DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE SELLADO DE TIEMPO

Presentado por:

PBS El Salvador

Marzo 2022

Carlos Molina
Gerente PV & SI
+503 2239 3000
Carlos.molina@grouppbs.com

Información general

Control documental

Clasificación de seguridad:	**Público**
Versión:	**1**
Fecha edición:	**23/03/2022**
Fichero:	**PBS_TSA_ES_v1.docx**

Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: Albert Borrás Fecha: 23/03/2022	Nombre: Carlos Molina Fecha: 23/03/2022	Nombre: Fecha: 23/03/2022

Control de versiones

Versión	Partes que cambian	Descripción cambio	Autor cambio	Fecha cambio
1.0	Original	Creación del documento	Albert Borrás	23/03/2022

Contenido

1. Introducción

1.1 Presentación

Este documento constituye la Declaración de Prácticas de Certificación para el Servicio de expedición de sellos de tiempo electrónicos de *PRODUCTIVE BUSINESS SOLUTIONS EL SALVADOR, S.A. DE CV,* en lo sucesivo PBS.

1.2 Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación de Sellado de Tiempo de PRODUCTIVE BUSINESS SOLUTIONS EL SALVADOR, S.A. DE CV".

El servicio de sellado de tiempo electrónico de PBS se identifica con el OID: 1.3.6.1.4.1.57626.4.

1.3 Participantes en los servicios de certificación

1.3.1 Proveedor de Servicios de certificación

El Proveedor de Servicios Electrónicos de Certificación, en adelante "*PSC*" es la persona, natural o jurídica, que presta uno o más servicios de Certificación. PBS es un Proveedor de Servicios electrónicos de certificación, que actúa de acuerdo con la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento, Decreto 534 de Ley de Acceso a la Información Pública,así como las normas técnicas ETSI aplicables a la expedición de sellos de tiempo electrónicos, principalmente EN 319 421, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

1.3.2 Autoridad de Sellado de Tiempo

La Autoridad de Sellado de Tiempo, en lo sucesivo "*TSA*" es el tercero de confianza que presta el servicio de expedición de sellos de tiempo electrónicos. PBS es el Proveedor de Servicios de Certificación que actúa como Autoridad de Sellado de Tiempo para la expedición de sellos de tiempo electrónicos cualificados.

1.3.3 Suscriptores del servicio de certificación

Los suscriptores son los usuarios finales de los sellos de tiempo electrónicos cualificados expedidos por PBS. Los suscriptores del servicio pueden ser:

- Empresas, entidades, corporaciones u organizaciones que solicitan a PBS (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo.
- Las personas físicas que solicitan el servicio para sí mismas.

El suscriptor del servicio electrónico de certificación es, por tanto, el cliente del Proveedor de Servicios de Certificación.

1.3.4 Partes usuarias

Las partes usuarias son las personas y organizaciones que reciben los sellos de tiempo electrónicos cualificados.

Como paso previo a confiar en los sellos de tiempo, las partes usuarias deben verificarlos, como se establece en esta Declaración de Prácticas de Certificación.

1.3.5 Proveedor de Servicios de Infraestructura de Clave Pública

PBS y "Uanataca, S.A." han suscrito un contrato de prestación de servicios de tecnología en el que Uanataca, S.A., proveerá la infraestructura de clave pública (PKI) que sustenta el servicio de certificación de PBS. Así mismo Uanataca, S.A., pone a disposición de PBS el personal técnico necesario para correcto desempeño de las funciones fiables propias de un Proveedor de Servicios de Certificación.

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

Asimismo, se informa que Uanataca, S.A., es un Proveedor de Servicios de Certificación cuya PKI se somete a auditorías anuales para la evaluación de la conformidad de prestadores de servicios de certificación de acuerdo con la normativa aplicable, bajo las normas:

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

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

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

1.4 Uso del servicio de Sellado de Tiempo

1.4.1 Usos permitidos

El Servicio de Sellado de Tiempo expide sellos de tiempo con el fin de probar que una serie de datos han existido y no han sido alterados a partir de un instante específico en el tiempo. Su uso se limita a las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios.

1.4.2 Límites y prohibiciones de uso

El Servicio de Sellado de Tiempo no se utilizará para fines distintos de los especificados en el presente documento. Del mismo modo, el servicio deberá emplearse únicamente de acuerdo con la regulación aplicable.

