TEXTO DE DIVULGACIÓN – PDS (PKI DISCLOSURE STATEMENT) PARA LOS CERTIFICADOS DE FIRMA ELECTRÓNICA Y AUTENTICACIÓN

INDIZE

Información general

Control documental

Clasificación de seguridad:	**Público**
Versión:	**1**
Fecha edición:	**11/11/2021**
Fichero:	**INDIZE_PDS - FIRMA_ES_v.1.docx**

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 11/11/2021	Nombre: María Moreno Fecha: 18/11/2021	Nombre: María Moreno Fecha: 18/11/2021

Control de versiones

Versión	Partes que cambian	Descripción cambio	Autor cambio	Fecha cambio
1.0	Original	Creación del documento	AGB	11/11/2021

Firmado digitalmente por 45712278P MARIA TRINIDAD MORENO (R: A18962399)
Nombre de reconocimiento (DN): 2.5.4.13=Reg:18020 /Hoja:GR-39663 / Tomo:1520 /Folio:186 /Fecha:29/12/2020 / Inscripción:6, serialNumber=IDCES-45712278P, givenName=MARIA TRINIDAD, sn=MORENO HIDALGO, cn=45712278P MARIA TRINIDAD MORENO (R: A18962399), 2.5.4.97=VATES-A18962399, o=INSTITUTO PARA LA DINAMIZACION ECONOMICA SOCIEDAD ANONIMA, c=ES
Fecha: 2021.11.20 12:48:25 +01'00'

Índice

1. TEXTO DIVULGATIVO APLICABLE A LOS CERTIFICADOS DE FIRMA ELECTRÓNICA Y AUTENTICACIÓN

Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación del Prestador de Servicios Electrónicos de Confianza INDIZE.

1.1. Información de contacto

1.1.1. Organización responsable

El Prestador de Servicios Electrónicos de Confianza INSTITUTO PARA LA DINAMIZACIÓN ECONÓMICA S.A., en lo sucesivo "INDIZE", es una iniciativa de:

INSTITUTO PARA LA DINAMIZACIÓN ECONÓMICA S.A. POLÍGONO INDUSTRIAL LA ERMITA EDIF. CEG. OF 25 18230. ATARFE. (GRANADA) 18230 GRANADA EMPRESA@INDIZE.ES

1.1.2. Contacto

Para cualquier consulta, diríjanse a:

INSTITUTO PARA LA DINAMIZACIÓN ECONÓMICA S.A. POLÍGONO INDUSTRIAL LA ERMITA EDIF. CEG. OF 25 18230. ATARFE. (GRANADA) 18230 GRANADA EMPRESA@INDIZE.ES

1.1.3. Prestador de Servicios Electrónicos de Confianza emisor

Los certificados descritos en este documento son emitidos por INDIZE, identificada mediante los datos indicados anteriormente.

1.1.4. Contacto para procesos de revocación

Para cualquier consulta, diríjanse a:

INSTITUTO PARA LA DINAMIZACIÓN ECONÓMICA S.A.
POLÍGONO INDUSTRIAL LA ERMITA EDIF. CEG. OF 25 18230. ATARFE. (GRANADA)
18230 GRANADA
EMPRESA@INDIZE.ES

1.2. Tipos de Certificados

Los siguientes certificados emitidos por INDIZE son cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2. INDIZE ha asignado a cada tipo de certificado un identificador de objeto (OID), para su identificación por las aplicaciones, las cuales de detallan a continuación:

Número OID	Tipo de certificados
	Persona Física
1.3.6.1.4.1.57967.1.1.1	*Certificado cualificado de Persona Física en HSM centralizado*
1.3.6.1.4.1.57967.1.1.2	Certificado cualificado de Persona Física en QSCD centralizado
	Representante de Persona Jurídica ante AAPP
1.3.6.1.4.1.57967.1.2.1	*Certificado cualificado de persona física Representante de Persona Jurídica ante las administraciones en HSM Centralizado*
1.3.6.1.4.1.57967.1.2.2	*Certificado cualificado de persona física Representante de Persona Jurídica ante las administraciones en QSCD centralizado*

