ALCANCE

Marco de referencia para en la declaración de prácticas de certificación

Aplica a personal tanto interno como externo de Transacciones y Transferencias S.A.

DESCRIPCIÓN DE LA POLÍTICA

1 Introducción

1.1. Presentación

Este documento constituye la declaración de prácticas de certificación de Transacciones y Transferencias S.A. (en lo sucesivo 5B) en relación a la prestación de sus servicios de certificación de acuerdo a la normativa legalmente aplicable.

Los certificados que se emiten son los siguientes:

- De Persona Natural
- De Personal Natural Representante
- De Persona Jurídica

1.2. Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación de 5B".

1.2.1. Identificadores de certificados

5B ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

Número OID	Tipo de certificados
	Persona Natural
1.3.6.1.4.1.51963.1.1.1	*Certificado de Persona Natural*
1.3.6.1.4.1.51963.1.1.2	*Certificado de Persona Natural Representante*
	Representante de Entidad
1.3.6.1.4.1. 51963.1.2.1	*Certificado de Persona Jurídica*

En caso de contradicción entre esta Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas.

USO PÚBLICO

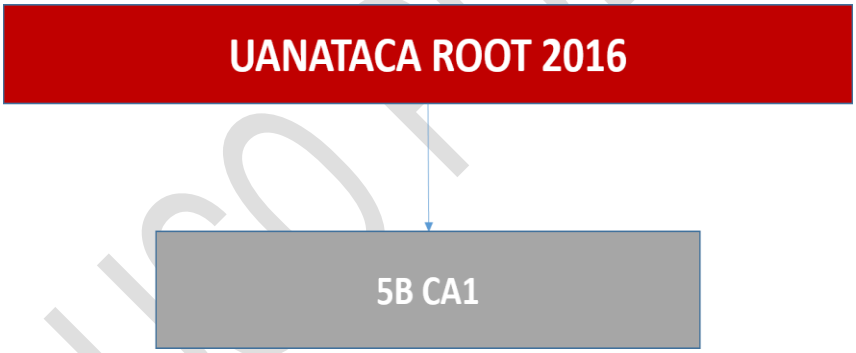
1.3. Participantes en los servicios de certificación

1.3.1. Prestador de servicios de certificación

El prestador de servicios de certificación es la persona jurídica, que expide y gestiona certificados para entidades finales, empleando una Autoridad de Certificación, o presta otros servicios relacionados con la firma electrónica.

5B es un prestador de servicios de certificación que actúa de conformidad con las previsiones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, su reglamento, así como las normas técnicas que establece el Registro de Prestadores de Servicios de Certificación aplicables a la expedición y gestión de certificados de firma electrónica avanzada, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, 5B ha establecido una jerarquía de autoridades de certificación:



1.3.1.1. UANATACA ROOT 2016

Se trata de la autoridad de certificación raíz de la jerarquía que emite certificados a otras autoridades de certificación, y cuyo certificado de clave público ha sido auto firmado.

Datos de identificación:

CN:	UANATACA ROOT 2016
Huella digital:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 ad
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Lunes, 11 de marzo de 2041
Longitud de clave RSA:	4.096 bits

U. USO PÚBLICO

1.3.1.2. 5B CA1

Se trata de la autoridad de certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la UANATACA ROOT 2016.

Datos de identificación:

CN:	5B CA1
Huella digital:	41F5 3131 DD44 6942 162028 7F7E75 B46C 89EA 7535
Válido desde:	Jueves, 17 de mayo de 2018
Válido hasta:	Viernes, 16 de mayo de 2031
Longitud de clave RSA:	4.096 bits

1.3.2. Autoridad de Registro

La Autoridad de Registro es 5B, en consecuencia, es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante/suscriptor del certificado.
- Gestionar la generación de claves y la emisión del certificado, o hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

1.3.3. Entidades finales

Las entidades finales son las personas u organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de autenticación y firma electrónica.
Serán entidades finales de los servicios de certificación de 5B las siguientes:

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

0- USO PÚBLICO

1.3.3.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- Las empresas, entidades, corporaciones u organizaciones que los adquieren a 5B (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo, y se encuentran identificados en los certificados.
- Las personas naturales 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, 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 de certificación es, por tanto, el cliente del prestador de servicios de certificación, de acuerdo con la legislación y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación y la normativa legalmente aplicable, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes.

1.3.3.2. Firmantes

Los firmantes son las personas naturales que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma electrónica avanzada; pudiendo ser personas típicamente empleados, representantes legales o voluntarios, así como otras personas vinculadas a los suscriptores; incluyendo las personas al servicio de las Administraciones Públicas, en los certificados de empleado público.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre 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 de certificación, por lo que las personas naturales identificadas en los correspondientes certificados son las únicas responsables de su protección y deben 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 natural identificada en el

0 - USO PÚBLICO

certificado", siempre con pleno respeto al cumplimiento de la regulación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.3.3.3. Partes usuarias

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

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en la página web del 5B como Prestador de Servicios de Certificación.

1.4. Uso de los certificados

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

1.4.1. Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, disponibles en el web https://www.5b.com.gt/identidad-digital.php.

1.4.1.1. Certificado de firma de Persona Natural

Este certificado dispone del OID 1.3.6.1.4.1.51963.1.1.1. Es un certificado que se emite para la autenticación y la firma electrónica avanzada, de acuerdo a las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Este certificado garantiza la identidad del firmante y su vinculación con el suscriptor (si lo hubiese) del servicio electrónico de confianza, y permite la generación de la "firma electrónica avanzada", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

0-USO PUBLICO

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

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

El campo "key usage" tiene activadas y por tanto 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 avanzada).
c) Key Encipherment.

1.4.1.2. Certificado de Persona Natural Representante

Este certificado dispone del OID 1.3.6.1.4.1.51963.1.1.2. Es un certificado que se emite para la autenticación y la firma electrónica avanzada, de acuerdo a las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

El uso de este certificado garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y la entidad, empresa u organización descrita en el campo "O" (Organization), y permite la generación de la "firma electrónica avanzada", es decir, la firma electrónica que está vinculada al firmante de manera única, permitiendo su identificación y ha sido generada utilizando medios que el firmante puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

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

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

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

0-USO PÚBLICO

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 avanzada).
c) Key Encipherment.

1.4.1.3. Certificado de Persona Jurídica

Este certificado dispone del OID 1.3.6.1.4.1.51963.1.2.1. Es un certificado que se emite para la autenticación y la firma electrónica avanzada de una persona jurídica, de acuerdo a las disposiciones del Decreto No. 47-2008 de Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Estos certificados garantizan la identidad de la entidad, empresa u organización suscriptora identificada en el certificado, y en su caso la del responsable de gestionar el certificado (si se hubiese identificado). Este certificado permite la generación de la "firma electrónica avanzada", es decir, la firma electrónica que está vinculada al firmante (entidad, empresa u organización) de manera única, permitiendo su identificación y ha sido generada utilizando medios que puede mantener bajo su control exclusivo, vinculada a los datos a que se refiere, de modo tal que cualquier cambio ulterior de los mismos es detectable.

La firma electrónica avanzada generada a través de este certificado tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio conforme a las previsiones del artículo 33 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:
a) Autenticación en sistemas de control de acceso.
b) Firma de correo electrónico seguro.
c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

El campo "key usage" tiene activadas y por tanto 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 avanzada).
c) Key Encipherment.

0-USO PÚBLICO

SI ESTA UTILIZANDO UNA VERSION IMPRESA O UN ARCHIVO ELECTRONICO DE ESTE DOCUMENTO, RECUERDE VERIFICAR QUE NO HA TENIDO CAMBIOS CONSULTANDO LA VERSION ELECTRONICA DEL PORTAL DEL COMITE DE SEGURIDAD DE LA INFORMACIO

1.4.2. Límites y prohibiciones de uso de los certificados

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

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

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

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, disponibles en la web de 5B.

El empleo de los certificados digitales en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos con las autoridades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a 5B, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

5B 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 5B emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad que provenga del contenido aparejado al uso de un certificado.