1.5 Administración de la política

1.5.1 Organización que administra el documento

Productive Business Solutions El Salvador, S.A. de CV
Final Blvd Santa Elena y Blvd Orden de Malta
Edificio Xerox, Antiguo Cuscatlan, La libertad

1.5.2 Datos de contacto de la organización

Productive Business Solutions El Salvador, S.A. de CV
Final Blvd Santa Elena y Blvd Orden de Malta
Edificio Xerox, Antiguo Cuscatlan, La libertad
Correo electrónico: info.sv@grouppbs.com
Teléfono: +503 2239 3000
Página web: [https://www.pbssoluciones.com]

1.5.3 Procedimientos de gestión del documento

El sistema documental y de organización de PBS 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.

2. Publicación y preservación

2.1 Depósito

PBS custodia de manera segura todos los sellos de tiempo generados como mínimo durante 15 años. Asimismo, dispone de un Depósito, en el que se publican las informaciones relativas al servicio de expedición de sellos de tiempo electrónicos cualificados.

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 PBS, éste realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo de acuerdo con los plazos y procedimientos establecidos con respecto de la continuidad del negocio.

2.2 Publicación de información del Proveedor de Servicios de certificación

PBS publica las siguientes informaciones, en su Depósito:

- La Declaración de Prácticas de Certificación de Sellado de Tiempo.
- El texto de divulgación con respecto del servicio.
- La clave pública del certificado de sello de tiempo electrónico.
- Referencias a los mecanismos de validación de los sellos de tiempo.

2.3 Frecuencia de publicación

La información del Proveedor de Servicios de Certificación, incluyendo el texto de divulgación y la Declaración de Prácticas de Certificación de Sellado de Tiempo, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación de Sellado de Tiempo se rigen por lo establecido en el procedimiento de gestión de este documento y de acuerdo la normativa de aplicación.

2.4 Control de acceso

PBS 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.

PBS 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.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3. Identificación y autenticación

3.1 Registro inicial

3.1.1 Tipos de nombres

Los Certificados electrónicos utilizados en el servicio de expedición de sellos de tiempo electrónicos, son denominados Certificados de la Unidad de Sellado de tiempo, en adelante "Certificado/s de TSU", contienen un nombre distintivo (DN o distinguished name) conforme al estándar X.501 en el campo Subject, incluyendo un componente Common Name (CN=).

Los Certificados de TSU son emitidos por PBS como Autoridad de Certificación, son certificados electrónicos de acuerdo con lo establecido en la legislación de El Salvador, conformada por el Decreto Legislativo No. 133 de Ley de Firma Electrónica y su correspondiente reglamento.

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.

3.1.3 Empleo de anónimos y seudónimos

N/A

3.1.4 Interpretación de formatos de nombres

PBS cumple con los requisitos del estándar X500.

3.1.5 Unicidad de los nombres

El nombre distintivo de los certificados de TSU será único.

3.2 Validación inicial de la identidad

N/A

3.3 Identificación y autenticación de solicitudes de renovación

N/A

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

N/A

4. Requisitos operacionales

4.1 Solicitud de emisión de sellos de tiempo

4.1.1 Legitimación para solicitar el servicio de sellado de tiempo

El solicitante o usuario del servicio de sellado de tiempo, sea persona natural o jurídica, puede realizar la solitud de emisión de sellos de tiempo mediante petición directa a PBS o bien a través de los servidores de TSA disponibles, que permiten el sellado de tiempo de los documentos que desee.

El solicitante o usuario del servicio de sellado de tiempo puede usar su propio aplicativo o software a través del protocolo definido en el RFC 3161 y conforme a la ETSI 319 422, todo ello conectándose a una dirección web y mediante unas credenciales proporcionadas por PBS.

Una vez que la solicitud ha sido aceptada y registrada y se han llevado a cabo las comprobaciones adecuadas, se genera la marca de tiempo y la envía al solicitante.

4.1.2 Procedimiento de alta y responsabilidades

PBS recibe solicitudes para el servicio de sellado de tiempo, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se realizan directamente a través de los sistemas informáticos de PBS.