	Representante Entidad sin Personalidad Jurídica ante AAPP
1.3.6.1.4.1.57967.1.3.1	*Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en HSM centralizado*
1.3.6.1.4.1.57967.1.3.2	*Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en QSCD centralizado*

1.3. Finalidad de los certificados

1.3.1. Estipulaciones comunes

Los certificados cualificados descritos en este documento y emitidos en HSM Centralizado, garantizan la identidad del suscriptor y de la persona indicada en el certificado, permitiendo la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

Los certificados cualificados descritos este documento y emitidos en QSCD Centralizado, funcionan con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, y dan 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 cualificados garantizan la identidad del firmante, permitiendo la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

1.3.2. Certificado cualificado de Persona Física en HSM centralizado

Este certificado dispone del OID 1.3.6.1.4.1.57967.1.1.1. 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. Los certificados de persona física emitidos en HSM Centralizado, son certificados

cualificados de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014.

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:

2. Autenticación en sistemas de control de acceso.
3. Firma de correo electrónico seguro.
4. 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:

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

1.3.3. Certificado cualificado de Persona Física en QSCD centralizado

Este certificado dispone del OID 1.3.6.1.4.1.57967.1.1.2. 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 emitido en QSCD centralizado, es un certificado cualificado de acuerdo con lo establecido en el artículo 28 del Reglamento (UE) 910/2014 eIDAS.

Funciona con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, y da 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"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, 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:

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

1.3.4. Certificado cualificado de persona física Representante de Persona Jurídica ante las administraciones en HSM Centralizado

Este certificado dispone del OID 1.3.6.1.4.1.57967.1.2.1. 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, lo cual se declara en el certificado.

Es un certificado cualificado de acuerdo con lo establecido en el artículo 28 del Reglamento (UE) 910/2014 eIDAS, y da 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 permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

Por otra parte, los certificados se pueden utilizar en otras 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.

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

1.3.5. Certificado cualificado de persona física Representante de Persona Jurídica ante las administraciones en QSCD centralizado

Este certificado dispone del OID 1.3.6.1.4.1.57967.1.2.2. 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, lo cual se declara en el certificado.

Este certificado emitido en QSCD centralizado, es un certificado cualificado de acuerdo con lo establecido en el artículo 28 del Reglamento (UE) 910/2014 eIDAS, y funciona con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, y da 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" es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

También se pueden 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:

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

1.3.6. Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en HSM centralizado

Este certificado dispone del OID 1.3.6.1.4.1.57967.1.3.1. 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.

Es un certificado cualificado, de acuerdo con lo establecido en el artículo 28 del Reglamento (UE) 910/2014 eIDAS, y da 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 descrita en el campo "O" (Organization), y permiten la generación de la "firma electrónica avanzada basada en certificado electrónico cualificado".

Por otra parte, el certificado se puede utilizar en otras 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.

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

1.3.7. Certificado cualificado de persona física Representante de Entidad sin Personalidad Jurídica ante las administraciones en QSCD centralizado

Este certificado dispone del OID 1.3.6.1.4.1.57967.1.3.2. 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, lo cual se declara en el certificado. Este certificado emitido en QSCD, es un certificado cualificado de acuerdo con lo establecido en los artículos 28 del Reglamento (UE) 910/2014 eIDAS.

El certificado emitido en QSCD centralizado, funciona con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, y da 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 descrita en el campo "O" (Organization), y permite la generación de la "firma electrónica cualificada" es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, 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:

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. Límites de uso del certificado

1.4.1. Límites de uso dirigidos a los firmantes

El firmante ha de utilizar el servicio de certificación de certificados prestado por INDIZE, exclusivamente para los usos autorizados en el contrato firmado entre INDIZEy el SUSCRIPTOR, y que se reproducen posteriormente (sección "obligaciones de los firmantes").

Asimismo, el firmante se obliga a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por INDIZE.

El firmante ha de cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.

El firmante no puede adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de INDIZE, sin previo permiso expreso.

1.4.2. Límites de uso dirigidos a los verificadores

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 normativa 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).

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, visibles en el web de INDIZE (https://indize.es).

