DECLARACIÓN DE PRÁCTICAS DE REGISTRO

Información general

Control documental

Clasificación de seguridad:	Público
Entidad de destino:	**Sotronic Innovation Technology S.L.**
Versión:	1.0
Fecha edición:	09/09/2020

Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: Alejandro Grande Fecha: 09/09/2020	Nombre: Iria Costas Fecha: 6/10/2020	Nombre: Iria Costas Fecha: 01/02/2021

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	Alejandro Grande	09/09/2020

ÍNDICE

INFORMACIÓN GENERAL **2**

CONTROL DOCUMENTAL 2
ESTADO FORMAL 2
CONTROL DE VERSIONES 3

ÍNDICE **4**

1. INTRODUCCIÓN **7**

2. PARTICIPANTES **8**

2.1. AUTORIDAD DE CERTIFICACIÓN (CA) 8
2.2. AUTORIDAD DE REGISTRO (RA) 8
2.3. PRESTADOR DE SERVICIOS DE CERTIFICACIÓN (PSC) 9
2.4. ENTIDADES FINALES 9
2.4.1. Suscriptores del servicio de certificación 9
2.4.2. Firmantes 10
2.4.3. Partes usuarias o terceros que confían 11
2.5. TERCEROS VINCULADOS 11

3. USO APROPIADO DEL CERTIFICADO **12**

4. ADMINISTRACIÓN DE LA POLÍTICA **13**

4.1. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN 13
4.2. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE DPR 13
4.3. PROCEDIMIENTO DE GESTIÓN DE DPR 13
4.4. DATOS DE CONTACTO LA ORGANIZACIÓN 13

5. PUBLICACIÓN Y REGISTRO **14**

5.1. PUBLICACIÓN DE LA INFORMACIÓN SOBRE CERTIFICACIÓN 14
5.2. TIEMPO O FRECUENCIA DE LA PUBLICACIÓN 14
5.3. CONTROLES DE ACCESO A LOS REGISTROS 14

6. IDENTIFICACIÓN Y AUTENTICACIÓN **15**

6.1. RECONOCIMIENTO, AUTENTICACIÓN Y ROL DE LAS MARCAS REGISTRADAS 15
6.2. VALIDACIÓN INICIAL DE LA IDENTIDAD 16
6.2.1. Método para probar el control exclusivo de la clave privada 16
6.2.2. Autenticación de la identidad de una persona jurídica 16
6.2.3. Autenticación de la identidad de persona natural 18
6.2.4. Información no verificada del suscriptor 18

6.2.5. Validación de la autoridad.....19
6.3. IDENTIFICACIÓN Y AUTENTICACIÓN PARA SOLICITUDES DE RENOVACIÓN DE CERTIFICADO.....19
6.3.1. Identificación y Autenticación para solicitudes de renovación de certificados rutinaria.....19
6.3.2. Identificación y Autenticación para la renovación de certificado luego de la revocación.....20
6.4. IDENTIFICACIÓN Y AUTENTICACIÓN PARA LA SOLICITUD DE REVOCACIÓN.....20
7. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS.....21
7.1. SOLICITUD DEL CERTIFICADO.....21
7.1.1. Habilitados para presentar la solicitud de un certificado.....21
7.1.2. Proceso de solicitud y responsabilidades.....22
7.2. PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO.....22
7.2.1. Realización de las funciones de identificación y autenticación.....22
7.2.2. Aprobación o rechazo de la solicitud de certificado.....23
7.2.3. Tiempo para el procesamiento de la solicitud de un certificado.....23
7.3. RENOVACIÓN DE CERTIFICADO.....23
7.3.1. Circunstancias para la renovación de un certificado.....23
7.3.2. Personas habilitadas para solicitar la reemisión de certificado.....24
7.3.3. Procesamiento de las solicitudes para renovación de certificados.....24
7.4. REVOCACIÓN Y SUSPENSIÓN DEL CERTIFICADO.....25
7.4.1. Circunstancias para la revocación.....25
7.4.2. Personas habilitadas para solicitar la revocación.....25
7.4.3. Procedimiento para la solicitud de revocación.....26
***7.4.4. Causas de suspensión de un certificado*.....26**
7.4.5. Personas habilitadas para solicitar la revocación, suspensión o reactivación.....27
***7.4.6. Procedimientos de solicitud de revocación, suspensión o reactivación*.....27**
7.5. MODIFICACIÓN DE CERTIFICADOS.....27
8. GESTIÓN DE LA SEGURIDAD Y DE LAS OPERACIONES.....28
8.1. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES.....28
8.2. CONTROLES DE SEGURIDAD TÉCNICA.....28
9. OTRAS MATERIAS DE NEGOCIO Y LEGALES.....30
9.1. TARIFAS Y REEMBOLSO.....30
9.2. CONFIDENCIALIDAD DE LA INFORMACIÓN DEL NEGOCIO.....30
9.2.1. Alcances de la información confidencial.....30
9.2.2. Responsabilidad de protección de la información confidencial.....30
9.2.3. Información tratada como privada.....31
9.2.4. Información no considerada privada.....31
9.2.5. Notificación y consentimiento para el uso de información.....31