4.2 Procesamiento de la solicitud

El solicitante presenta a través de los procedimientos establecidos, la solicitud del sello de tiempo para un documento electrónico directamente al servicio de sellado / servidor encargado del sellado. Se hace la petición se envía al documento, apuntando a la dirección correspondiente y se retorna sellado.

4.3 Emisión del sello de tiempo

Los sellos de tiempo electrónicos se generan automáticamente a través del sistema o del servidor encargado del servicio de sellado de tiempo. Tras la aprobación de la solicitud se procede a la emisión del sello de tiempo de forma segura y se pone a disposición del suscriptor.

Durante el proceso, PBS:

- 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.
- Indica la fecha y la hora en que se expidió un sello de tiempo.

4.4 Entrega y aceptación del certificado

La entrega y aceptación de los Certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de PBS como Autoridad de Certificación, todo ello disponible en la página web: https://www.pbssoluciones.com.

4.5 Uso del par de claves y del certificado

El Certificado de TSU únicamente se utiliza exclusivamente para el servicio de expedición de sellos de tiempo electrónicos.

4.6 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 dispuesto en la Declaración de Prácticas de Certificación y Texto divulgativo de PBS, como Autoridad de Certificación, todo ello disponible en la página web: https://www.pbssoluciones.com.

4.7 Revocación, suspensión o reactivación de certificados

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

La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible.

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

Los procedimientos de revocación, suspensión y reactivación de los Certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación de PBS como Autoridad de Certificación, todo ello disponible en la página web: https://www.pbssoluciones.com.

4.7.1 Causas de revocación de certificados

PBS procederá a la revocación de los Certificados de TSU cuando concurra alguna de las siguientes causas:

4.7.1.1 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.

4.7.1.2 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 Proveedor de Servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

b) Infracción, por PBS, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación de Sellado de Tiempo.

c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.

d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.

4.7.1.3 Otras circunstancias:

a) La terminación del servicio de certificación de PBS.

b) El uso del certificado que sea dañino y continuado para PBS. En este caso, se considera que un uso es dañino en función de los siguientes criterios:

I. La naturaleza y el número de quejas recibidas.
II. La identidad de las entidades que presentan las quejas.
III. La legislación relevante vigente en cada momento.
IV. La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

4.7.2 Causas de suspensión de un certificado

Los Certificados de TSU pueden ser suspendidos si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, PBS tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

4.7.3 Causas de reactivación de un certificado

Los Certificados de TSU pueden ser reactivados.

4.7.4 Quién puede solicitar la revocación, suspensión o reactivación

La revocación, suspensión o reactivación será solicitada por PBS.

4.7.5 Procedimientos de solicitud de revocación, suspensión o reactivación

El Procedimiento de solicitud de la revocación, suspensión y/o reactivación de los certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de PBS, como Autoridad de Certificación, todo ello disponible en la página web: https://www.pbssoluciones.com.

4.7.6 Plazo temporal de solicitud y procesamiento de la revocación, suspensión o reactivación

El Plazo temporal de la solicitud y del procesamiento de esta para la revocación, suspensión y/o reactivación de los certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de PBS, como Autoridad de Certificación, todo ello disponible en la página web: https://www.pbssoluciones.com.

4.7.7 Obligación de consulta de información de revocación o suspensión de certificados

Los terceros deben comprobar el estado de los sellos de tiempo electrónicos en los cuales desean confiar, para ello deberán consultar el estado del Certificado de TSU. Un método por el cual se puede verificar el estado de los certificados de TSU es consultando la Lista de Revocación de Certificados más reciente emitida por la Autoridad de Certificación de PBS responsable de la emisión de estos.

Las Listas de Revocación de Certificados o LRC se publican en la página web de PBS, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- http://crl1.uanataca.com/public/pki/crl/PBSCA1.crl
- http://crl2.uanataca.com/public/pki/crl/PBSCA1.crl

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP, a través de los siguientes enlaces:

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

4.7.8 Frecuencia de emisión de listas de revocación de certificados (LRCs)

PBS, Autoridad de Certificación emisora de los certificados de TSU emite una LRC al menos cada 24 horas.

