Texto de divulgación - PDS (PKI Disclosure Statement) para el certificado de Empleado Público – nivel alto

Índice

ÍNDICE **2**

TEXTO DIVULGATIVO APLICABLE A LOS CERTIFICADOS DE PERSONA FÍSICA EMPLEADO PÚBLICO NIVEL ALTO **4**

1.1. INFORMACIÓN DE CONTACTO 4
1.1.1. Organización responsable *4*
1.1.2. Contacto *4*
1.1.3. Contacto para procesos de revocación *5*
1.2. TIPO Y FINALIDAD DEL CERTIFICADO DE PERSONA FÍSICA EMPLEADO PÚBLICO NIVEL ALTO 5
1.2.1. Entidad de Certificación emisora *7*
1.3. LÍMITES DE USO DEL CERTIFICADO 7
1.3.1. Límites de uso dirigidos a los firmantes *7*
1.3.2. Límites de uso dirigidos a los verificadores *8*
1.4. OBLIGACIONES DE LOS SUSCRIPTORES 9
1.4.1. Generación de claves *9*
1.4.2. Solicitud de certificados *9*
1.4.3. Obligaciones de información *9*
1.4.4. Obligaciones de custodia *10*
1.5. OBLIGACIONES DE LOS FIRMANTES 10
1.5.1. Obligaciones de custodia *10*
1.5.2. Obligaciones de uso correcto *11*
1.5.3. Transacciones prohibidas *11*
1.6. OBLIGACIONES DE LOS VERIFICADORES 12
1.6.1. Decisión informada *12*
1.6.2. Requisitos de verificación de la firma electrónica *12*
1.6.3. Confianza en un certificado no verificado *13*
1.6.4. Efecto de la verificación *14*
1.6.5. Uso correcto y actividades prohibidas *14*
1.6.6. Cláusula de indemnidad *14*
1.7. OBLIGACIONES DE UANATACA 15
1.7.1. En relación a la prestación del servicio de certificación digital *15*
1.7.2. En relación a las comprobaciones del registro *16*
1.7.3. Periodos de conservación *17*
1.8. GARANTÍAS LIMITADAS Y RECHAZO DE GARANTÍAS 17
1.8.1. Garantía de UANATACA por los servicios de certificación digital *17*
1.8.2. Exclusión de la garantía *19*
1.9. ACUERDOS APLICABLES Y DPC 19
1.9.1. Acuerdos aplicables *19*

1.9.2. DPC 20
1.10. REGLAS DE CONFIANZA PARA FIRMAS LONGEVAS 20
1.11. POLÍTICA DE INTIMIDAD 21
1.12. POLÍTICA DE PRIVACIDAD 21
1.13. POLÍTICA DE REINTEGRO 22
1.14. NORMATIVA APLICABLE Y JURISDICCIÓN COMPETENTE 22
1.15. ACREDITACIONES Y SELLOS DE CALIDAD 22
1.16. VINCULACIÓN CON LA LISTA DE PRESTADORES 22
1.17. DIVISIBILIDAD DE LAS CLÁUSULAS, SUPERVIVENCIA, ACUERDO ÍNTEGRO Y NOTIFICACIÓN 23

TEXTO DIVULGATIVO APLICABLE A LOS CERTIFICADOS DE PERSONA FÍSICA EMPLEADO PÚBLICO NIVEL ALTO

Este documento contiene las informaciones esenciales a conocer en relación con el servicio de certificación de la Entidad de Certificación UANATACA.

1.1. Información de contacto

1.1.1. Organización responsable

La Entidad de Certificación UANATACA, en lo sucesivo "UANATACA", es una iniciativa de:

UANATACA, S.A.
CALLE RIERA DE CAN TODÀ, 24-26, 6º, 1ª
08024 BARCELONA
TELÉFONO: 935 272 290
EMAIL: INFO@UANATACA.COM

1.1.2. Contacto

Para cualquier consulta, diríjanse a:

UANATACA, S.A.
EMAIL: INFO@UANATACA.COM
TELÉFONO: 935 272 290

1.1.3. Contacto para procesos de revocación

Para cualquier consulta, diríjanse a:

UANATACA, S.A. EMAIL: INFO@UANATACA.COM TELÉFONO: 935 272 290

1.2. Tipo y finalidad del certificado de persona física empleado público nivel alto

Este certificado dispone del OID 1.3.6.1.4.1.47286.1.4.2.1 para la identificación, del OID 1.3.6.1.4.1.47286.1.4.2.2 para la firma y del OID 1.3.6.1.4.1.47286.1.4.2.3 para el cifrado.