9.2.6. Divulgación realizada con motivo de un proceso judicial o administrativo.....32
9.2.7. Otras circunstancias para divulgación de información.....32
9.3. DERECHO DE PROPIEDAD INTELECTUAL.....32
9.4. REPRESENTACIONES Y GARANTÍAS.....32
9.5. EXENCIÓN DE GARANTÍAS.....33
9.6. LIMITACIÓN DE RESPONSABILIDAD.....33
9.7. CLÁUSULAS DE DIVISIBILIDAD, SUPERVIVENCIA, ACUERDO ÍNTEGRO, NOTIFICACIÓN Y FUERZA MAYOR.....33
9.8. PROVISIONES SOBRE RESOLUCIÓN DE DISPUTAS.....34
9.9. LEY APLICABLE.....34

1. Introducción

Sotronic Innovation Technology S.L., en adelante SOTRONIC, es una entidad registrada en ESPAÑA y que Presta Servicios de Certificación, mediante la explotación de infraestructura de clave pública (PKI) de Uanataca, S.A., quien actúa como Autoridad de Certificación.

2. PARTICIPANTES

Son considerados como participantes, para efectos del presente documento, la Autoridad de Certificación (CA), la Autoridad de registro (RA), los titulares y/o suscriptores, los terceros de confianza y otros terceros vinculados que realizan funciones de registro.

2.1. Autoridad de Certificación (CA)

La CA es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación electrónica, proveyendo la infraestructura de clave pública (PKI) para la prestación de servicios de certificación electrónica.

SOTRONIC ha suscrito un contrato de prestación de servicios de tecnología con Uanataca, S.A., (en lo sucesivo UANATACA) quien se configura como CA proporcionando la infraestructura de clave pública (PKI) y servicios de certificación electrónica. Asimismo, la CA establece la Declaración de Prácticas de Certificación (DPC) y Políticas de Certificación (PC), disponibles en https://www.uanataca.com/public/cps_nc/.

2.2. Autoridad de Registro (RA)

La RA es la persona jurídica, encargada del levantamiento de datos, comprobación de éstos respecto a un solicitante de un mecanismo de firma electrónica o certificación electrónica, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados electrónicos, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados electrónicos. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la norma vigente.

2.3. Prestador de Servicios de Certificación (PSC)

El prestador de servicios electrónicos de certificación es la persona, física o jurídica, que expide y gestiona certificados para entidades finales, empleando una Autoridad de Certificación y actuando como Autoridad de Registro.

SOTRONIC a través de la Autoridad de Certificación Uanataca, S.A., presta servicios electrónicos de certificación como Prestador de Servicios de Certificación, llevando a cabo las tareas propias de una Autoridad de Registro, expidiendo y gestionando el ciclo de vida de los certificados electrónicos.

2.4. Entidades finales

Las entidades finales son las personas u organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados electrónicos.

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

1. Suscriptores del servicio de certificación
2. Firmantes
3. Partes usuarias o terceros que confían

2.4.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- Las empresas, entidades, corporaciones u organizaciones que adquieren certificados electrónicos de distribuidos por SOTRONIC (directamente o a través de un tercero autorizado) para su uso en su ámbito 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.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio – certificados de sello electrónico –, o al objeto de facilitar la

certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor – certificados de firma electrónica. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio electrónico de certificación es, por tanto, el cliente del Prestador de Servicios de Certificación, de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en el contrato de prestación de servicios y/o en los términos y condiciones del servicio según corresponda.

2.4.2. Firmantes

Los firmantes son las personas físicas que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma electrónica.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, 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 certificación, 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 a los derechos y obligaciones del firmante.

2.4.3. Partes usuarias o terceros que confían

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

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en este documento y en la Declaración de Prácticas de Certificación de la Autoridad de Certificación.

2.5. Terceros vinculados

Los terceros vinculados son personas naturales o jurídicas que realizan funciones de registro, tales como solicitudes de emisión, revocación, renovación, etc. En concreto serán los encargados 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.
- Si fuera necesario, gestionar la generación de claves y la emisión del certificado.
- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar temporalmente de manera segura la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.
- Enviar de manera segura la documentación relativa al ciclo de vida de los certificados a las oficinas de la ER para su debida custodia y archivo.