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

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

4.7.9 Plazo máximo de publicación de LRCs

Las LRCs se publican en https://www.pbssoluciones.com y en las direcciones web indicadas, en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

4.7.10 Disponibilidad de servicios de comprobación en línea de estado de certificados

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

- https://www.pbssoluciones.com

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

- AUTORIDAD DE CERTIFICACIÓN RAÍZ EL SALVADOR:
  - http://crl1.firmaelectronica.minec.gob.sv/crl/arl_minec.crl
  - http://crl2.firmaelectronica.minec.gob.sv/crl/arl_minec.crl
- PBS EL SALVADOR CA1:

- http://crl1.uanataca.com/public/pki/crl/PBSCA1.crl
- http://crl2.uanataca.com/public/pki/crl/PBSCA1.crl

4.7.11 Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los Certificados de TSU antes de confiar en los sellos de tiempo electrónicos de PBS.

4.7.12 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de los Certificados de TSU de PBS 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 PBS, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.8 Finalización de la suscripción

N/A

4.9 Depósito y recuperación de claves

4.9.1 Política y prácticas de depósito y recuperación de claves

N/A

4.9.2 Política y prácticas de encapsulado y recuperación de claves de sesión

N/A

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

5.1 Controles de seguridad física

PBS presta sus servicios de Certificación a través de la infraestructura de clave pública de UANATACA S.A, la cual ha establecido 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 Certificación.

En concreto, la política de seguridad aplicable a los servicios electrónicos 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 Proveedor de Servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios electrónicos de Certificación, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias 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.

5.2 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.

Se dispone de instalaciones que protegen físicamente la prestación de los servicios de certificación, así como la gestión de la validación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de estos.

5.2.1 Acceso físico

Se 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), debiendo accederse desde los niveles inferiores a los niveles superiores.

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

a) Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por circuito cerrado de televisión y su archivo.
b) 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.
c) Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.2.2 Electricidad y aire acondicionado

Las instalaciones 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.

5.2.3 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.

5.2.4 Prevención y protección de incendios

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

5.2.5 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.

5.2.6 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.

5.2.7 Copia de respaldo fuera de las instalaciones

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

5.3 Controles de procedimientos

Se garantiza que los 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 la Prestación de Servicios de Certificación ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.3.1 Funciones fiables

Se han 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
- Responsable de Seguridad: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de PBS. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.
- Operador de Sistemas: Responsable necesario juntamente con el Administrador de Sistemas del funcionamiento correcto del hardware y software soporte de la plataforma de certificación. El operador es responsable de los procedimientos de copia de respaldo y mantenimiento de las operaciones diarias de los sistemas.

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

5.3.2 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.

5.3.3 Roles que requieren separación de tareas

Las funciones fiables se establecen bajo el principio del mínimo privilegio, garantizado una segregación de funciones, de modo que la persona que ostente un rol no tenga un control total o especialmente amplio de todas las funciones de certificación, asegurando

el debido control y vigilancia, limitando así cualquier tipo de comportamiento fraudulento a nivel interno.

La concesión del mínimo privilegio para las funciones de confianza, se hará teniendo en cuenta el mejor desarrollo de la actividad y será lo más limitado posible, considerando la estructura organizativa en cada momento.

5.4 Controles de Personal

5.4.1 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.

En general, se 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.

PBS 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.

5.4.2 Procedimientos de investigación de historial

Antes de contratar a una persona o de que ésta acceda al puesto de trabajo, se realizan 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.

5.4.3 Requisitos de formación

PBS 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. 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.

5.4.4 Requisitos y frecuencia de actualización formativa

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

5.4.5 Secuencia y frecuencia de rotación laboral

N/A

5.4.6 Sanciones para acciones no autorizadas

PBS 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.

5.4.7 Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por PBS. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

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 Proveedor 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 PBS.

5.4.8 Suministro de documentación al personal

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

5.5 Procedimientos de auditoría de seguridad

5.5.1 Tipos de eventos registrados

Se producen y guardan 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 TSA 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 TSA.
- Encendido y apagado de la aplicación de la TSA.
- Cambios en los detalles de la TSA y/o sus claves.
- 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.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al servicio.
- Eventos relativos a la sincronización y recalibración del reloj.

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.

5.5.2 Frecuencia de tratamiento de registros de auditoría

Se procede a la revisión de los 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.

Se mantiene un sistema que permite garantizar:

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

5.5.3 Período de conservación de registros de auditoría

La información relativa a los logs se almacena durante un periodo de entre 1 y 15 años, en función del tipo de información registrada.