El empleo de los certificados digitales en operaciones que contravienen este texto de divulgación, o los contratos con los suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a INDIZE, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

INDIZE 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, no es posible por parte de INDIZE 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 este texto de divulgación, o en los contratos con los suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la normativa aplicable.

1.5. Obligaciones de los suscriptores

1.5.1. Generación de claves

El suscriptor autoriza a INDIZE a gestionar de acuerdo con los métodos y procedimientos que correspondan, la emisión de las claves privada y pública para los firmantes, y solicita en su nombre la emisión del certificado de acuerdo a las políticas de certificación de INDIZE.

1.5.2. Solicitud de certificados

El suscriptor se obliga a realizar las solicitudes de certificados cualificados de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados por INDIZE, de conformidad con lo que se establece en la declaración de prácticas de certificación (DPC) y en la documentación de operaciones de INDIZE.

1.5.3. Obligaciones de información

El suscriptor se responsabiliza de que toda la información incluida en su solicitud del certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor tiene que informar inmediatamente a INDIZE:

- De cualquier inexactitud detectada en el certificado una vez se haya emitido.
- De los cambios que se produzcan en la información aportada y/o registrada para la emisión del certificado.
- De la pérdida, robo, sustracción, o cualquier otro tipo de pérdida de control de la clave privada por el firmante.

1.6. Obligaciones de los firmantes

1.6.1. Obligaciones de custodia

El firmante se obliga a custodiar el código de identificación personal o cualquier soporte técnico entregado por INDIZE, las claves privadas y, si fuese necesario, las especificaciones propiedad de INDIZE que le sean suministradas.

En caso de pérdida o robo de la clave privada del certificado, o en caso de que el firmante sospeche que la clave privada ha perdido fiabilidad por cualquier motivo, dichas circunstancias han de ser notificadas inmediatamente a la Autoridad de Registro de referencia o a INDIZE.

1.6.2. Obligaciones de uso correcto

El firmante tiene que utilizar el servicio de certificación de certificados de persona física emitido en DCCF (QSCD) prestado por INDIZE, exclusivamente para los usos autorizados en la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

El firmante tiene que cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas empleadas.

El firmante no podrá adoptar medidas de inspección, alteración o descompilación de los servicios de certificación digital prestados.

El firmante reconocerá:

a) Que cuando utilice cualquier certificado, y mientras el certificado no haya expirado ni haya sido suspendido o revocado, habrá aceptado dicho certificado y estará operativo.

b) Que no actúa como entidad de certificación y, por lo tanto, se obliga a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados con el propósito de firmar certificado alguno.

c) Que en caso de quedar comprometida la clave privada, debe cesar inmediata y permanentemente de su uso y proceder de acuerdo con este documento.

1.7. Obligaciones de los verificadores

1.7.1. Decisión informada

INDIZE informa al verificador que tiene acceso a información suficiente para tomar una decisión informada en el momento de verificar un certificado y confiar en la información contenida en dicho certificado.

Adicionalmente, el verificador reconocerá que el uso del Registro y de las Listas de Revocación de Certificados (en lo sucesivo, "las LRCs" o "las CRLs) de INDIZE , se rigen por la DPC de INDIZE y se comprometerá a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

1.7.2. Requisitos de verificación de la firma electrónica

La comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC, con los siguientes requisitos:

- Es necesario utilizar el software apropiado para la verificación de una firma electrónica con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa la firma electrónica a verificar, ya que la firma electrónica se verifica utilizando esta cadena de certificados.

- Es necesario asegurar que la cadena de certificados identificada es la más adecuada para la firma electrónica que se verifica, ya que una firma electrónica puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse el uso de la cadena más adecuada para verificarla.
- Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada al Registro de INDIZE (con LRCs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede considerarse correctamente verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.
- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado y el firmante, ya que existe la posibilidad de que alguno de los certificados incluya límites de uso que impidan confiar en la firma electrónica que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.
- Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado por el firmante.

1.7.3. Confianza en un certificado no verificado

Si el verificador confía en un certificado no verificado, asumirá todos los riesgos derivados de esta actuación.