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

0 - USO PÚBLICO

1.4.3. Certificados de corta duración

Los certificados de corta duración, son certificados expedidos con un período de validez máximo de veinticuatro (24) horas, para la firma electrónica de una transacción de firma para la cual se emitió dentro de las veinticuatro (24) horas de su vigencia. Inmediatamente después de su uso, la clave privada se deshabilita imposibilitando su uso posterior hasta su caducidad. La transacción a la que se hace referencia puede contener varios documentos dentro de una única solicitud de transacción para la que se genera el certificado de firma electrónica.

1.5. Administración de la política

1.5.1. Organización que administra el documento

Transacciones y Transferencias S.A., identificada en este documento por su marca comercial “5B”.

1.5.2. Datos de contacto de la organización

Transacciones y Transferencias S.A.
15 avenida 17-40 zona 13, edificio Tetra Center Torre I, 4to nivel.
Guatemala, Guatemala

1.5.3. Procedimientos de gestión del documento

El sistema documental y de organización de 5B 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.

0 - USO PÚBLICO

2. Publicación de información y depósito de certificados

2.1. Depósito(s) de certificados

5B dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de 5B, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de esta Declaración de Prácticas de Certificación

2.2. Publicación de información del prestador de servicios de certificación

5B publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos, cuando se haya obtenido consentimiento de la persona natural identificada en el certificado.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados aplicables.
- La Declaración de Prácticas de Certificación.

2.3. Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo las políticas y la Declaración de Prácticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.9 y 4.9.10 de esta Declaración de Prácticas de Certificación.

0 - USO PÚBLICO

2.4. Control de acceso

5B no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

5B emplea sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si la persona natural identificada en el certificado ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

0 - USO PÚBLICO

3. Identificación y autenticación

3.1. Registro inicial

3.1.1. Tipos de nombres

Todos los certificados contienen un nombre distintivo (DN o *distinguished name*) conforme al estándar X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y/o de la persona natural identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

3.1.1.1. Certificado de Persona Natural

Country (C)	Estado[1]
Organization (O)	Organización suscriptora a la que está vinculado el firmante (si la hubiese)
Organization Unit (OU)	Unidad de la Organización suscriptora a la que está vinculado el firmante (si la hubiese)
Organization Identifier	Número de identificación fiscal de la Organización suscriptora a la que está vinculado el firmante (si la hubiese)
Title	Título/especialidad o cargo del de firmante (según aplique)
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número del Documento de Identidad utilizado para la identificación del firmante.
Common Name (CN)	Nombre y apellidos del firmante acompañado de una referencia de la persona jurídica suscriptora o del número de habilitación profesional cuando aplique, de acuerdo a la política de certificación.

[1] El campo "Estado" corresponderá Estado de la nacionalidad de la persona natural identificada en el certificado o el Estado donde la persona jurídica suscriptora (si la hubiese) se encuentra registrada.

0-USO PÚBLICO

3.1.1.2. Certificado de Persona Natural Representante

Country (C)	Estado[2]
Organization (O)	Organización suscriptora que representa el firmante
Organization Unit (OU)	Unidad de la Organización suscriptora a la que está vinculado el firmante
Organization Identifier	Número de identificación fiscal de la Organización suscriptora a la que representa el firmante
Title	Tipo de representación (Ej. Representante Legal)
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número del Documento de Identidad utilizado para la identificación del firmante.
Common Name (CN)	Nombre y apellidos del representante, su número de identificación y el identificador fiscal de la persona jurídica.

3.1.1.3. Certificado de Persona Jurídica

Country (C)	Estado donde la entidad está registrada la Organización
Organization (O)	Nombre de la Organización
Organization Unit (OU)	Indica la naturaleza del certificado
Organization Identifier	Número de identificación fiscal de la Organización a la que está vinculado el certificado
Surname	Apellidos del responsable de la gestión certificado
Given Name	Nombre del responsable de la gestión del certificado
Serial Number	Número de identificación fiscal de la Organización a la que está vinculado el sello electrónico
Common Name (CN)	Nombre del sistema automático

3.1.2. Significado de los nombres

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

[2] El campo "Estado" corresponderá Estado donde la persona jurídica suscriptora se encuentra registrada.

0 USO PÚBLICO

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

En el caso que los datos indicados en el DN o Subject fueran ficticios (ej. “Test Organization”, “Test Nombre”, “Apellido1”) o se indique expresamente palabras que denoten su invalidez (ej. “TEST”, “PRUEBA” o “INVALIDO”), se considerará al certificado sin validez legal y por lo tanto sin responsabilidad alguna sobre 5B. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y permitir al ente regulador su evaluación.

3.1.3. Empleo de anónimos y seudónimos

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

3.1.4. Interpretación de formatos de nombres

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

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

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

En el campo “número de serie” se incluye el DPI, Identificación de Extranjero, Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

3.1.5. Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de 5B.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del número de los números de los documentos de identificación de las personas o sus números de identificación tributaria, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

0 - USO PÚBLICO

- Número de Identificación tributaria u otro identificador legalmente válido de la persona natural.
- Número de Identificación tributaria u otro identificador legalmente válido del suscriptor.
- Tipo de certificado (OID de identificador de política de certificación).
- Soporte del certificado.

Como excepción esta DPC permite emitir un certificado cuando coincida el número de identificación fiscal del suscriptor, número de identificación fiscal del firmante, Tipo de certificado, soporte del certificado, con un certificado activo, siempre que exista algún elemento diferenciador entre ambos, por ejemplo en los campos cargo (title) y/o departamento (Organizational Unit).

3.1.6. Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

5B no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, CRECIG (Centro de Resolución de Conflictos de la Cámara de Industria), a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte en el documento contractual que formaliza el servicio.

0-USO PÚBLICO

3.2. Validación inicial de la identidad

Para la solicitud de certificados los Operadores de la Autoridad de Registro de 5B verificarán la identidad del firmante a la que se le expide el certificado (véase la persona natural o representante autorizado de la persona jurídica), así como cualquier atributo especifico de la persona natural o jurídica con la que tenga relación o vinculación. Para esta verificación se procederá de acuerdo con uno de los siguientes métodos:

1. En presencia de la persona natural o de un representante autorizado de la persona jurídica. Se podrá prescindir de la presencia física, cuando la solicitud de expedición de un certificado cualificado haya sido legitimada en presencia notarial, o

2. Por medio del procedimiento de identificación electrónica a través del sistema de vídeo identificación remota de 5B o utilizando otros métodos de identificación reconocidos a escala nacional.

La identidad de los suscriptores de los certificados resulta fijada en el momento de la firma del contrato entre 5B y el suscriptor, momento en el que queda verificada la existencia del suscriptor mediante su documento oficial de identidad o las escrituras correspondientes según sea el caso, al igual que los poderes de actuación de la persona que presente como representante de una organización si fuese el caso. Para esta verificación, se podrá emplear cualquier documentación privada, pública o notarial, así como la consulta directa a los registros públicos correspondientes.

En el caso de personas naturales identificadas en certificados cuyo suscriptor sea una persona jurídica, sus identidades se validarán mediante la presentación de su documento oficial de identificación o mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. En este último caso, el suscriptor producirá una certificación de los datos necesarios, y la remitirá a 5B, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

Los ficheros de datos personales de cada entidad, empresa u organización de derecho público o privado a que se refiere el párrafo anterior son responsabilidad de cada organización, siendo su responsabilidad, y no la de 5B.

3.2.1. Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor en el caso de certificados de persona jurídica, o por el firmante en certificados de personal natural.

0 - USO PÚBLICO

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

Las personas naturales con capacidad de actuar en nombre de las personas jurídicas u organizaciones suscriptoras en general, podrán actuar como representantes de las mismas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona natural y la organización de la que se trate, que exige su reconocimiento por 5B, sus autoridades de registro y/o terceros vinculados, la cual se realizará mediante el siguiente procedimiento:

1. El representante del suscriptor deberá acreditar su identidad por uno de los métodos de identificación especificados en el apartado 3.2., de tal manera que:
    - (i) Si se identifica presencialmente ante un operador de la Autoridad de Registro de 5B:
        - Mostrando su Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación.
        - Acreditando el carácter y facultades que alegue poseer.

    - (ii) Si se identifica electrónicamente a través del sistema de vídeo identificación remota de 5B:
        - Mostrando su Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación.
        - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.
        - Acreditando el carácter y facultades que alegue poseer.