Podrán actuar como terceros vinculados de SOTRONIC, cualquier entidad debidamente autorizada mediante la formalización de un contrato o documento análogo en el que se regularán las relaciones entre cada una de las partes.

Los terceros vinculados quedan sujetos al presente documento, en concreto a los mismos requisitos de seguridad y procedimientos propios de una RA.

3. USO APROPIADO DEL CERTIFICADO

Los criterios para definir el uso apropiado, rango de acción o aplicabilidad de un certificado electrónico solicitado a SOTRONIC en calidad de Prestador de Servicios de Certificación, dependerán de lo establecido en la Política de Certificación y Declaración de Prácticas de Certificación de la Autoridad de Certificación UANATACA.

Las mismas se encuentran a disposición de cualquier interesado en la siguiente página web: https://www.uanataca.com/public/cps_nc/

4. ADMINISTRACIÓN DE LA POLÍTICA

4.1. Nombre del documento e identificación

Este documento es la Declaración de Prácticas de Registro (DPR) de SOTRONIC.

4.2. Organización que administra los documentos de DPR

La persona responsable de la administración de los servicios de certificación electrónica es ubicable mediante la siguiente información de contacto:

Nombre: Sotronic Innovation Technology S.L
Dirección: Avda.Aeropuerto Nº 7, 36206 VIGO (Pontevedra)
Correo electrónico: info@df-server.com
Página web: https://www.df-server.com/

4.3. Procedimiento de gestión de DPR

El sistema documental y de organización de SOTRONIC garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

4.4. Datos de contacto la organización

Nombre: Sotronic Innovation Technology S.L
Dirección: Avda.Aeropuerto Nº 7, 36206 VIGO (Pontevedra)
Correo electrónico: info@df-server.com
Página web: https://www.df-server.com/

5. PUBLICACIÓN Y REGISTRO

5.1. Publicación de la información sobre certificación

La Declaración de Prácticas de Registro, así como toda la documentación pertinente y vigente de SOTRONIC; y en general relativa a la Prestación de Servicios de Certificación, son publicadas en la siguiente dirección web:
https://www.uanataca.com/public/pki/dpr-sotronic-es/

La Declaración de Prácticas de Certificación y Políticas de Certificación con respecto de los certificados electrónicos expedidos por SOTRONIC, se encuentran publicadas en la web de UANATACA, como Autoridad de Certificación, en la siguiente dirección: https://www.uanataca.com/public/cps_nc/.

5.2. Tiempo o frecuencia de la publicación

Las modificaciones relativas a la DPR u otra documentación de SOTRONIC, se publicarán tan pronto como razonablemente sea posible, debiendo tener cuidado de cumplir con los requisitos que fueren necesarios para la aprobación de dichas modificaciones.

5.3. Controles de acceso a los registros

El acceso a los registros es restringido únicamente para el uso de los titulares y suscriptores legítimos, así como a los trabajadores del Prestador de Servicios de Certificación y/o la CA, teniendo en cuenta los temas de privacidad que pudieran existir en los contratos de los suscriptores o titulares de conformidad con la normativa correspondiente.

El PSC emplea sistemas fiables para el registro, de modo tal que:

- Únicamente personas autorizadas tengan acceso a lectura y modificaciones.
- Pueda comprobarse la autenticidad de la información.

6. IDENTIFICACIÓN Y AUTENTICACIÓN

En la Prestación de Servicios de Certificación se emplean procedimientos seguros para garantizar el control exclusivo de la clave privada, conformes con los estándares y mejores prácticas internacionales de seguridad. En este sentido, se implementan procedimientos para la autenticación de la identidad de personas físicas y jurídicas, en la solicitud de emisión y renovación de certificados, estableciendo procedimientos análogos que les permita la suspensión y revocación de estos.

SOTRONIC declara verificar documental y/o telemáticamente todos los datos que incluye en los certificados emitidos. En este sentido, desarrolla la presente Declaración de Prácticas de Registro estableciendo los procedimientos de identificación y verificación mencionados en el párrafo precedente.

6.1. Reconocimiento, autenticación y rol de las marcas registradas

Se prohíbe a los solicitantes de certificados de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros.

En el caso de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

No le corresponde al PSC determinar si un solicitante de certificados le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales. Sin embargo, el PSC debe cerciorarse mediante la validación de la documentación, registros y en general cualquier tipo de información indicada por el solicitante del certificado que tanto el nombre del titular como del suscriptor correspondan a los solicitantes.

