petición de revocación, suspensión o reactivación según los propios medios que considere necesarios.

Cuando en horario de oficina el suscriptor desee iniciar una petición de revocación y existan dudas para su identificación, su certificado pasa a estado de suspensión.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

3. Requisitos de operación del ciclo de vida de los certificados

3.1. Solicitud de emisión de certificado

3.1.1. Legitimación para solicitar la emisión

El solicitante del certificado sea persona física o jurídica, debe firmar un contrato de prestación de servicios de certificación con CCPSD.

Asimismo, con anterioridad a la emisión y entrega de un certificado, debe existir una solicitud de certificados ya sea en el mismo contrato, en un documento específico de hoja de solicitud de certificados o ante la Unidad de Registro.

Cuando el solicitante es una persona distinta al suscriptor, debe existir una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por dicho solicitante en nombre propio en el caso de certificados para persona física, o bien en nombre del suscriptor en el caso de que el suscriptor sea la por entidad, empresa u organización de derecho público o privado.

3.1.2. Procedimiento de alta y responsabilidades

CCPSD recibe solicitudes de certificados, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona física identificada en el certificado, de acuerdo con lo establecido en la sección 2.2.2. También se deberá acompañar una dirección física, u otros datos, tales como correo electrónico, teléfono de contacto, etc., que permitan contactar a la persona física identificada en el certificado.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

3.2. Procesamiento de la solicitud de certificación

3.2.1. Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, CCPSD se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, se verifica la información proporcionada, verificando los aspectos descritos en la sección 2.2.

En caso de un certificado cualificado, la documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 20 años desde la expiración del certificado, incluso en caso de pérdida anticipada de vigencia por revocación.

CCPSD, como entidad de certificación, lleva un registro de todos los certificados emitidos, que se encontrará a disposición del público, debiendo indicar las fechas de emisión, expiración y registros de suspensión, revocación o reactivación de estos. En este sentido, los registros de certificados expedidos por una entidad de certificación deben ser conservados por 40 años desde la fecha de revocación o expiración del certificado.

3.2.2. Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, la solicitud queda aprobada, y como consecuencia se aprueba la solicitud del certificado y se procede a su emisión y entrega.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

3.3. Emisión del certificado

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, CCPSD:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo de las claves por parte del usuario, no pudiendo la propia CCPSD o sus Unidades de Registro deducirlas o utilizarlas en ningún modo.

3.4. Entrega y aceptación del certificado

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

Cuando se haga entrega de la hoja de aceptación, la aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación.

3.5. Uso del par de claves y del certificado

3.5.1. Uso por el firmante

El firmante queda obligado a:

- Facilitar a CCPSD información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifiestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Cuando el certificado funcione juntamente con un Dispositivo Cualificado de Creación de Firma (DCCF), reconocer su capacidad de producción de firmas electrónicas digitales; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 1.4.2.
- Comunicar a CCPSD, Unidades de Registro y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
 - La pérdida, el robo o el compromiso potencial de su clave privada.
 - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
 - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.

El firmante queda obligado a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

3.5.2. Uso por el suscriptor

3.5.2.1. Obligaciones del suscriptor del certificado

El suscriptor queda obligado contractualmente a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifiestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4
- Comunicar a CCPSD, Unidades de Registro y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
 - La pérdida, el robo o el compromiso potencial de su clave privada.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

- La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
- Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas físicas identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de estas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación.

3.5.2.2. Responsabilidad civil del suscriptor de certificado

CCPSD obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

3.5.3. Uso por el tercero que confía en certificados

3.5.3.1. Obligaciones del tercero que confía en certificados

Se informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas, producidas en un dispositivo cualificado de creación de firma tienen la consideración legal de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

3.5.3.2. Responsabilidad civil del tercero que confía en certificados

CCPSD informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

3.6. Renovación de certificados

La renovación de los certificados exige la renovación de claves, de acuerdo con lo establecido en la Declaración de Prácticas de Certificación de CCPSD.

3.7. Revocación, suspensión o reactivación de certificados

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible. Sólo los certificados de entidad final podrán ser suspendidos.