2. El representante de la organización proporcionará la siguiente información y sus correspondientes soportes acreditativos:
    - Sus datos de identificación, como representante:
        - Nombre y apellidos
        - Lugar y fecha de nacimiento
        - Documento de identidad idóneo reconocido en derecho para la identificación del representante
    - Los datos de identificación del suscriptor al que representa:

0 - USO PUBLICO

- Denominación o razón social.
- Información de registro existente, que puede incluir los datos relativos a la constitución, personalidad jurídica, extensión y vigencia de las facultades de representación del solicitante.
- Documento: documento acreditativo de la identificación fiscal de la organización suscriptora.
- Documento: Documentos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

- Los datos relativos a la representación o la capacidad de actuación que ostenta:
  - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin) si resulta aplicable.
  - El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:
    - TOTAL. Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.
    - PARCIAL. Representación o capacidad parcial. Esta comprobación se podrá realizar mediante copia auténtica o electrónica de la escritura notarial de apoderamiento, en los términos de la normativa notarial.

3. El operador de la Autoridad de Registro de 5B comprobará la identidad del representante actuando del siguiente modo:
   - Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
     - Documento de identidad u otro medio idóneo reconocido en derecho para su identificación.
     - Documentación que acredite su representación.

   - Cuando la identificación se haya realizado a través del método de identificación electrónica a través de vídeo identificación de 5B mediante:
     - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.

0 - USO PÚBLICO

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

4. El operador de la Autoridad de Registro de 5B verificará la información suministrada para la autenticación y le devolverá cuando corresponda la documentación original aportada.

5. Alternativamente, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar al operador de la Autoridad de Registro 5B, en cuyo caso los pasos 3 y 4 anteriores no serán precisos.

La prestación del servicio de certificación se formaliza mediante el oportuno contrato entre 5B y el suscriptor, debidamente representado.

3.2.3. Autenticación de la identidad de una persona natural

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

3.2.3.1. En los certificados

La identidad de las personas naturales firmantes identificados en los certificados, se valida a través de los métodos de identificación especificados en el apartado 3.2., de tal manera que:

- (i) Si se identifica presencialmente ante un operador de la Autoridad de Registro de 5B:
  - Mostrando su Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación.

- (ii) Si se identifica electrónicamente a través del sistema de vídeo identificación remota de 5B:
  - Mostrando su Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación;
  - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e

0-USO PÚBLICO

inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.

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

3.2.3.2. Validación de la Identidad

Para la solicitud de certificados, el operador de la Autoridad de Registro 5B comprobará la identidad de la persona natural identificada en la solicitud del certificado, actuando del siguiente modo:

- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
  - Documento de identidad aportado.

- Cuando la identificación se haya realizado a través del método de identificación electrónica a través de vídeo identificación de 5B mediante:
  - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
  - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de vídeo identificación remota.
  - Revisión del cotejo producido por el sistema de vídeo identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
  - Revisión producida por el sistema de vídeo identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica los mismos pueden ser tramitados cuando medie un documento idóneo para la verificación de los extremos establecidos en esta declaración de prácticas de certificación. Sin embargo, la entrega del certificado o de las respectivas credenciales de generación y acceso deben deberán realizarse a persona autorizada del suscriptor, con la correspondiente verificación de su identidad.

0 - USO PÚBLICO

3.2.3.3. Vinculación de la persona natural

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

3.2.4. Información de suscriptor no verificada

5B no incluye ninguna información de identificación del suscriptor no verificada en los certificados. No obstante lo anterior, 5B puede incluir en los certificados, de acuerdo a las instrucciones del solicitante, información que no afecte su identificación personal, como por ejemplo la dirección de correo electrónico y/o número de teléfono.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, la Autoridad de Registro de 5B comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona naturales identificadas en el certificado continúan siendo válidos.

- Los métodos aceptables para dicha comprobación son alguno de los de Verificación presencial de la solicitud de la renovación del certificado.
- Solicitud de renovación del certificado digital realizada firmada con firma electrónica avanzada basada en certificado vigente para el momento de su renovación, siempre que no hayan cambios en la información contenida en el mismo.

Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2.

3.3.2. Identificación y autenticación de la solicitud de renovación

Antes de generar un certificado a un suscriptor cuyo certificado fue revocado, el operador de la Autoridad de Registro de 5B comprobará que la información empleada en su día para verificar la identidad y los restantes datos del suscriptor y de la persona natural identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

0-USO PÚBLICO

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

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

Si cualquier información del suscriptor o de la persona natural identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2.

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

5B a través de sus operadores de la Autoridad de Registro autentican las peticiones e informes relativos a la revocación, suspensión o reactivación de un certificado, comprobando que provienen de una persona autorizada.

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

- El suscriptor y/o firmante:
  - Identificándose y autenticándose mediante el uso del Código de Revocación (CRE o ERC) a través de la página web de 5B en horario 24x7.
  - Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la suspensión o revocación, a juicio de 5B y/o Autoridades de Registro.
- 5B como autoridad de registro, deberá identificar al firmante ante una petición de revocación, suspensión o reactivación según los propios medios que considere necesarios.

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

0- USO PÚBLICO

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

4.1. Solicitud de emisión de certificado

4.1.1. Legitimación para solicitar la emisión

El solicitante del certificado, sea persona natural o jurídica, debe firmar un contrato de prestación de servicios de certificación con 5B, el cual podrá presentarse en formato digital o en papel.

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

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

4.1.2. Procedimiento de alta y responsabilidades

5B recibe solicitudes de certificados, realizadas por personas naturales, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se instrumentan mediante un formulario en formato papel o electrónico, de manera individual o por lotes, o mediante la conexión con bases de datos externas, o a través de una capa de *Web Services* cuyo destinatario es 5B.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona natural identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la persona natural identificada en el certificado.

4.2. Procesamiento de la solicitud de certificación

0-USO PÚBLICO

4.2.1. Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, 5B se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, 5B verifica la información proporcionada, verificando los aspectos descritos en la sección 3.2

En relación a las evidencias recogidas durante el proceso de solicitud del certificado para la aprobación de la misma la misma es conservada con garantías de seguridad e integridad durante el plazo de 10 años desde la emisión del certificado, incluso en caso de pérdida anticipada de vigencia por revocación.

4.2.2. Aprobación o rechazo de la solicitud

En caso que los datos se verifiquen correctamente, 5B aprueba la solicitud del certificado y proceder a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si existen indicios de que no es correcta o que puede afectar a la reputación del Prestador de Servicios de Certificación, de las Autoridades de Registro o de los suscriptores, 5B denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, 5B denegará la solicitud definitivamente.

5B notifica al solicitante la aprobación o denegación de la solicitud.

5B podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

4.2.3. Plazo para resolver la solicitud

5B atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

0 - USO PÚBLICO

4.3. Emisión del certificado

4.3.1. Acciones de la CA durante el proceso de emisión

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

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

Durante el proceso, 5B:

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

4.3.2. Notificación de la emisión al suscriptor

5B notifica la emisión del certificado al suscriptor y/o a la persona natural identificada en el certificado y el método de generación/descarga/acceso.

4.4. Entrega y aceptación del certificado

4.4.1. Responsabilidades de la CA

Durante este proceso, el operador de la Autoridad de Registro 5B debe realizar las siguientes actuaciones:

0-USO PÚBLICO

- Acreditar definitivamente la identidad de la persona natural identificada en el certificado, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3.
- Disponer del Contrato de Prestación de Servicios de Certificación debidamente firmado por el Suscriptor.
- Entregar la hoja de entrega y aceptación del certificado a la persona natural identificada en el certificado con los siguientes contenidos mínimos:
    - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades.
    - Información acerca del certificado.
    - Reconocimiento, por parte del firmante, de recibir el certificado y/o los mecanismos para su generación/descarga y la aceptación de los citados elementos.
    - Régimen de obligaciones del firmante.
    - Responsabilidad del firmante.
    - Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
    - La fecha del acto de entrega y aceptación
      Toda esta información podrá incluirse en el propio Contrato de Prestación de Servicios de Certificación. Dicho lo cual, cuando se produzca la firma del Contrato Prestación de Servicios de Certificación por el Suscriptor, se entenderá perfeccionada la entrega y aceptación del certificado.
- Obtener la firma de la persona identificada en el certificado.