El PSC tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombres.

6.2. Validación inicial de la identidad

6.2.1. Método para probar el control exclusivo de la clave privada

El procedimiento y/o método para demostrar el control exclusivo sobre la clave privada se define en la DPC y PC de UANATACA, por el cual se establecen los procedimientos fiables de emisión, entrega y aceptación del correspondiente certificado y del par de claves, así como según corresponda del dispositivo seguro de creación de firma o de las credenciales para hacer uso de los certificados.

6.2.2. Autenticación de la identidad de una persona jurídica

El proceso de comprobación de la identidad de la persona jurídica cuyos datos se incluyen en un certificado, tiene como objetivo garantizar que el suscriptor y el titular sean las mismas personas identificadas en la solicitud de emisión de un certificado, y que la información que se incluya en el certificado sea verdadera y exacta.

Para ello, el PSC requiere al solicitante del certificado la presentación y/o justificación de la documentación correspondiente que justifique la información a incluirse en el certificado electrónico. Asimismo, se debe proceder a la identificación del firmante mediante métodos que aporten seguridad y fiabilidad a la misma, siguiendo los procedimientos descritos en este documento.

El personal asignado por el PSC, deberá validar la identidad del solicitante, para ello debe establecer los procedimientos de validación considerando los requerimientos de la normativa aplicable:

- El Representante Legal o una persona asignada por él deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, así como sus facultades como representante. Para ello, es preciso presentar un documento público o escritura que acredite dicha representación. Este requisito de presentación de documento público podrá ser omitido en caso de que el PSC pueda realizar consultas telemáticas para comprobar la vigencia de la representación que alega tener el solicitante.
- La existencia y vigencia de la persona jurídica deberá acreditarse con el documento de vigencia respectivo expedido por los Registros Públicos o

mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

La exigencia de presentar la documentación a que hace referencia el párrafo anterior, podrá ser omitida en caso de que el PSC pueda realizar consulta telemática a través de las que pueda verificar la información relativa a la existencia de la persona jurídica.

- El Representante Legal de la persona jurídica o una persona asignada por él, deberá firmar un contrato, que en adelante llamaremos "contrato del titular". A través de dicho contrato, el titular deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.
- Si fuera el caso, los responsables de realizar las solicitudes de certificados, en representación de la persona jurídica, deben enviar las solicitudes a través de medios no repudiables.
- En general cualquier documento que se requiera aportar para acreditar requisitos para la emisión de certificados, podrá ser cumplido mediante la consulta telemática a registros públicos y/o privados por parte del PSC.
- La identidad de la persona titular del certificado electrónico ya sea como representante legal o como responsable del certificado, deberá acreditar su identidad mediante la metodología descrita a continuación:
    - SOTRONIC realizará la identificación de la persona titular del certificado electrónico atendiendo a los procedimientos y controles de registro de clientes, en los que se solicitará al cliente y titular del certificado que cumplimente un formulario aportando sus datos personales, tales como nombre, apellidos, correo electrónico y teléfono móvil, así como copia de su documento de identidad, siendo revisados y validados por el personal asignado por el PSC.

El firmante quedará identificado si se considera que los datos proporcionados corresponden al firmante, finalizando en este momento la identificación. También se considerará identificado, cuando existan registros previos en base a relaciones anteriores, por el que ya conste en el PSC los datos de identidad de este.

6.2.3. Autenticación de la identidad de persona natural

El proceso de comprobación de la identidad de la persona natural cuyos datos se incluyen en un certificado electrónico tiene como objetivo garantizar que el titular sea la misma persona identificada en la solicitud de emisión de un certificado, y que la información que se incluya en el certificado sea verdadera y exacta. Para ello, el PSC procederá de la siguiente manera:

- SOTRONIC realizará la identificación de la persona titular del certificado electrónico atendiendo a los procedimientos y controles de registro de clientes, en los que se solicitará al cliente y titular del certificado que cumplimente un formulario aportando sus datos personales, tales como nombre, apellidos, correo electrónico y teléfono móvil, así como copia de su documento de identidad, siendo revisados y validados por el personal asignado por el PSC.

El personal asignado por el PSC, deberá validar la identidad del solicitante, para ello la Autoridad de Registro establece procedimientos de validación de los soportes de acuerdo con la normativa aplicable.

- Se verifica la identidad del solicitante mediante la verificación de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro.
- La información proporcionada por los solicitantes es validada por la RA a través de un mecanismo de consulta confiable, como es el caso de las bases de datos nacionales o registros públicos.
- Se validan y comprueban los datos aportados por el formulario de registro de clientes, verificándolo contra el documento de identidad aportado asegurando la identificación del titular del certificado.