La reactivación de un certificado supone su paso de estado suspendido a estado activo.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

3.7.1. Procedimientos de solicitud de revocación, suspensión o reactivación

La entidad que precise revocación, suspensión o reactivación de un certificado puede solicitarlo directamente a CCPSD a través de un correo electrónico a digifirma@camarasantodomingo.do. La solicitud de revocación, suspensión o reactivación deberá incorporar la siguiente información:

- Fecha de solicitud de la revocación, suspensión o reactivación.
- Identidad del suscriptor.
- Nombre y título de la persona que pide la revocación, suspensión o reactivación.
- Información de contacto de la persona que pide la revocación, suspensión o reactivación.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, de acuerdo con los requisitos establecidos en la sección 2.4 de esta política, antes de proceder a la revocación, suspensión o reactivación.

El servicio de revocación, suspensión o reactivación se encuentra en la página web de CCPSD en la dirección: <https://lcmpl.camarasantodomingo.do/>

En caso de que el destinatario de una solicitud de revocación, suspensión o reactivación por parte de una persona física identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a CCPSD.

La solicitud de revocación, suspensión o reactivación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la persona física identificada en el certificado, acerca del cambio de estado del certificado.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

Tanto el servicio de gestión de revocación, suspensión o reactivación como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencia y el plan de continuidad de negocio de CCPSD.

3.7.2. Obligación de consulta de información de revocación o suspensión de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de CCPSD.

Las Listas de Revocación de Certificados se publican en el Depósito de la Autoridad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- <http://crl1.camarasantodomingo.do/public/pki/crl/CCPSD.crl>
- <http://crl2.camarasantodomingo.do/public/pki/crl/CCPSD.crl>

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- <http://ocsp1.camarasantodomingo.do/public/pki/ocsp/>
- <http://ocsp2.camarasantodomingo.do/public/pki/ocsp/>

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

3.7.3. Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

4. Perfiles de certificados y listas de certificados revocados

4.1. Perfil de certificado

Todos los certificados cualificados emitidos bajo esta política cumplen con el estándar X.509 versión 3 y el RFC 3739 y los diferentes perfiles descritos en la norma EN 319 412.

La documentación relativa a los perfiles de la norma EN 319 412 puede solicitarse a CCPSD.

4.1.1. Número de versión

CCPSD emite certificados X.509 Versión 3.

4.1.2. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

4.2. Perfil de la lista de revocación de certificados

4.2.1. Número de versión

Las CRL emitidas por CCPSD son de la versión 2.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

4.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960.

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

5. Anexo I – Acrónimos

AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
RA	Autoridad de Registro
CP	Certificate Policy
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DCCF	Dispositivo Cualificado de Creación de Firma
QSCD	Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol

	GERENCIA SOLUCIONES DIGITALES		Código GSD-SD-001
	POLÍTICA DE CERTIFICACIÓN		Versión Documento 3.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	12 julio 2021	15 mayo 2024
OBJETIVO DE LAS POLITICAS:	Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza CCPSD.		

6. Control de Cambios y Aprobación

TABLA DE CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
01	12 julio 2021	Creación del documento
02	10 septiembre 2021	Corrección de la descripción de los perfiles de los certificados
03	9 mayo 2024	Actualización relación contractual con Uanataca directa y contactos internos.

TABLA DE CONTROL DE APROBACIONES			
DOCUMENTO QUE SE APRUEBA O ACTUALIZA:		GSD-SD-001 POLÍTICA DE CERTIFICACIÓN	
CÓDIGO DOCUMENTO QUE SE ACTUALIZA:	GSD-SD-001	NÚMERO DE LA VERSIÓN:	03
FUNCIÓN	PERSONA	CARGO	FECHA
CREADO	Alberto Borrás	(UANATACA)	12 julio 2021
REVISADO	Judit Guzmán	Sub-Gerente Desarrollo Empresarial & Soluciones Digitales	15 mayo 2024
APROBADO	Vanessa Mota	Gerente De Proyectos	15 mayo 2024
APROBADO	Antonio Ramos	Vicepresidente Ejecutivo	15 mayo 2024