Las Autoridades de Registro son las encargadas de realizar estos procesos, debiendo registrar documentalmente los anteriores actos y conservar las evidencias correspondientes.

4.4.2. Conducta que constituye aceptación del certificado

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

Cuando la generación y entrega del certificado ocurre en el mismo momento siguiendo el procedimiento definido por 5B, la aceptación del certificado por la persona física identificada en el mismo se produce mediante la firma del contrato de Prestación de Servicios de Certificación.

0 - USO PÚBLICO

4.4.3. Publicación del certificado

5B publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes y siempre que 5B disponga de la autorización de la persona natural identificada en el certificado.

4.4.4. Notificación de la emisión a terceros

5B no realiza ninguna notificación de la emisión a terceras entidades.

4.5. Uso del par de claves y del certificado

4.5.1. Uso por el firmante

Los firmantes se obligan a:

- Facilitar a 5B información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en las políticas y prácticas de certificación de 5B.
- Reconocer la capacidad de producción de firmas electrónicas avanzadas mediante el certificado emitido por 5B; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada y/o las credenciales de acceso a la misma, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en esta Declaración de Prácticas de Certificación.
- Comunicar a 5B, Autoridades de Registro y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.

Los firmantes se responsabilizan de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.

0-USO PÚBLICO

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

4.5.2. Uso por el suscriptor

4.5.2.1. Obligaciones del suscriptor del certificado

5B obliga contractualmente al suscriptor a:

- Facilitar al Prestador de Servicios de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la utilización de un certificado.
- Emplear el certificado de acuerdo con lo establecido en las políticas y prácticas de certificación de 5B en su condición de Prestador de Servicios de Certificación.
- Comunicar a 5B, Autoridades de Registro y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
    - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas naturales identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de las mismas.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de 5B, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de 5B.

0 - USO PÚBLICO

4.5.2.2. Responsabilidad civil del suscriptor de certificado

5B obliga contractualmente al suscriptor a responsabilizarse de:

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

4.5.3. Uso por el tercero que confía en certificados

4.5.3.1. Obligaciones del tercero que confía en certificados

5B informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma electrónica o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas basadas en certificados emitidos por 5B como Prestador de Servicios de Certificación debidamente autorizado para operar como tal por el Registro de Prestadores de Servicios de Certificación, tienen la consideración legal de firmas electrónicas avanzadas; esto es, equivalentes a firmas manuscritas.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.

0-USO PÚBLICO

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de 5B, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la 5B.

4.5.3.2. Responsabilidad civil del tercero que confía en certificados

5B informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

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

4.6. Renovación de certificados

La renovación de los certificados exige la renovación de claves, por lo que debe atenderse a lo establecido en la sección 4.7.

4.7. Renovación de claves y certificados

4.7.1. Causas de renovación de claves y certificados

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación. Dadas las características particulares de los certificados de corta duración este proceso de renovación no les es aplicable.

Se consideran al menos las siguientes posibilidades para la renovación de certificados:

a) Proceso de renovación presencial, que se efectuará del mismo modo que la emisión de un nuevo certificado.

b) Proceso de renovación telemático, mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación, de acuerdo a las disposiciones siguientes.

0-USO PÚBLICO

4.7.2. Legitimación para solicitar la renovación

Con anterioridad a la emisión y entrega de un certificado renovado, debe existir una solicitud de renovación de certificado, que puede producirse de oficio o a instancia de parte interesada.

4.7.3. Procedimientos de solicitud de renovación

4.7.3.1. Realización de la solicitud

5B recibe solicitudes de certificados, realizadas por las entidades, empresas u organizaciones de derecho público o privado. Existe un documento, el cual podrá ser en soporte papel o soporte digital con firma electrónica avanzada, referente a la solicitud de renovación de certificados, realizada por la entidad, empresa u organización de derecho público o privado, el cual incluirá los datos de las personas a las que se expedirán certificados. La solicitud debe indicar que los datos de los certificados no han cambiado. En todos los casos, la solicitud de renovación del certificado se realizará a instancia de la parte interesada y nunca por iniciativa del prestador de servicio de certificación.

4.7.3.2. Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de renovación de certificado, 5B se asegura que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

4.7.3.3. Aprobación o rechazo de la solicitud

En caso que los datos se verifiquen correctamente, 5B debe aprobar la solicitud de renovación del certificado y proceder a su emisión y entrega.

5B notifica al solicitante la aprobación o denegación de la solicitud.

5B podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

4.7.3.4. Plazo para resolver la solicitud

0 - USO PÚBLICO

5B atiende las solicitudes de renovación de certificados por orden de llegada, en un plazo razonable anterior a la expiración de los certificados a revocar, pudiendo especificarse una garantía de plazo máximo en el convenio de emisión de certificados. Las solicitudes de renovación se mantienen activas hasta su aprobación o rechazo.

4.7.4. Notificación de la emisión del certificado renovado

5B notifica la emisión del certificado al suscriptor y/o a la persona natural identificada en el certificado.

4.7.5. Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona natural identificada en el certificado se produce mediante la firma, escrita o electrónica, de la hoja de entrega y aceptación ante el responsable de certificación de la entidad, empresa u organización de derecho público o privado.

4.7.6. Publicación del certificado

5B publica el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes de acuerdo a las previsiones de dicha sección.

4.7.7. Notificación de la emisión a terceros

5B no realiza notificación alguna de la emisión a terceras entidades

4.8. Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

4.9. Revocación, suspensión o reactivación de certificados

0-USO PUBLICO

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.
La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible. Sólo los certificados de entidad final podrán ser suspendidos.
La reactivación de un certificado supone su paso de estado suspendido a estado activo.

4.9.1. Causas de revocación de certificados

5B revoca un certificado cuando concurre alguna de las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:
   a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
   b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
   c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
2) Circunstancias que afectan a la seguridad de la clave o del certificado:
   a) Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
   b) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
   c) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
   d) El uso irregular del certificado por la persona natural identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.
3) Circunstancias que afectan al suscriptor o a la persona natural identificada en el certificado:
   a) Finalización de la relación jurídica de prestación de servicios entre 5B y el suscriptor.
   b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona 5B identificada en el certificado.
   c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
   d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.
   e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.
   f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.
   g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.

USO PUBLICO

4) Otras circunstancias:
   a) La terminación del servicio de certificación de 5B como Prestador de Servicios de Certificación.
   b) El uso del certificado que sea dañino y continuado para 5B. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
      - La naturaleza y el número de quejas recibidas.
      - La identidad de las entidades que presentan las quejas.
      - La legislación relevante vigente en cada momento.
      - La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

4.9.2. Causas de suspensión de un certificado

Los certificados de 5B 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. En este caso, 5B tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

4.9.3. Causas de reactivación de un certificado

Los certificados de 5B pueden ser reactivados a partir de las siguientes causas:

- Cuando el certificado se encuentre en un estado de suspendido.
- Cuando así sea solicitado por el suscriptor o la persona natural identificada en el certificado.

4.9.4. Quién puede 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 responsable del servicio de certificación.

0-USO PÚBLICO

4.9.5. Procedimientos de solicitud de revocación, suspensión o reactivación

La entidad que precise revocación, suspensión o reactivación de un certificado puede solicitarlo directamente a 5B o realizarlo él mismo a través del servicio en línea disponible en la página web de 5B. La revocación de los certificados de corta duración se tramitarán mediante solicitud directa a la Autoridad de Registro de 5B.

La solicitud de revocación, suspensión o reactivación deberá incorporar la siguiente información:

- Fecha de solicitud de la revocación, suspensión o reactivación.
- Identidad del suscriptor/firmante.
- Nombre y título de la persona (si aplica) 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, por 5B, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación, suspensión o reactivación.

El servicio de revocación, suspensión o reactivación se encuentra en la página web de 5B en la dirección: https://www.5b.com.gt/identidad-digital.php

En caso de que el destinatario de una solicitud de revocación, suspensión o reactivación por parte de una persona natural identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a 5B como Autoridad de Registro.

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

Tanto el servicio de gestión de revocación, suspensión o reactivación como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de 5B.