6.2.4. Información no verificada del suscriptor

De manera general, no se incluye en los certificados, información no verificada del suscriptor o el titular según sea el caso.

Como excepción a lo anterior, no se comprueba la dirección de correo electrónico y el número de teléfono indicado por el suscriptor. En este caso se debe comprobar que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente

desea incluir el solicitante. El PSC no está obligado a comprobar ni la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, todo lo cual es responsabilidad del solicitante.

6.2.5. Validación de la autoridad

Cuando un individuo solicita la emisión de un certificado que sirva para acreditar el ejercicio de un cargo en concreto, se requiere a este solicitante las pruebas que evidencien su cargo, incluyendo la facultad de actuar en nombre de la persona jurídica en la que ocupa dicho cargo. El requerimiento de este documento puede ser cumplido mediante consulta telemática al registro público o privado donde se encuentre la información que acredita el carácter del solicitante.

6.3. Identificación y autenticación para solicitudes de renovación de certificado

SOTRONIC informa a sus suscriptores la posibilidad de renovación de los certificados.

6.3.1. Identificación y Autenticación para solicitudes de renovación de certificados rutinaria

La renovación rutinaria puede producirse cuando el certificado sigue vigente y no han cambiado los datos contenidos en él. Sólo los titulares y suscriptores de certificados pueden solicitar la renovación de certificados, tanto en el caso de personas naturales como personas jurídicas.

Los medios de verificación de la identidad del solicitante para la renovación del certificado son los siguientes:

- 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 natural identificada en el certificado, y que le permite renovar de forma automática sin tener que identificarse de nuevo ante la Autoridad de Registro su certificado, en el marco de la legislación aplicable.
- A través del empleo del certificado vigente para solicitar su renovación.

Antes de aprobar la renovación el certificado con la nueva clave pública, la RA comprueba que la información del titular y del suscriptor contenida en el certificado continúa siendo válida, para lo cual podrá valerse documentación acreditativa que aporte el solicitante o bien de consultas telemáticas a bases de datos públicas o privadas que contengan la información correspondiente. Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información.

En los casos que el certificado del titular hubiera expirado o hubiera sido revocado, deberá seguirse el proceso para la emisión de un nuevo certificado y la validación de identificación inicial descrita en este documento.

6.3.2. Identificación y Autenticación para la renovación de certificado luego de la revocación

En el caso que el certificado del titular haya sido revocado, deberá seguirse el proceso de validación de identidad inicial, especificado en de este documento.

6.4. Identificación y autenticación para la solicitud de revocación

El suscriptor y el titular puede tramitar y/o solicitar la revocación de su certificado a través de medios telemáticos, utilizando un mecanismo que garantice el no repudio, como un mensaje firmado con un certificado válido, código de revocación, la autenticación a través de una frase secreta conocida sólo por el suscriptor del certificado entre otro. También podrá solicitarlo acreditando su identidad ante la Autoridad de Registro.

7. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

El ciclo de vida de los certificados electrónicos lo determina la Autoridad de Certificación de acuerdo con sus Políticas de Certificación y su Declaración de Prácticas de Certificación. No obstante, SOTRONIC como Prestador de Servicios de Certificación gestiona la emisión de certificados, así como su ciclo de vida desempeñado las funciones propias de una Autoridad de Registro.

7.1. Solicitud del certificado

7.1.1. Habilitados para presentar la solicitud de un certificado

La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado o por un representante que cuente con facultades expresas para tales efectos otorgadas mediante poder o documento análogo. En este caso, el titular del certificado será el poderdante y corresponderá al apoderado la condición de suscriptor. El ámbito de utilización del certificado digital en este supuesto, se encontrará circunscrito y limitado a las facultades expresamente conferidas en el poder.

En el caso de personas jurídicas, se pueden solicitar certificados de atributo para ser usados por personal específico de la entidad, incluso por el Representante legal. En este caso, se considera como aspirante a titular del certificado a la persona jurídica y dichas personas naturales vienen a ser los aspirantes a suscriptor. El solicitante deberá especificar en su solicitud el tipo de atributo al que corresponderá el certificado.

El Prestador de Servicios de Certificación gestionará la emisión de un perfil que se corresponda con los atributos de un representante legal de la persona jurídica, en forma diferenciada de un perfil de certificado identifique a trabajadores, agentes o personas vinculadas que como parte de su cargo requieren de un certificado electrónico, lo cual se advertirá al solicitante.

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por un representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas electrónicas generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Un suscriptor puede efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera.