5.5.4 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.

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.

5.5.5 Procedimientos de copia de respaldo

Se dispone de un procedimiento adecuado de copia de seguridad de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de respaldo de los logs.

Se tiene implementado un procedimiento de copia de seguridad 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.

5.5.6 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 sellado de tiempo, 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.

5.5.7 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.

5.5.8 Análisis de vulnerabilidades

Los análisis de vulnerabilidades quedan cubiertos por los procesos de auditoría. Los mismos deben ser ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el 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.

5.6 Archivos de informaciones

5.6.1 Período de conservación de registros

Los registros especificados anteriormente son archivados durante al menos 15 años, o el período que establezca la legislación vigente.

5.6.2 Protección del archivo

El archivo está protegido 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.

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

5.6.3 Procedimientos de copia de respaldo

Se 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.

Como mínimo se realizan copias de respaldo incrementales diarias de todos sus documentos electrónicos y realizar copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, en los casos que exista la necesidad de guardar copia de documentos en papel, los mismos se almacenan en un lugar seguro.

5.6.4 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.

5.6.5 Localización del sistema de archivo

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

5.6.6 Procedimientos de obtención y verificación de información de archivo

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

5.7 Renovación de claves

Cada par de claves de los Certificados de TSU utilizados en el servicio de sellado de tiempo es únicamente asociado con el sistema que presta dicho servicio. Con anterioridad a que el uso de la clave privada de los Certificados de TSU caduque, se realizará un cambio de claves antes de la caducidad o revocación de las actuales.

5.8 Compromiso de claves y recuperación de desastre

5.8.1 Procedimientos de gestión de incidencias y compromisos

Se han desarrollado políticas de seguridad y continuidad del negocio que permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones.

5.8.2 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 con las políticas de seguridad y gestión de incidentes establecidas, que contemplan escalado, investigación y respuesta al incidente.

Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres.

5.8.3 Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso, se activarán los procedimientos de compromiso de claves de acuerdo con 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.

5.8.4 Continuidad del negocio después de un desastre

Se restablecerán los servicios críticos 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.

Se 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.

5.9 Terminación del servicio

PBS asegura que las posibles interrupciones a los suscriptores del servicio y a terceras partes son mínimas como consecuencia del cese de los servicios del Proveedor de Servicios de certificación. En este sentido, PBS garantiza un mantenimiento continuo de los registros definidos y por el tiempo establecido de acuerdo con la presente Declaración de Prácticas de Certificación de Sellado de Tiempo.

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

Antes de terminar sus servicios, PBS llevará a cabo un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- Informará a todos los Suscriptores del servicio, Terceros que confían y en general cualquier tercero con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 2 meses.
- Destruirá o deshabilitará para su uso las claves privadas encargadas del servicio de sellado de tiempo.
- 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.
- Comunicará al Organismo Supervisor Nacional que tenga atribuidas las competencias correspondientes, con una antelación mínima de 2 meses, el cese de su actividad.
- Comunicará, le comunicará la apertura de cualquier proceso concursal que se siga contra PBS, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6. Controles de seguridad técnica

En la Prestación de Servicios de Certificación se emplean sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves del Certificado de TSU son generadas por PBS como Autoridad de Certificación, de acuerdo con su Declaración de Prácticas de Certificación y su texto de divulgación, encontrándose disponibles en la página web: https://www.pbssoluciones.com .

Asimismo, se han seguido los procedimientos de ceremonia de claves, 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 PBS.

Para la generación de la clave del certificado de TSU se utilizan dispositivos con las certificaciones FIPS 140-2 level 3 y Common Criteria EAL4+.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

Certificados de la Unidad de Sello de tiempo	2.048 bits	Hasta 5 años

6.1.2 Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al Proveedor de Servicios electrónicos de certificación es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por PBS.

6.1.3 Distribución de la clave pública del Proveedor de Servicios de certificación

Las claves de PBS 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.

6.1.4 Tamaños de claves

La longitud de las claves de los Certificados de TSU es de 2048 bits.

6.1.5 Generación de parámetros de clave pública

La clave pública de los certificados de TSU está codificada de acuerdo con RFC 5280.

6.1.6 Comprobación de calidad de parámetros de clave pública

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

6.1.7 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.