1.7.4. Efecto de la verificación

En virtud de la correcta verificación de los certificados de persona física emitidos en DCCF (QSCD), de conformidad con este texto divulgativo, el verificador puede confiar en la identificación y, en su caso, clave pública del firmante, dentro de las limitaciones de uso correspondientes, para generar mensajes cifrados.

1.7.5. Uso correcto y actividades prohibidas

El verificador se obliga a no utilizar ningún tipo de información de estado de los certificados o de ningún otro tipo que haya sido suministrada por INDIZE, en la

realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de INDIZE, sin previo consentimiento escrito.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de certificación de INDIZE.

Los servicios de certificación digital prestados por INDIZE no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

1.7.6. Cláusula de indemnidad

El tercero que confía en el certificado se compromete a mantener indemne a INDIZE de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.
- Falta de comprobación de la totalidad de medidas de aseguramiento prescritas en la DCP o resto de normas de aplicación.

1.8. Obligaciones de INDIZE

1.8.1. En relación con la prestación del servicio de certificación digital

INDIZE se obliga a:

a) Emitir, entregar, administrar, suspender, reactivar, revocar y renovar certificados, de acuerdo con las instrucciones suministradas por el suscriptor y/o firmante, en los casos y por los motivos descritos en la DPC de INDIZE.
b) Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPC.
c) Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPC, en los aspectos técnicos, operativos y de seguridad.
d) Notificar al suscriptor y al firmante, con anterioridad a la fecha de expiración de los certificados, de la posibilidad de renovarlos, así como la suspensión, alzamiento de esta suspensión o revocación de los certificados, cuando se produzcan dichas circunstancias.
e) Comunicar a las terceras personas que lo soliciten, el estado de los certificados, de acuerdo con lo que se establece en la DPC para los diferentes servicios de verificación de certificados.

1.8.2. En relación a las comprobaciones del registro

INDIZE se obliga a la emisión de certificados en base a los datos suministrados por el suscriptor, por lo cual podrá realizar las comprobaciones que considere oportunas respecto de la identidad y otras informaciones personales y complementarias de los suscriptores y, cuando resulte procedente, de los firmantes.

Estas comprobaciones podrán incluir la justificación documental aportada, y cualquier otro documento e información relevantes facilitados por el suscriptor y/o el firmante.

En el caso de que INDIZE detecte errores en los datos que se deben incluir en los certificados o que justifican estos datos, podrá realizar los cambios que considere necesarios antes de emitir el certificado o suspender el proceso de emisión y gestionar con el suscriptor la incidencia correspondiente. En caso de que INDIZE

corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

INDIZE se reserva el derecho a no emitir el certificado, cuando considere que la justificación documental resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del firmante.

Las anteriores obligaciones quedarán en suspenso en los casos en que el suscriptor actúe como autoridad de registro y disponga de los elementos técnicos correspondientes a la generación de claves, emisión de certificados y grabación de dispositivos de firma corporativos.

1.8.3. Periodos de conservación

INDIZE archiva los registros correspondientes a las solicitudes de emisión y revocación de certificados durante al menos 15 años.

INDIZE almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada, de acuerdo a lo previsto en sus políticas y procedimientos.

1.9. Garantías limitadas y rechazo de garantías

1.9.1. Garantía de INDIZE por los servicios de certificación digital

INDIZE garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Autoridad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la DPC.
- Que los servicios de revocación y el empleo del depósito cumplen con todos los requisitos materiales establecidos en la DPC.

INDIZE garantiza al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el depósito, que el certificado ha sido emitido al suscriptor y firmante identificado en el mismo y que el certificado ha sido aceptado.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la DPC.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y depósito.

Adicionalmente, INDIZE garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado cualificado para firma contiene las informaciones que debe contener un certificado cualificado, de acuerdo con lo establecido en el artículo 28 del Reglamento (UE) 910/2014, dando cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Autoridad de Certificación, con los límites que se establezcan. En ningún caso INDIZE responderá por caso fortuito y en caso de fuerza mayor.

1.9.2. Exclusión de la garantía

INDIZE rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

Específicamente, INDIZE no garantiza software alguno utilizado por cualquier persona para firmar, verificar firmas, cifrar, descifrar, o utilizar de otra forma certificado digital alguno emitido por INDIZE, excepto en los casos en que exista una declaración escrita en sentido contrario.