7.1.2. Proceso de solicitud y responsabilidades

El proceso de solicitud y las responsabilidades asumidas por el uso del certificado dependerán de lo establecido en las Políticas de Certificación y su Declaración de Prácticas de Certificación de UANATACA, así como lo descrito en el presente documento y/o términos y condiciones del servicio.

7.2. Procesamiento de la solicitud de un certificado

7.2.1. Realización de las funciones de identificación y autenticación

SOTRONIC utiliza los siguientes procedimientos de verificación para la validación de la identidad de una persona jurídica o natural:

a. Se requiere una identificación del solicitante del certificado para la verificación de su identidad, siguiendo los medios identificados en el presente documento.
b. Se establece la persona responsable de la verificación.
c. Se determinan los documentos requeridos para identificar a una persona según la siguiente clasificación:
    1. Natural
    2. Jurídica
d. Se establecen procedimientos para la validación de la documentación presentada por el solicitante del certificado para cada uno de los casos.

7.2.2. Aprobación o rechazo de la solicitud de certificado

Las solicitudes serán rechazadas si el resultado de la validación realizada por la Autoridad de Registro fuese negativo, conforme a lo establecido en este documento.

En caso de que la solicitud sea aprobada, se procederá a:

- Comunicar a la CA su aprobación para la emisión del certificado a través de los canales seguros de comunicación para la generación del certificado.
- La RA emitirá el contrato del servicio que el suscriptor (o su representante) deberá firmar, el cual contendrá las obligaciones que garanticen el efecto legal de las transacciones realizadas con el certificado y las responsabilidades de su incumplimiento.

Corresponderá a SOTRONIC establecer el contenido del contrato del suscriptor, reflejando tanto las responsabilidades de la CA, la RA y la de los suscriptores y titulares; y los procedimientos a seguir para realizar la firma del mismo. Los contratos firmados se podrán emitir y archivar de forma digital o manuscrita.

7.2.3. Tiempo para el procesamiento de la solicitud de un certificado

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la RA debe enviar a la CA la autorización de la emisión del certificado de manera inmediata, salvo que medie alguna razón justificada.

El tiempo necesario para el procesamiento de solicitudes, no debe ser mayor a 5 días útiles a partir de la solicitud por parte de la RA, considerando el intercambio de información necesario entre la CA y la RA.

7.3. Renovación de certificado

7.3.1. Circunstancias para la renovación de un certificado

La renovación de un certificado implica que se generarán un nuevo par de claves y un nuevo certificado correspondiente a una nueva clave pública, pero manteniendo la mayor parte de la información del suscriptor contenida en el certificado a expirar, de acuerdo con lo establecido en este documento.

La renovación de claves rutinaria es un proceso programado cada vez que un nuevo par de claves debe ser emitido debido a su expiración y con anticipación a ésta. Se permitirá a los titulares solicitar una renovación rutinaria del mismo, antes de que ocurra la expiración de su certificado.

En el caso que el certificado del titular haya expirado o haya sido revocado, deberá seguirse el proceso de identificación inicial descrito en el presente documento. No será necesaria la identificación para la renovación, de acuerdo con lo establecido en esta DPR, siempre y cuando no se altere la información contenida en el certificado electrónico.

7.3.2. Personas habilitadas para solicitar la reemisión de certificado

Sólo el titular de un certificado puede solicitar la renovación de su certificado, en las condiciones indicadas en esta DPR.

7.3.3. Procesamiento de las solicitudes para renovación de certificados

La solicitud de renovación de certificado podrá ser rechazada en caso de que el periodo de uso del certificado o las claves haya expirado, en este caso deberá seguirse el proceso inicial de verificación de identificación ante la Autoridad de Registro.

Antes de aprobar la renovación de un certificado, la RA comprueba que la información utilizada para verificar la identidad y los restantes datos del titular y del suscriptor continúan siendo válidos. Si cualquier información del titular o del suscriptor ha cambiado, se registra adecuadamente la nueva información. La validación de la información se realizará de acuerdo con lo previsto en este documento. La solicitud de renovación será firmada por el solicitante.

Verificados los datos del titular, se procederá la renovación del certificado, notificando a la CA los datos de la solicitud y la aprobación de la misma, a través de los mecanismos que ésta establezca. La RA en la notificación envía copia de la solicitud de renovación firmada.

7.4. Revocación y suspensión del certificado

7.4.1. Circunstancias para la revocación

El titular y el suscriptor del certificado están obligados, bajo su responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la CA.
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido a través de lo estipulado en el contrato del suscriptor y/o titular.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Por decisión de la legislación respectiva.
- Por muerte, o por inhabilitación o incapacidad declarada judicialmente de la persona natural titular del certificado.