6.2 Protección de la clave privada

En el presente apartado se recogen los controles relativos a la clave privada de la Certificado de TSU, por tal de garantizar el control exclusivo por parte de PBS.

6.2.1 Estándares de módulos criptográficos

Los módulos que gestionan claves de PBS cumplen con las certificaciones FIPS 140-2 level 3 y Common Criteria EAL4+.

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

Se requiere un control multi-persona, para el acceso a la clave privada del Certificado de TSU. Cómo mínimo se requerirán dos personas autenticadas al mismo tiempo.

Asimismo, los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3 Copia de respaldo de la clave privada

Se realiza copia de seguridad de las claves privadas de los certificados de TSU, de tal manera que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de estas. 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.

6.2.4 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos que conforman la infraestructura de clave pública.

6.2.5 Método de activación de la clave privada

Las claves privadas de los Certificados de TSU se almacenan cifradas en los módulos criptográficos que conforman la infraestructura de clave pública.

6.2.6 Método de desactivación de la clave privada

Los procedimientos de gestión de la clave privada del Certificado de TSU de PBS se activan mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por personas que desempeñen funciones fiables.

6.2.7 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 PBS. Para el reinicio se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

6.3 Controles de seguridad informática

Se emplean sistemas fiables para ofrecer sus servicios de certificación. Para ello se han 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, PBS aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas, 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 copia de seguridad y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

Cada servidor incluye las siguientes funcionalidades:

- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Auditoria de eventos relativos a la seguridad.
- Mecanismos de recuperación de claves y del sistema de la TSA.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.4 Controles técnicos del ciclo de vida

6.4.1 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.

6.4.2 Controles de gestión de seguridad

Se llevan a cabo 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 por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

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

6.4.2.1 Clasificación y gestión de información y bienes

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

La política de seguridad 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.

6.4.2.2 Operaciones de gestión

Se 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 se desarrolla en detalle el proceso de gestión de incidencias.

PBS 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.

6.4.2.3 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.

6.4.2.4 Planificación del sistema

El departamento de Sistemas al cargo de la infraestructura de clave pública mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

6.4.2.5 Reportes de incidencias y respuesta

Se dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación del proceso de resolución de la incidencia

6.4.2.6 Procedimientos operacionales y responsabilidades

Se han definido 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.

6.4.2.7 Gestión del sistema de acceso

Se llevan a cabo todas las actividades necesarias para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

- 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.
- Se dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.

- Se 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 es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

6.4.2.8 Gestión del ciclo de vida del hardware criptográfico

PBS se asegura que el hardware criptográfico usado para el servicio de sellado de tiempo no se manipula durante su transporte mediante la inspección del material entregado.

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

Se registran todo tipo de información pertinente con respecto del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de sellado de tiempo requiere el uso de al menos dos empleados de confianza.

Se llevan a cabo test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada del certificado de TSU de PBS almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema, 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.

6.5 Controles de seguridad de red

Se 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.

6.6 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 son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3.

6.7 Fuentes de Tiempo

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

6.8 Cambio de estado de un Dispositivo Seguro de Creación de Firma (SSCD)

En el caso de modificación del estado de la certificación de los dispositivos seguros de creación de firma (SSCD) que sustentan la Prestación de Servicios de Certificación, se procederá de la siguiente manera:

1. Se dispone de una lista de varios SSCD 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 SSCD.

2. En el supuesto de finalización del periodo de validez o pérdida de la certificación, no se utilizarán dichos SSCD para la prestación del servicio de sellado de tiempo.

3. Se procederá de inmediato a cambiar a de dispositivos SSCD con certificación válida.

4. En el supuesto caso que un dispositivo SSCD haya demostrado no haberlo sido nunca, por falsificación o cualquier otro tipo de fraude, se procederá de inmediato a comunicárselo a sus clientes y al ente regulador, revocar los certificados emitidos en estos dispositivos y reemplazarlos emitiéndolos en SSCD válidos.

7. Perfil del certificado de TSU

El perfil de certificado de TSU para la prestación del servicio de sellado de tiempo siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de PBS, todo ello disponible en la página web: https://www.pbssoluciones.com

7.1 Perfil de certificado

Los certificados de TSU cumplen con el estándar X.509 versión 3, el RFC 3739 y la norma EN 319 422.