USO PÚBLICO

4.9.6. Plazo temporal de solicitud de revocación, suspensión o reactivación

Las solicitudes de revocación, suspensión o reactivación se remitirán de forma inmediata en cuanto se tenga conocimiento.

4.9.7. Plazo temporal de procesamiento de la solicitud de revocación, suspensión o reactivación

La revocación, suspensión o reactivación se producirá inmediatamente cuando sea recibida. Si se realiza a través de un operador, se ejecutará dentro del horario ordinario de operación de 5B. Si se realiza a través del servicio en línea, será inmediata. La solicitud de reactivación de un certificado que ha sido suspendido deberá realizarse presencialmente ante la autoridad de registro, salvo en los casos en que su suspensión se haya realizado debido a problemas o inconvenientes técnicos.

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

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

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por el Prestador de Servicios de Certificación 5B.

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

- http://crl1.uanataca.com/public/pki/crl/transacciones-y-transferencias-ca1.crl
- http://crl2.uanataca.com/public/pki/crl/transacciones-y-transferencias-ca1.crl

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

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.9.9. Frecuencia de emisión de listas de revocación de certificados (CRLs)

5B emite una CRL al menos cada 24 horas.

La CRL indica el momento programado de emisión de una nueva CRL, si bien se puede emitir una CRL antes del plazo indicado en la CRL anterior, para reflejar revocaciones.

La CRL mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

0-USO PÚBLICO

4.9.10. Plazo máximo de publicación de CRLs

Las CRLs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en cualquier caso no supera unos pocos minutos.

4.9.11. Disponibilidad de servicios de comprobación en línea de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de 5B, que se encuentra disponible las 24 horas de los 7 días de la semana en el web:

- https://www.uanataca.com/5b/crtlist

Para comprobar la última CRL emitida en cada CA se debe descargar:

- *Autoridad de Certificación Raíz (UANATACA ROOT 2016):*
  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *Autoridad de Certificación Intermedia o Subordinada (5B CA1):*
  - http://crl1.uanataca.com/public/pki/crl/transacciones-y-transferencias-ca1.crl
  - http://crl2.uanataca.com/public/pki/crl/transacciones-y-transferencias-ca1.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de 5B, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

5B suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

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

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

0 - USO PÚBLICO

4.9.13. Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de 5B es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de 5B, así como, -si se considera necesario-, en otros medios de comunicación, incluso en papel.

4.9.14. Período máximo de un certificado digital en estado suspendido

El plazo máximo de un certificado digital en estado suspendido es indefinido hasta su caducidad.

4.10. Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de Prácticas de Certificación. 5B puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

4.11. Depósito y recuperación de claves

4.11.1. Política y prácticas de depósito y recuperación de claves

5B no presta servicios de depósito y recuperación de claves.

4.11.2. Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

0- USO PÚBLICO

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

5.1. Controles de seguridad física

5B garantiza controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones para la prestación de los servicios electrónicos de confianza.

En concreto, la política de seguridad de 5B aplicable a los servicios de certificación establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios de certificación, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo a la normativa aplicable y a las políticas propias de 5B destinadas a este fin.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso

5.1.1. Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

0-USO PÚBLICO

5B dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

5.1.2. Acceso físico

5B dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al Rack) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias de 5B donde se llevan a cabo procesos de criptográficos está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa de 5B a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.1.3. Electricidad y aire acondicionado

Las instalaciones de 5B disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

5.1.4. Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

0 - USO PÚBLICO

5.1.5. Prevención y protección de incendios

Las instalaciones y activos de 5B cuentan con sistemas automáticos de detección y extinción de incendios.

5.1.6. Almacenamiento de soportes

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos.

5.1.7. Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8. Copia de respaldo fuera de las instalaciones

5B utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

5.2. Controles de procedimientos

5B garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de 5B ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

0- USO PUBLICO

5.2.1. Funciones fiables

5B ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Administrador de Sistemas**: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Administrador de CA**: Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA:** Responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.
- **Operador de Información:** Persona encargada de identificar y verificar la autenticidad de las personas que solicitan un certificado de firma electrónica avanzada, así como registrar la información correcta y vigente de las personas en la herramienta tecnológica que se destine para ese propósito.
- **Operador de Registro:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor y emitir certificados digitales.
- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de 5B. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, 5B implementa criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

5.2.2. Número de personas por tarea

5B garantiza al menos dos personas para realizar las tareas relativas a la generación, recuperación y back-up de la clave privada de las Autoridades de Certificación. Igual criterio se aplica para la ejecución de tareas de emisión y activación de certificados y claves privadas de las Autoridades

0 - USO PÚBLICO

de Certificación, y en general cualquier manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

5.2.3. Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

5.2.4. Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:

- Las tareas propias del rol de Auditor serán incompatibles con la operación y administración de sistemas, y en general aquellas dedicadas a la prestación directa de los servicios electrónicos de confianza.
- Emisión y revocación de certificados, serán tareas incompatibles con la Administración y operación de los sistemas.
- La administración y operación de los sistemas y las CAs, serán incompatibles entre sí.

5.2.5. Sistema de gestión PKI

El sistema de PKI se compone de los siguientes módulos:

- Componente/módulo de gestión de la Autoridad de Certificación Subordinada.
- Componente/módulo de gestión de la Autoridad de Registro.
- Componente/módulo de gestión de solicitudes.
- Componente/módulo de gestión de claves (HSM).
- Componente/módulo de bases de datos.
- Componente/módulo de gestión de CRL.
- Componente/módulo de gestión de la Autoridad de Validación (servicios de OCSP).

5.3. Controles de personal

O-USO PÚBLICO

5.3.1. Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal está cualificado y/o ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

5B se asegura de que el personal de registro es confiable para realizar las tareas de registro. El Operador de Registro recibe formación para realizar las tareas de validación de las peticiones.

En general, 5B retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

5B no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación **hasta donde permita la legislación aplicable**, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales.
- Referencias profesionales.

5.3.2. Procedimientos de investigación de historial

5B, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

0-USO PÚBLICO

5.3.3. Requisitos de formación

5B forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son revisados periódicamente, y son actualizados para su mejor y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de 5B.
- Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4. Requisitos y frecuencia de actualización formativa

5B, actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

5.3.5. Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6. Sanciones para acciones no autorizadas

5B dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

0 - USO PUBLICO

5.3.7. Requisitos de contratación de profesionales

Las personas designadas para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por 5B. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían dar lugar a la separación de las funciones fiables, una vez evaluados.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la Declaración de Prácticas de Certificación, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, el Prestador de Servicios de Certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a 5B.

5.3.8. Suministro de documentación al personal

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal interno y externo en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

5B produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la autoridad de certificación a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la autoridad de certificación.
- Encendido y apagado de la aplicación de la autoridad de certificación.
- Cambios en los detalles de la autoridad de certificación y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.

0-USO PÚBLICO

- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona natural identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada del Prestador de Servicios de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

5.4.2. Frecuencia de tratamiento de registros de auditoría

5B revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

5B mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.

0 - USO PÚBLICO

- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3. Período de conservación de registros de auditoría

5B almacena la información de los logs durante un periodo de entre 1 y 10 años, en función del tipo de información registrada.

5.4.4. Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la autoridad de certificación.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5. Procedimientos de copia de respaldo

5B dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

5B tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6. Localización del sistema de acumulación de registros de auditoría

La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados,

0-USO PÚBLICO

además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7. Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8. Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de 5B.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo al procedimiento interno que previsto para este fin.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

5.5. Archivos de informaciones

5B, garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1. Tipos de registros archivados

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por 5B:

- Todos los datos de auditoría de sistema.
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Autoridad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.

0-USO PÚBLICO

- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 5.4
- Información de solicitudes de certificación.
- Evidencias aportadas para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

5B será responsable del correcto archivo de todo este material.

5.5.2. Período de conservación de registros

5B archiva los registros especificados anteriormente durante al menos 10 años, o el período que establezca la legislación vigente.
En particular, los registros de certificados revocados estarán accesibles para su libre consulta durante al menos 10 años o el periodo que establezca la legislación vigente desde su cambio de estado.

5.5.3. Protección del archivo

5B protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

5B asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

5.5.4. Procedimientos de copia de respaldo

5B dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

5B como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

0 - USO PÚBLICO

5.5.5. Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP.