En caso de que los cambios en la información del titular no tengan impacto en los terceros que confían, no es necesaria la revocación del certificado existente ni la emisión de uno nuevo.

7.4.2. Personas habilitadas para solicitar la revocación

Las personas que pueden solicitar la revocación de un certificado:

- El titular o suscriptor del certificado.
- La CA o RA que emitió el certificado.
- Un juez que de acuerdo con la legislación aplicable decida revocar el certificado.

7.4.3. Procedimiento para la solicitud de revocación

El suscriptor y el titular pueden solicitar la revocación de su certificado a través de medios telemáticos utilizando un medio que garantice el no repudio, como un mensaje firmado con un certificado válido, la autenticación a través de una frase secreta conocida sólo por el suscriptor del certificado, etc. El suscriptor también puede realizar la solicitud directamente a la RA. En todos los casos la solicitud de revocación deberá ser firmada por el solicitante.

La RA deja constancia de la identidad del solicitante, los motivos de la revocación y cualquier otra observación que resulte pertinente. En caso de que no se acepte la revocación, la RA deja constancia de los hechos que motivaron dicha denegatoria.

Los terceros (incluyendo órdenes judiciales) deben presentarse personalmente o mediante un representante legalmente autorizado en las instalaciones de la RA para realizar la solicitud de revocación, con la documentación que corresponda de acuerdo con esta DPR.

La CA establece el procedimiento para realizar las solicitudes de revocación de los certificados de los suscriptores.

Cuando se produzca la revocación, la misma indicará el momento desde la que se aplica, precisando la fecha, hora, minuto y segundo. La revocación no aplicará de manera retroactiva y se notificará al titular del certificado digital.

7.4.4. Causas de suspensión de un certificado

Los certificados pueden ser suspendidos a partir de las siguientes causas:

- Cuando así sea solicitado por el suscriptor o la persona natural identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al suscriptor o la persona natural identificada en el certificado.
- La falta de uso del certificado durante un periodo prolongado de tiempo, conocido previamente.

- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado.

7.4.5. Personas habilitadas para solicitar la revocación, suspensión o reactivación

Pueden solicitar la revocación, suspensión o reactivación de un certificado:

- La persona identificada en el certificado.
- El suscriptor del certificado por medio de su representante legal o agente debidamente autorizado.

7.4.6. Procedimientos de solicitud de revocación, suspensión o reactivación

La persona o entidad que precise la suspensión de un certificado, deberá realizarlo él mismo a través de Autoridad de Registro

La solicitud suspensión 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 para la petición de revocación.

La solicitud debe ser autenticada de acuerdo con los requisitos establecidos en este documento, antes de proceder a la suspensión.

7.5. Modificación de certificados

SOTRONIC no prestará el servicio de modificación de certificados.

8. Gestión de la seguridad y de las operaciones

SOTRONIC garantiza la implementación de medidas de seguridad para asegurar la información en sus operaciones, así como de la infraestructura que sostiene el servicio, las cuales se encuentran detalladas en los apartados 5 y 6 de la Declaración de Prácticas de Certificación de UANATACA como CA y proveedor de la infraestructura de clave pública utilizada para la prestación de los servicios de certificación.

8.1. Controles de seguridad física, de gestión y de operaciones

Se han dispuesto medidas de seguridad de acuerdo con los mejores estándares internacionales, de tal manera que existen:

- Controles de seguridad física
- Controles de procedimientos
- Controles de personal
- Procedimientos de auditoría de seguridad
- Controles para el archivo de informaciones
- Procedimientos seguros de renovación de claves
- Procedimientos ante el compromiso de claves y recuperación de desastre

Para más información revisar la Declaración de Prácticas de Certificación de Uanataca, disponibles en: https://www.uanataca.com/public/cps_nc/.

8.2. Controles de seguridad técnica

El PSC utiliza la infraestructura técnica y lógica de la CA a la que está vinculada, con el fin de proteger tanto los sistemas como toda la información y documentación electrónica que se derive de la prestación de servicios de certificación. Por ello, se asegura de que se emplean sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

Se establecen procedimientos, procesos y controles de seguridad para:

- Generación e instalación del par de clave
- Protección de la clave privada
- Otros aspectos de gestión del par de claves
- Fatos de activación
- Controles de seguridad informática
- Controles técnicos del ciclo de vida
- Controles de seguridad de red
- Controles de ingeniería de módulos criptográficos
- Fuentes de tiempo

9. OTRAS MATERIAS DE NEGOCIO Y LEGALES

9.1. Tarifas y reembolso

SOTRONIC establece el monto de sus tarifas para la emisión, renovación y en general cualquier otro servicio, las cuales son referenciadas en los contratos de suscriptores. Igualmente se referencian las políticas de reembolso.