7.1.1 Número de versión

Los certificados son X.509 Versión 3

7.1.2 Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la página web de PBS (https://www.pbssoluciones.com).

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.

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.

7.2 Perfil de la lista de revocación de certificados

El Procedimiento de revocación, suspensión y/o reactivación de los certificados de TSU siguen los procesos e indicaciones establecidas en la Declaración de Prácticas de Certificación y Texto divulgativo de PBS como Autoridad de Certificación, todo ello disponible en la página web: https://www.pbssoluciones.com .

7.2.1 Número de versión

Las CRL emitidas por PBS son de la versión 2.

7.2.2 Perfil de OCSP

Según el estándar IETF RFC 6960.

8. Auditoría de conformidad

PBS ha comunicado el inicio de su actividad como Proveedor de Servicios de certificación al Órgano Supervisor Nacional y se encuentra sometida a las revisiones de control que este organismo considere necesarias

8.1 Frecuencia de la auditoría de conformidad

PBS lleva a cabo una auditoría de conformidad anualmente, 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

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con PBS.

8.4 Listado de elementos objeto de auditoría

La auditoría verifica respecto a PBS:

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 PBS y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información.

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, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solventen dichas deficiencias.

Si PBS 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, deberá comunicarlo inmediatamente al equipo responsable de la seguridad que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave del Certificado de TSU y regenerar la infraestructura.
- Terminar el servicio de la Autoridad de Sellado de Tiempo (TSA).
- Otras acciones complementarias que resulten necesarias.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al equipo responsable de la seguridad en un plazo máximo de 15 días tras la ejecución de la auditoría.

9. Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa del servicio de sellado de tiempo

PBS puede establecer una tarifa por el servicio de sellado de tiempo, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2 Tarifa de acceso a información de estado del sello de tiempo

PBS no ha establecido ninguna tarifa por el acceso a la información del estado de los sellos de tiempo.

9.1.3 Tarifas de otros servicios

Sin estipulación.

9.1.4 Política de reintegro

Sin estipulación.

9.2 Capacidad financiera

PBS 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, en relación con la gestión de la finalización de los servicios y plan de cese.

9.2.1 Cobertura de seguro

PBS ha constituido una fianza que mantiene vigente en los términos previstos en los artículos 8 y 9 del Reglamento de la Ley de Firma Electrónica.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura de seguro para suscriptores y terceros que confían en los sellos de tiempo

PBS ha constituido una fianza que mantiene vigente en los términos previstos en los artículos 8 y 9 del Reglamento de la Ley de Firma Electrónica.

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por PBS:

- Las solicitudes del servicio, así como toda otra información personal obtenida para la prestación de este, excepto las informaciones indicadas en la sección siguiente.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa.
- 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 Divulgación legal de información

PBS divulga la información confidencial únicamente en los casos legalmente previstos.

9.4 Protección de datos personales

PBS garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales. En cumplimiento de la misma, PBS 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, asegurando la confidencialidad e integridad de los mismos.

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

9.4.1 Finalidad del tratamiento

PBS tiene el deber de informar a los usuarios, que todos sus datos de carácter personal facilitados se tratan para las siguientes finalidades:

- Prestación de Servicios Electrónicos de Certificación. Los datos son recabados mediante el contrato oportuno y son tratados con la finalidad de llevar a cabo los servicios electrónicos solicitados y contratados por los usuarios, todo ello en base a lo establecido en la presente Declaración de Prácticas de Certificación.

- Atender las consultas y solicitudes. Los datos se recaban mediante el formulario de contacto disponible en la página web (https://www.pbssoluciones.com) y serán utilizados exclusivamente para gestionar las consultas y solicitudes recibidas.

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

9.4.2 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 Electrónicos 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. Dicho consentimiento puede ser retirado en cualquier momento mediante el envío de un correo electrónico a info@pbs.com.

9.4.3 Transferencia de datos

Los datos personales no se cederán a terceros salvo obligación legal.

9.4.4 Derechos de los usuarios

- **Acceso y rectificación**. Los usuarios tienen derecho a acceder a todos sus datos personales, así como solicitar la rectificación de aquellos que sean inexactos o erróneos.