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6. Localización del sistema de archivo

5B dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7. Procedimientos de obtención y verificación de información de archivo

5B dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. 5B proporciona la información y medios de verificación al auditor.

5.6. Renovación de claves

Con anterioridad a que el uso de la clave privada de la Autoridad de Certificación caduque, será realizado un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha Autoridad de Certificación. Se generará una nueva Autoridad de Certificación Intermedia con una clave privada nueva y un nuevo DN. El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

Alternativamente, en el caso de Autoridades de Certificación subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves, no resultando aplicable el procedimiento antes descrito.

5.7. Compromiso de claves y recuperación de desastre

5.7.1. Procedimientos de gestión de incidencias y compromisos

5B ha desarrollado políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones, asegurando los servicios críticos de revocación y publicación del estado de los certificados.

0 - USO PÚBLICO

5.7.2. Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo a las políticas de seguridad y gestión de incidentes de 5B, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de 5B.

5.7.3. Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de 5B, se activarán los procedimientos de compromiso de claves de acuerdo a las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

5.7.4. Continuidad del negocio después de un desastre

5B restablecerá los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el plan de incidencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

5B dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

5.8. Terminación del servicio

5B asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación. En este sentido, 5B garantiza un mantenimiento continuo de los registros definidos indicados en esta Declaración de Prácticas de Certificación.

No obstante lo anterior, si procede 5B ejecutará todas las acciones que sean necesarias para transferir a un tercero, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta Declaración de Prácticas de Certificación o la previsión legal que corresponda.

Antes de terminar sus servicios, 5B desarrolla un plan de terminación, con las siguientes provisiones:

0-USO PÚBLICO

- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otros Prestadores de Servicios de Certificación con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de 5B en la prestación de servicios de certificación.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios sino pudiera mantenerlo.
- Destruirá o deshabilitará para su uso las claves privadas de 5B como Prestador de Servicios de Certificación.
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.
- Comunicará al Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, con una antelación mínima de noventa (90) días, el cese de su actividad y el destino de los certificados especificando si se transfiere la gestión y a quién o si se extinguirá su vigencia.
- Comunicará, también al Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, la apertura de cualquier proceso concursal que se siga contra 5B, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

0 - USO PUBLICO

6. Controles de seguridad técnica

5B emplea 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.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves de la autoridad de certificación intermedia "5B CA1" es creada por la autoridad de certificación raíz "UANATACA ROOT 2016" de acuerdo con los procedimientos de ceremonia de 5B en coordinación con UANATACA S.A. Prestador de Servicios de Confianza Cualificados de acuerdo a la regulación de la Unión Europea, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por 5B.

Para la generación de la clave de las autoridades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones FIPS 140-2 level 3 y Common Criteria EAL4+.

UANATACA ROOT 2016	4.096 bits	25 años
5B CA1	4.096 bits	13 años
- Certificados de entidad final	2.048 bits	Hasta 3 años

6.1.1.1. Generación del par de claves del firmante

Las claves del firmante pueden ser generadas por él mismo mediante dispositivos hardware y/o software autorizados por 5B. Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.2. Envío de la clave privada al firmante

Los certificados son emitidos en dispositivos seguros de creación de firma la clave privada se genera y se almacena debidamente protegida en el interior de dicho dispositivo, garantizando el control exclusivo de la clave por parte del usuario

USO PÚBLICO

En certificados que utilizan un HSM Centralizado para la generación de las claves como dispositivo seguro de creación de firma, la clave privada se genera en un área privada del firmante en un HSM remoto. Las credenciales de acceso a la clave privada son introducidas por el propio firmante, no siendo almacenadas ni susceptibles de capacidad de deducción o intercepción por el sistema de generación y custodia remota. La clave privada no se envía al firmante, es decir, nunca abandona el entorno de seguridad que garantiza el control exclusivo de la clave privada por parte del firmante.

6.1.3. Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al prestador de servicios de certificación es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por 5B.

6.1.4. Distribución de la clave pública del prestador de servicios de certificación

Las claves de 5B son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.
Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las Autoridades de Certificación Raíz y Subordinada estarán a disposición de los usuarios en la página web de 5B.

6.1.5. Tamaños de claves

- La longitud de las claves de la Autoridad de Certificación raíz es de 4096 bits.
- La longitud de las claves de las Autoridad de Certificación subordinadas es de 4096 bits.
- La longitud de las claves de los Certificados de Entidad final es de 2048 bits.

6.1.6. Generación de parámetros de clave pública

La clave pública de la Autoridades de Certificación raíz, subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

0 - USO PÚBLICO

6.1.7. Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096 bits
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

6.1.8. Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

6.1.9. Propósitos de uso de claves

Los usos de las claves para los certificados de las Autoridades de Certificación son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final son exclusivamente para la firma electrónica, el no repudio y cifrado de datos.

6.2. Protección de la clave privada

6.2.1. Estándares de módulos criptográficos

En relación a los módulos que gestionan claves de 5B y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores y por la normativa legalmente aplicable.

6.2.2. Control por más de una persona (n de m) sobre la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la autoridad de certificación. En el caso de esta Declaración de Prácticas de Certificación, en concreto existe una política de **3 de 6** personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3. Depósito de la clave privada

5B no almacena copias utilizables por medios propios de las claves privadas de los firmantes.

0-USO PÚBLICO

6.2.4. Copia de respaldo de la clave privada

5B realiza copia de backup de las claves privadas de las autoridades de certificación que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Claves generadas en Dispositivo Seguro de Creación de Firma: no se puede realizar backups de las claves, ya que no es posible su exportación del dispositivo.

Claves generadas en HSM Centralizado: Sólo es posible realizar backups de un blob cifrado con la clave Security World del HSM utilizado, siendo imposible su descifrado sin el uso de las credenciales que sólo el titular del certificado conoce.

6.2.5. Archivo de la clave privada

Las claves privadas de las autoridades de certificación son archivadas por un periodo de **10 años** después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

Solo en caso de certificados de cifrado, el suscriptor podrá almacenar la clave privada el tiempo que crea oportuno. En este caso 5B también guardará copia de la clave privada asociada al certificado de cifrado.

5B no genera ni archiva claves de certificados, emitidas en software.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción de 5B.

6.2.7. Método de activación de la clave privada

Las claves privadas del Prestador de Servicios de Certificación se almacenan cifradas en los módulos criptográficos de producción de 5B.

0 - USO PÚBLICO

6.2.8. Método de desactivación de la clave privada

La clave privada de 5B se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la autoridad de certificación se activan por un proceso de m de n (3 de 6).

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC.

6.2.9. Método de destrucción de la clave privada

Para la desactivación de la clave privada de 5B se seguirán los pasos descritos en el manual correspondiente.

6.2.10. Clasificación de módulos criptográficos

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de 5B. Para la eliminación se seguirán los pasos descritos en el manual correspondiente. Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante se podrán destruir mediante el borrado de las mismas.

6.2.11. Clasificación de módulos criptográficos

Ver la sección 6.2.1

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

5B archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de este documento.

0-USO PÚBLICO

6.3.2. Períodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

Como excepción y en caso de existir, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de 5B son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada.

Asimismo, 5B genera de forma segura los datos de activación.

6.4.2. Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de certificación raíz y intermedias, están protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una o varias contraseñas lo más completas y complejas posible. El firmante debe recordar dicha(s) contraseña(s).

6.5. Controles de seguridad informática

5B emplea sistemas fiables para ofrecer sus servicios de certificación. El Prestador de Servicios de Certificación ha realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, 5B aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

0-USO PÚBLICO

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

6.5.1. Requisitos técnicos específicos de seguridad informática

Cada servidor del Prestador de Servicios Certificación incluye las siguientes funcionalidades:

- Control de acceso a los servicios de las Autoridades de Certificación intermedias y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor, de las Autoridades de Certificación subordinadas y datos de auditoria.
- Auditoria de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de las Autoridades de Certificación subordinadas.
- Mecanismos de recuperación de claves y del sistema de las Autoridades de Certificación subordinadas.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de Infraestructura de Clave Pública (PKI), protección física y procedimientos.

6.5.2. Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por 5B son fiables.