Este certificado cualificado para firma con OID 1.3.6.1.4.1.47286.1.4.2.2, se emite 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.

El certificado para firma de persona física empleado público nivel alto, es un certificado cualificado de acuerdo con lo establecido en los artículos 24 y 28 del Reglamento (UE) 910/2014, todo ello en concordancia con el artículo 11.1, con el contenido prescrito por el artículo 11.2, y dando cumplimiento a las obligaciones previstas para su emisión, contenidas en los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Este certificado cualificado para firma se emite a empleados públicos para identificarlos como personas al servicio de la Administración Pública, vinculándolos con ésta, cumpliendo los requisitos establecidos en el artículo 43 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para la firma electrónica del personal al servicio de las Administraciones Públicas.

El certificado para firma de persona física empleado público nivel alto, funciona con dispositivos cualificados de creación de firma, de acuerdo con los artículos 29 y 51 del Reglamento (UE) 910/2014, en concordancia con con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Asimismo, los certificados de persona física empleado público nivel alto se emiten de acuerdo con los niveles de aseguramiento medio de los perfiles de certificados establecidos en el punto 10 del documento "Perfiles de Certificados electrónicos" de la Subdirección General de Información, Documentación y Publicaciones del Ministerio de Hacienda y Administraciones Públicas.

Este certificado cualificado para firma garantiza la identidad del suscriptor y del firmante, 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 de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 eIDAS, y el artículo 3 de la Ley 59/2003, de 19 de diciembre, 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 digital.

Estos certificados permiten el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

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

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    a. En el perfil de autenticación:
        i. Firma digital (Digital Signature, para realizar la función de autenticación)

b. En el perfil de firma:
    i. Compromiso con el contenido (Content commintment, para realizar la función de firma electrónica)
c. En el perfil de cifrado:
    i. Key Encipherment
    ii. Data Encipherment

1.2.1. Entidad de Certificación emisora

Los certificados de persona física empleado público nivel alto son emitidos por UANATACA, identificada mediante los datos indicados anteriormente.

1.3. Límites de uso del certificado

1.3.1. Límites de uso dirigidos a los firmantes

El firmante ha de utilizar el servicio de certificación de certificados de persona física empleado público nivel alto prestado por UANATACA exclusivamente para los usos autorizados en el contrato firmado entre UANATACA y 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 UANATACA.

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 UANATACA, sin previo permiso expreso.

1.3.2. 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 peticiones de emisión, renovación, suspensión o revocación de certificados, ni 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 UANATACA (https://www.uanataca.com).

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 UANATACA, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.
UANATACA 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 UANATACA 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 legislación vigente.

1.4. Obligaciones de los suscriptores

1.4.1. Generación de claves

El suscriptor autoriza a UANATACA a generar las claves, privada y pública, para la identificación y la firma electrónica de los firmantes, y solicita en su nombre la emisión del certificado de persona física empleado público nivel alto.

1.4.2. Solicitud de certificados

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

1.4.3. 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 UANATACA:

- 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.

1.4.4. Obligaciones de custodia

El suscriptor se obliga a custodiar toda la información que genere en su actividad como entidad de registro.

1.5. Obligaciones de los firmantes

1.5.1. Obligaciones de custodia

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

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 UANATACA por medio del suscriptor.

1.5.2. Obligaciones de uso correcto

El firmante tiene que utilizar el servicio de certificación de certificados de persona física empleado público nivel alto prestado por UANATACA, 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 haya sido 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, su uso queda inmediata y permanentemente suspendido.

1.5.3. Transacciones prohibidas

El firmante se obliga a no utilizar sus claves privadas, los certificados o cualquier otro soporte técnico entregado por UANATACA en la realización de transacción alguna prohibida por la ley aplicable.

Los servicios de certificación digital prestados por UANATACA no han sido diseñados ni permiten su 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, en las que un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

1.6. Obligaciones de los verificadores

1.6.1. Decisión informada

UANATACA 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 UANATACA, se rigen por la DPC de UANATACA y se comprometerá a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

1.6.2. 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 digital 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 UANATACA (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.