1.10. Acuerdos aplicables y DPC

1.10.1. Acuerdos aplicables

Los acuerdos aplicables a los certificados son los siguientes:

- Contrato de servicios de certificación, que regula la relación entre INDIZE y el suscriptor de los certificados.
- Condiciones generales del servicio incorporadas en este documento.
- Declaración de Prácticas de Certificación, que regulan la emisión y utilización de los certificados.

1.10.2. Declaración de Prácticas de Certificación

Los servicios de confianza de INDIZE se regulan técnica y operativamente por la Declaración de Prácticas de Certificación (DPC) de INDIZE, por sus actualizaciones posteriores, así como por documentación complementaria.

La DPC y la documentación de operaciones se modifica periódicamente en el Registro y se puede consultar en la página de Internet: https://indize.es

1.11. Reglas de confianza para firmas longevas

INDIZE informa a los solicitantes de los certificados, que no ofrece un servicio que garantice la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

1.12. Política de intimidad

INDIZE no puede divulgar ni puede ser obligada a divulgar información confidencial alguna en lo referente a certificados sin una solicitud específica previa que provenga de:

a) La persona con respecto a la cual INDIZE tiene el deber de mantener la información confidencial, o
b) Una orden judicial, administrativa o cualquier otra prevista en la legislación vigente.

Sin embargo, el suscriptor acepta que determinada información, personal y de otro tipo, proporcionada en la solicitud de certificados, sea incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados, y que la información mencionada no tenga carácter confidencial, por imperativo legal.

INDIZE no cede a ninguna persona los datos entregados específicamente para la prestación del servicio de certificación.

1.13. Política de privacidad

INDIZE dispone de una política de privacidad en el apartado 9.4 de la DPC, y regulación específica de la privacidad en relación al proceso de registro, la confidencialidad del registro, la protección del acceso a la información personal, y el consentimiento del usuario.

Asimismo, se contempla que 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 15 años desde la expiración del certificado, incluso en caso de pérdida anticipada de vigencia por revocación.

1.14. Política de reintegro

INDIZE no reintegrará el coste del servicio de certificación en ningún caso.

1.15. Normativa aplicable y jurisdicción competente

Las relaciones con INDIZE se regirán por lo dispuesto Reglamento (UE) 910/2014 eIDAS, por las leyes españolas, y, en especial por todas aquellas que se desprendan de su política de cumplimiento.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

1.16. Vinculación con la lista de Prestadores Cualificados de Servicios Electrónicos de Confianza

http://www.minetur.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx

1.17. Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación

Las cláusulas del presente texto de divulgación son independientes entre sí, motivo por el cual, si cualquier cláusula es considerada inválida o inaplicable, el resto de cláusulas de las PDS seguirán siendo aplicables, excepto acuerdo expreso en contrario de las partes.

Los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad) de la DPC de INDIZE continuarán vigentes tras la terminación del servicio en los términos allí previstos.

Este texto contiene la voluntad completa y todos los acuerdos entre las partes.

Las partes se notifican hechos mutuamente mediante un procedimiento envío email a las siguientes direcciones:

- EMPRESA@INDIZE.ES, por parte de INDIZE
- La dirección electrónica, indicada por el suscriptor en el contrato con INDIZE.

Firmado digitalmente por 45712278P MARIA TRINIDAD MORENO (R: A18962399)
Nombre de reconocimiento (DN): 2.5.4.13=Reg:18020 /Hoja:GR-39663 / Tomo:1520 /Folio:186 /Fecha:29/12/2020 / Inscripción:6, serialNumber=IDCES-45712278P, givenName=MARIA TRINIDAD, sn=MORENO HIDALGO, cn=45712278P MARIA TRINIDAD MORENO (R: A18962399), 2.5.4.97=VATES-A18962399, o=INSTITUTO PARA LA DINAMIZACION ECONOMICA SOCIEDAD ANONIMA, c=ES
Fecha: 2021.11.20 12:49:07 +01'00'