0 - USO PÚBLICO

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.6.2. Controles de gestión de seguridad

5B desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos, son actualizados después de su aprobación de acuerdo a las políticas del Prestador de Servicios de Certificación. En la realización de esta función dispone de un plan de formación anual.

5B exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios de certificación.

6.6.2.1. Clasificación y gestión de información y bienes

5B mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de 5B detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: SIN CLASIFICAR, USO INTERNO y CONFIDENCIAL.

6.6.2.2. Operaciones de gestión

5B dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad de 5B se desarrolla en detalle el proceso de gestión de incidencias.

0-USO PÚBLICO

5B tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

6.6.2.3. Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Planificación del sistema

5B mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Reportes de incidencias y respuesta

5B dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

Procedimientos operacionales y responsabilidades

5B define actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.4. Gestión del sistema de acceso

5B realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

AC General

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- 5B dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.

0 - USO PÚBLICO

- 5B dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal de 5B es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de 5B.

Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de 5B.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.5. Gestión del ciclo de vida del hardware criptográfico

5B se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

5B registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

5B realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

0 - USO PÚBLICO

La clave privada de firma de 5B almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de 5B, así como sus modificaciones y actualizaciones son documentadas y controladas.

Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7. Controles de seguridad de red

5B protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8. Controles de ingeniería de módulos criptográficos

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas de 5B son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3.

6.9. Fuentes de Tiempo

5B tiene un procedimiento de sincronización de tiempo coordinado vía NTP, que accede a dos servicios independientes:
La primera sincronización es con un servicio basado en antenas y receptores GPS que permite un nivel de confianza de STRATUM 1 (con dos sistemas en alta disponibilidad).

0 - USO PÚBLICO

La segunda dispone de una sincronización complementaria, vía NTP, con el Real Instituto y Observatorio de la Armada (ROA) de España.

6.10. Cambio de estado de un Dispositivo Seguro de Creación de Firma

5B en el caso de modificación del estado de la certificación de los dispositivos seguros de creación de firma procederá de la siguiente manera:

1. 5B dispone de una lista de varios dispositivos seguros de creación de firma certificados, así como una estrecha relación con proveedores de dichos dispositivos, con el fin de garantizar alternativas a posibles pérdidas de estado de certificación de dispositivos seguros de creación de firma.
2. En el supuesto de finalización del periodo de validez o pérdida de la certificación, 5B no utilizará dichos dispositivos seguros de creación de firma para la emisión de nuevos certificados digitales, bien sea en nuevas emisiones como eventualmente en posibles renovaciones.
3. Procederá de inmediato a cambiar a de dispositivos seguros de creación de firma con certificación válida de acuerdo a la normativa legalmente aplicable.
4. En el supuesto caso que un dispositivo seguro de creación de firma haya demostrado no haberlo sido nunca, por falsificación o cualquier otro tipo de fraude, 5B procederá de inmediato a comunicárselo a sus clientes y al ente regulador, revocar los certificados digitales emitidos en estos dispositivos y reemplazarlos emitiéndolos en dispositivos seguros de creación de firma válidos

0 - USO PÚBLICO

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de certificado

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

7.1.1. Número de versión

5B emite certificados X.509 Versión 3

7.1.2. Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de políticas que son accesibles desde la página web de 5B (https://www.5b.com.gt/identidad-digital.php).

De esta forma se permite mantener unas versiones más estables de la Declaración de Prácticas de Certificación y desligarlos de los frecuentes ajustes en los perfiles.

7.1.3. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

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

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

7.1.5. Restricción de los nombres

Los nombres contenidos en los certificados están restringidos a “Distinguished Names” X.500, que son únicos y no ambiguos.

0 - USO PÚBLICO

7.1.6. Identificador de objeto (OID) de los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1

7.2. Perfil de la lista de revocación de certificados

7.2.1. Número de versión

Las CRL emitidas por 5B son de la versión 2.

7.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960.

0 - USO PÚBLICO

8. Auditoría de conformidad

5B ha comunicado el inicio de su actividad como prestador de servicios de certificación al Registro de Prestadores de Servicios de Certificación y se encuentra sometida a las revisiones de control que este organismo considere necesarias de acuerdo a la normativa legalmente aplicable.

8.1. Frecuencia de la auditoría de conformidad

5B lleva a cabo una auditoría de conformidad de acuerdo a la periodicidad y condiciones que establece el Registro de Prestadores de Servicios de Certificación a través de la correspondiente normativa técnica y la correspondiente programación anual, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

8.2. Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

8.3. Relación del auditor con la entidad auditada

El Registro de Prestadores de Servicios de Certificación es un organismo del Estado altamente especializado en la materia, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con 5B.

8.4. Listado de elementos objeto de auditoría

La auditoría verifica respecto a 5B:

a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
b) Que la entidad cumple con los requerimientos de la Declaración de Prácticas de Certificación y otra documentación vinculada con la emisión de los distintos certificados digitales.
c) Que la Declaración de Prácticas de Certificación y demás documentación jurídica vinculada, se ajusta a lo acordado por 5B y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información

0 - USO PÚBLICO

En particular, los elementos objeto de auditoría serán los siguientes:

a) Procesos de las autoridades de certificación, autoridades de registro y elementos relacionados.
b) Sistemas de información.
c) Protección del centro de proceso de datos.
d) Documentos.

8.5. Acciones a emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solventen dichas deficiencias.

Si 5B es incapaz de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, se comunica inmediatamente al Comité de Seguridad de 5B que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la Autoridad de Certificación y regenerar la infraestructura.
- Terminar el servicio de la Autoridad de Certificación.
- Otras acciones complementarias que resulten necesarias.

0-USO PÚBLICO

8.6. Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Seguridad de 5B.

0 - USO PÚBLICO

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifa de emisión o renovación de certificados

5B puede establecer una tarifa por la emisión o por la renovación de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2. Tarifa de acceso a certificados

5B no ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3. Tarifa de acceso a información de estado de certificado

5B no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4. Tarifas de otros servicios

Sin estipulación.

9.1.5. Política de reintegro

Sin estipulación.

9.2. Capacidad financiera

5B dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401-1 7.12 c), en relación a la gestión de la finalización de los servicios y plan de cese.

9.2.1. Cobertura de seguro

5B dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo a la normativa vigente aplicable.

0-USO PÚBLICO

9.2.2. Otros activos

Sin estipulación.

9.2.3. Cobertura de seguro para suscriptores y terceros que confían en certificados

5B dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, para los servicios de certificación de acuerdo con la normativa legalmente aplicable.

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por 5B:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por el Prestador de Servicios de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Planes de seguridad.
- Documentación de operaciones, archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

9.3.2. Informaciones no confidenciales

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por el Prestador de Servicios de Certificación.
- El nombre y los apellidos de la persona natural identificada en el certificado.

0 -USO PÚBLICO

- La dirección de correo electrónico de la persona natural identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (CRLs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

9.3.3. Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4. Divulgación legal de información

5B divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

5B indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5. Divulgación de información por petición de su titular

5B incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona natural identificada en el certificado, directamente a los mismos o a terceros.

0 - USO PÚBLICO

9.3.6. Otras circunstancias de divulgación de información

Sin estipulación.

9.4. Protección de datos personales

5B ha documentado en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad y organizativos, con el fin de garantizar que todos los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

A continuación, se detalla toda la información necesaria con respecto al tratamiento de datos personales realizado por 5B:

Responsable del tratamiento
Transacciones y Transferencias S.A.
NIT: 44581181
Dirección: 15 avenida 17-40 zona 13, edificio Tetra Center Torre I, 4to nivel. Guatemala, Guatemala
Teléfono: (+502) 24207220
Correo electrónico: fid@5b.com.gt

Finalidad del tratamiento
5B trata los datos de carácter personal facilitados para llevar a cabo los servicios electrónicos solicitados, concretamente la expedición de certificados electrónicos, todo ello de acuerdo con lo previsto en la Declaración de Prácticas de Certificación (DPC) de 5B, la cual se encuentra disponible en el siguiente enlace: https://www.5b.com.gt/identidad-digital.php.