1.6.3. Confianza en un certificado no verificado

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

1.6.4. Efecto de la verificación

En virtud de la correcta verificación de los certificados de persona física empleado público nivel alto, 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.

1.6.5. 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 UANATACA, 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 UANATACA, sin previo consentimiento escrito.

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

Los servicios de certificación digital prestados por UANATACA 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.

1.6.6. Cláusula de indemnidad

El tercero que confía en el certificado se compromete a mantener indemne a UANATACA 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.

El certificado indicado permite el cifrado de documentos, contenidos y mensajes de datos, bajo la exclusiva responsabilidad del firmante, dado que UANATACA no ofrece servicios de copia de seguridad ni recuperación de claves. Por ello, UANATACA no responderá en ningún caso por pérdida alguna de información cifrada que no se pueda recuperar.

1.7. Obligaciones de UANATACA

1.7.1. En relación a la prestación del servicio de certificación digital

UANATACA se obliga a:

a) Emitir, entregar, administrar, suspender, revocar y renovar certificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPC de UANATACA.

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, de acuerdo con las indicaciones del artículo 10.2 de la Ley de Firma Electrónica.

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.

1.7.2. En relación a las comprobaciones del registro

UANATACA 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 por el firmante por medio del suscriptor, si UANATACA lo considera necesario, y cualquier otro documento e información relevantes facilitados por el suscriptor y/o el firmante.

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

UANATACA 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.

1.7.3. Periodos de conservación

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

UANATACA almacena la información de los logs durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

1.8. Garantías limitadas y rechazo de garantías

1.8.1. Garantía de UANATACA por los servicios de certificación digital

UANATACA garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad 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.

UANATACA 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, UANATACA 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, en concordancia con artículo 11 de la Ley 59/2003, de 19 de diciembre y 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 Entidad de Certificación, con los límites que se establezcan. En ningún caso UANATACA responderá por caso fortuito y en caso de fuerza mayor.

1.8.2. Exclusión de la garantía

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

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

1.9. Acuerdos aplicables y DPC

1.9.1. Acuerdos aplicables

Los acuerdos aplicables al certificado de persona física empleado público nivel alto son los siguientes:

- Contrato de servicios de certificación, que regula la relación entre UANATACA y la empresa suscriptora de los certificados.

- Condiciones generales del servicio incorporadas en el texto de divulgación del certificado o PDS.

- DPC, que regulan la emisión y utilización de los certificados.

1.9.2. DPC

Los servicios de certificación de UANATACA se regulan técnicamente y operativamente por la DPC de UANATACA, 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://www.uanataca.com.

1.10. Reglas de confianza para firmas longevas

El punto b.2 del artículo 18 de la Ley 59/2003, de 19 de diciembre, de firma electrónica hace referencia a la obligación de las entidades de certificación de informar a los solicitantes de los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

UANATACA informa a los solicitantes de los certificados de persona física empleado público nivel alto que no ofrece un servicio que garantice la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

UANATACA recomienda, para la fiabilidad de la firma electrónica de un documento a lo largo del tiempo, el uso de los estándares indicados en el apartado 7.3 (reglas de confianza para firmas longevas) de la Guía de Aplicación de la Norma Técnica de Interoperabilidad "Política de Firma Electrónica y de certificados de la Administración".

Las consideraciones generales para las reglas de confianza de firmas longevas se recogen en el subapartado IV.3 de la NTI de firma electrónica.

1.11. Política de intimidad

UANATACA 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 UANATACA 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.

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

1.12. Política de privacidad

UANATACA 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 todo en caso de pérdida anticipada de vigencia por revocación.

1.13. Política de reintegro

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

1.14. Normativa aplicable y jurisdicción competente

Las relaciones con UANATACA se regirán por lo dispuesto Reglamento (UE) 910/2014, por las leyes españolas, y, en concreto para la Ley 59/2003, de 19 de diciembre, de firma electrónica, así como por la legislación civil y mercantil aplicable.

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

1.15. Acreditaciones y sellos de calidad

Sin estipulación.

1.16. Vinculación con la lista de prestadores

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 UANATACA continuarán vigentes tras la terminación del servicio.

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:

- info@uanataca.com, por parte de UANATACA
- La dirección electrónica, indicada por el suscriptor en el contrato con UANATACA.