9.2. Confidencialidad de la información del negocio

9.2.1. Alcances de la información confidencial

Se mantiene de manera confidencial la siguiente información:

- Material comercialmente reservado del PSC, de los suscriptores de empresa y de los terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual;
- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores de empresa y los terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- Información que mantiene, la cual pudiera perjudicar la normal realización de sus operaciones.
- Los motivos o causales de revocación de un certificado.

9.2.2. Responsabilidad de protección de la información confidencial

En todo momento se establecen medidas de seguridad que aseguran el cumplimiento de las disposiciones de confidencialidad como leyes sobre protección de datos personales, confidencialidad de la información y propiedad intelectual que les fueren aplicables.

No obstante lo anterior, se debe permitir la publicación de información del estado de los certificados, así como la información en relación a la revocación de un certificado sin

revelar la razón de dicha revocación. La publicación se podrá limitar a suscriptores legítimos, titulares o terceros que confían.

9.2.3. Información tratada como privada

Se debe mantendrá confidencial la siguiente información:

- Información personal provista por los suscriptores, titulares y terceros que confían que no sea la autorizada para estar contenida en certificados y repositorios;
- Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre suscriptores, titulares y terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.

Se permite expresamente la publicación de información respecto a la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha suspensión o revocación.

9.2.4. Información no considerada privada

Se permite la divulgación de información personal sólo en los casos en que exista consentimiento expreso del individuo cuya información corresponde.

9.2.5. Notificación y consentimiento para el uso de información

Los contratos firmados con suscriptores referencian el tipo de datos personales que pueden ser recolectados, cómo serán utilizados, protegidos y cómo estos pueden ser revisados/corregidos, las circunstancias bajo las cuales serán divulgados, la manera de desagravios y sanciones para las fallas en el cumplimiento del acuerdo con la parte o partes que utilizan o recolectan dichos datos y el consentimiento necesario para su divulgación. Igual referencia contiene las notificaciones con terceros que confían.

9.2.6. Divulgación realizada con motivo de un proceso judicial o administrativo

SOTRONIC permitirá la revelación de información personal a oficiales encargados del cumplimiento de leyes o como parte de un descubrimiento civil, donde se hace una solicitud de conformidad con la ley aplicable en la jurisdicción en donde la Autoridad de Registro se encuentra localizada.

9.2.7. Otras circunstancias para divulgación de información

Los suscriptores, titulares y terceros que confían pueden solicitar la divulgación de la información que han provisto a terceros. Se requiere que la divulgación de la información bajo otras circunstancias se realice de conformidad con la legislación aplicable.

9.3. Derecho de propiedad intelectual

SOTRONIC mantiene derecho de propiedad sobre todos los registros y demás información necesaria para asegurar la continuidad de los servicios.

9.4. Representaciones y garantías

SOTRONIC referencia provisiones de garantía y responsabilidad en relación con errores u omisiones, incluyendo limitaciones y exclusiones, términos, condiciones, incluyéndolas en los contratos con los suscriptores, y haciéndolos disponibles para los terceros que confían.

Los suscriptores y/o titulares están obligados a cumplir las obligaciones establecidas en el presente documento, así como en la DPC y PC de la CA. Estas obligaciones se referenciarán en los contratos respectivos. El PSC referencia igualmente las obligaciones de los terceros que confían, especialmente las relativas en su necesidad de verificar el estado de los certificados.

Cualquier otro participante que tenga obligaciones o se le ofrezcan garantías se referenciará específicamente en documento relevante.

9.5. Exención de garantías

SOTRONIC responde por las responsabilidades expresamente presentadas en esta DPR, el contrato y aquellas no previstas expresamente en este documento pero ordenadas por la legislación vigente.

9.6. Limitación de responsabilidad

SOTRONIC limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados, así como los acuerdos adoptados en los contratos con los suscriptores.

9.7. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro, notificación y fuerza mayor

SOTRONIC establece, tanto para el contrato de suscriptor y la presente DPR:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.
- En ningún caso SOTRONIC responderá por caso fortuito y en caso de fuerza mayor.

9.8. Provisiones sobre resolución de disputas

SOTRONIC establece, en el contrato de suscriptor y/o en el texto de divulgación o PDS, los procedimientos de mediación y resolución de conflictos aplicables.

9.9. Ley aplicable

SOTRONIC establece, en el contrato de suscriptor y en el texto de divulgación o PDS, una cláusula de jurisdicción competente, indicando que competencia judicial correspondiente.