Las finalidades de tratamiento de datos relativos al SERVICIO son las siguientes:

- Identificación de los suscriptores y/o firmantes de los certificados electrónicos.
- Expedición y gestión de certificados electrónicos.
- Gestión del ciclo de vida del certificado (suspensión, renovación, reactivación y revocación).
- Comunicaciones relativas al servicio.
- Custodia y mantenimiento del archivo relativo al certificado electrónico.

0- USO PÚBLICO

- Gestión administrativa, contable y de facturación derivada de la contratación.

5B informa que los datos personales facilitados únicamente se tratarán para las finalidades anteriormente descritas y no serán tratados de manera incompatible con las mismas.

Legitimación del tratamiento

De acuerdo con las finalidades de tratamiento indicadas, la base legal para el tratamiento de los datos personales de los usuarios es:

- La legitimación del tratamiento para la Prestación de Servicios de Certificación es la ejecución del contrato de los servicios solicitados, donde el usuario es parte del mismo.

- La legitimación del tratamiento para atender las consultas y solicitudes se basa en el consentimiento del interesado, el cual lo presta expresa e inequívocamente, mediante acción positiva y previa al envío, al aceptar las condiciones y la política de privacidad.

Datos tratados y conservación

Las categorías de datos personales tratados por 5B, a título enunciativo pero no limitativo, comprenden:

- Datos identificativos: nombre, apellidos y número oficial de identidad.

- Datos profesionales: organización, departamento y/o cargo.

- Datos de contacto: dirección postal, correo electrónico y número de teléfono.

- Datos relativos a la identidad o identificación de los usuarios: fotografías y/o cuando corresponda el patrón biométrico facial, con la finalidad de poder llevar a cabo el proceso de vídeo identificación de 5B.

Los datos personales se conservarán hasta la finalización de la relación contractual y posteriormente, durante los plazos legalmente exigidos acorde a cada caso, tal y como se encuentran definidos en la presente Declaración de Prácticas de Certificación.

Transferencia de datos

Los datos personales no se cederán a terceros salvo obligación legal, o sin autorización de los usuarios.

Como excepción a lo anterior, los datos pueden ser puestos a disposición de terceros, con motivo de la prestación de servicios contratados por el usuario (por ejemplo, proveedores de alojamiento

0-USO PÚBLICO

de datos (CPD), servicios de apoyo en la identificación, empresas del grupo, etc.), todo ello al amparo del correspondiente contrato que corresponda, garantizando en todo momento unas medidas de seguridad idóneas que aseguren la debida protección de los datos personales de los usuarios.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

Únicamente 5B goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2. Propiedad de la Declaración de Prácticas de Certificación

Únicamente 5B goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

9.5.3. Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona natural identificada en el certificado, conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido (DN) del certificado, formado por las informaciones especificadas en la sección 3.1.1.

9.5.4. Propiedad de claves

Los pares de claves son propiedad de los suscriptores de los certificados.

0 - USO PÚBLICO

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6. Obligaciones y responsabilidad civil

9.6.1. Obligaciones de 5B

5B garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la Declaración de Prácticas de Certificación, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo a las indicaciones contenidas en este documento.

5B presta los servicios de certificación conforme con esta Declaración de Prácticas de Certificación.

Con anterioridad a la emisión y entrega del certificado al suscriptor, 5B informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia las políticas y prácticas de certificación de 5B como Prestador de Servicios de Certificación.

9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en certificados

5B, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

5B, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por el Prestador de Servicios 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 Declaración de Prácticas de Certificación.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

5B, como mínimo, garantizará al tercero que confía en el certificado:

0-USO PÚBLICO

- 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 identificado en el mismo y que el certificado ha sido aceptado, de acuerdo a las previsiones de esta Declaración de Prácticas de Certificación.
- 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 Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, 5B garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado de firma electrónica avanzada, de acuerdo con el artículo 46 del Decreto 47-2008 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona natural identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad del Prestador de Servicios de Certificación, con los límites que se establezcan.

9.6.3. Rechazo de otras garantías

5b rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4. Responsabilidades y Obligaciones del PSC

5B como prestador de servicios de certificación:

- Se asegura de la emisión certificados conforme a lo solicitado o acordado con el firmante/suscriptor.
- Implementa de sistemas de seguridad para garantizar la emisión y creación de firmas electrónicas avanzadas, la conservación y archivo de certificados y documentos en soporte de mensaje de datos.
- Garantiza la protección, confidencialidad y debido uso de la información suministrada por el firmante.
- Garantiza la prestación permanente del servicio de entidad de certificación en los términos previstos en la Ley.

0-USO PÚBLICO

- Procura la atención oportuna de las solicitudes y reclamaciones hechas por los firmantes.
- Suministra la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas electrónicas y certificados emitidos y en general sobre cualquier comunicación electrónica que se encuentre bajo su custodia y administración.
- Notifica al RPSC del inicio de sus operaciones cumplimiento los extremos legales y también de cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. Igualmente permite y facilita la realización de las auditorías por parte del Registro de Prestadores de Servicios de Certificación.
- Elabora las políticas y manuales que definen las relaciones con el firmante y la forma de prestación del servicio. En este sentido, cuenta con reglas como la presente declaración de prácticas de certificación objetivas y no discriminatorias que se comunican a los usuarios cuando corresponde en idioma español, conforme al artículo 13.a) del acuerdo gubernativo No. 135-2009.
- Lleva un registro de los certificados que se conservan por al menos diez años desde la fecha de la emisión inicial de los mismos.
- Mantiene un Plan de Cese de Actividades conforme a la normativa legalmente aplicable. En este sentido, está obligado a solicitar la cancelación de su inscripción en el Registro de Prestadores de Servicios de Certificación en los plazos previstos en la normativa aplicable, la cual se comunicará igualmente a los usuarios.
- Publica en su sitio web todas las resoluciones del RPSC que le afectan.
- Comprueba fehacientemente la identidad de los solicitantes en el proceso de otorgamiento de los certificados.
- Resguarda los datos de firma que corresponden a su propio certificado, asumiendo responsabilidad por su control.
- Paga los aranceles fijados para la prestación de los servicios.
- Cualquier otra aplicable por mandato de la Ley.

9.6.5. Cláusulas de indemnidad

9.6.5.1. Cláusula de indemnidad de suscriptor

5B incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne al Prestador de Servicios de Certificación 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:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto al Prestados de Servicios de Certificación o a cualquier persona que confía en el certificado.

U-USO PÚBLICO

- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2. Cláusula de indemnidad de tercero que confía en el certificado

5B incluye en sus políticas de certificación, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne al Prestador de Servicios de Certificación 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.

9.6.6. Caso fortuito y fuerza mayor

5B incluye en sus políticas de certificación cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7. Ley aplicable

5B establece, en el contrato de suscriptor y las políticas de certificación, que la ley aplicable a la prestación de los servicios de certificación, es la Ley guatemalteca.

9.6.8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

5B establece, en el contrato de suscriptor, y en las políticas de certificación, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- 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. A este efecto, el Prestadores de Servicios de Certificación vela porque, al menos los

0-USO PUBLICO

requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.

- 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.

9.6.9. Cláusula de jurisdicción competente

5B establece, en el contrato de suscriptor y en las políticas de certificación, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces guatemaltecos.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10. Resolución de conflictos

5B establece, en el contrato de suscriptor, y en las políticas de certificación, los procedimientos de mediación y resolución de conflictos aplicables.

0 - USO PÚBLICO

10. Anexo I – Acrónimos y glosario

AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
RA	Autoridad de Registro
CP	Certificate Policy
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DCCF	Dispositivo Cualificado de Creación de Firma
QSCD	Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol
NTP	Network Time Protocol. Protocolo. Protocolo de internet para sincronizar relojes de sistemas informáticos.
Blob	Binary Large Objects. Objetos Binarios Grandes
Indemnidad	Estado o situación libre o exenta de daños.
Ignífugo/a	Que no se inflama ni propaga la llama o el fuego

USO PÚBLICO

RESPONSABLE DE ADMINISTRACIÓN

Este documento es administrado por el Oficial de Seguridad de la Información de Transacciones y Transferencias S.A.

RESPONSABLE DE CUMPLIMIENTO

Todo el personal involucrado en el proceso, tanto personal interno y externo debe cumplir con lo establecido en el presente documento

SANCION

N/A

0 - USO PÚBLICO