- **Confirmación**. Todos los usuarios tienen derecho a obtener confirmación sobre si PBS está tratando datos personales que les conciernan.

- **Cancelación**. Lo usuarios podrán solicitar la cancelación de los datos cuando, entre otros motivos, éstos no sean necesarios para los fines para los que fueron recogidos.

- **Oposición**. En determinadas circunstancias y por motivos relacionados con su situación particular, el usuario podrá oponerse al tratamiento de datos, estando PBS obligada a dejar de tratarlos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Para ejercer sus derechos, los usuarios pueden contactar con PBS a través del formulario de contacto disponible en la página web, mediante el envío de una petición a la dirección de correo electrónico info.sv@grouppbs.com o bien dirigir un escrito a la dirección indicada en el apartado de información del responsable del tratamiento.

En dicha petición, deberán adjuntar copia de su documento de identidad e indicar claramente cuál es el derecho que se desea ejercer.

Recibida una petición, PBS le dará el trámite oportuno, entregando la misma al responsable que corresponda en función del área que se vea afectada o del derecho que se desee ejercer.

Las solicitudes de ejercicio de los derechos de los usuarios que PBS se responderán dentro del plazo de diez (10) días hábiles contados desde el día siguiente de su recepción.

9.5 Derechos de propiedad intelectual

PBS goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación de Sellado de Tiempo.

9.6 Obligaciones y responsabilidad civil

9.6.1 Obligaciones de PBS

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

PBS presta los servicios electrónicos de certificación conforme con esta Declaración de Prácticas de Certificación de Sellado de Tiempo.

PBS informa al suscriptor de los términos y condiciones relativos a la prestación del servicio de sellado de tiempo, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia los textos de divulgación (PDS) del servicio.

El documento de texto de divulgación, también denominado PDS, cumple el contenido del anexo A de la ETSI EN 319 421, documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

DOCUTEN vincula a los suscriptores y terceros que confían en certificados, mediante dicho texto de divulgación o PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en el presente documento.
- Límites de uso de los sellos de tiempo.
- Información sobre cómo validar un sello de tiempo, incluyendo el requisito de comprobar el estado del mismo, y las condiciones en las cuales se puede confiar

razonablemente en él, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.

- Forma en que se garantiza la responsabilidad patrimonial del Proveedor de Servicios de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Proveedor de Servicios de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían

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

PBS garantiza al suscriptor que los sellos de tiempo cumplen con todos los requisitos materiales establecidos en esta Declaración de Prácticas de Certificación, así como las normas de referencia.

PBS garantiza al tercero que confía en el sello de tiempo que la información contenida o incorporada por referencia en el sello es correcta, excepto cuando se indique lo contrario.

9.6.3 Rechazo de otras garantías

PBS rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en este documento.

9.6.4 Limitación de responsabilidades

PBS limita su responsabilidad a la prestación del servicio de expedición de sellos de tiempo el cual se regulará por el contrato oportuno.

PBS no realiza ninguna verificación del documento para el que se solicita el Sello de tiempo, ya que el mismo se envía directamente por el Suscriptor bajo su propia y exclusiva responsabilidad.

PBS no asume ninguna obligación con respecto de la monitorización del contenido, tipo y/o formato de los documentos y del hash enviado por el proceso de sellado de tiempo.

PBS no será responsable de ningún daño directo y/o por terceros como consecuencia del uso indebido de los sellos de tiempo debidamente expedidos conforme el presente documento.

9.6.5 Caso fortuito y fuerza mayor

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

9.6.6 Ley aplicable

PBS establece, en el contrato de suscriptor y en el texto de divulgación o PDS que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley Salvadoreña.

9.6.7 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

PBS establece, en el contrato de suscriptor y en el texto de divulgación o PDS, 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, PBS vela porque, al menos los requisitos contenidos en las secciones 9.2 (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.

9.6.8 Cláusula de jurisdicción competente

PBS establece, en el contrato de suscriptor y en el texto de divulgación o PDS una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces de El Salvador.

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.

9.6.9 Resolución de conflictos

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

Anexo 1 - Acrónimos

AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
RA	Autoridad de Registro
CN	Common Name
CP	Certificate Policy
CPD	Centro de Procesamiento de Datos
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
DPC	Declaración de Prácticas de Certificación
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DCCF	Dispositivo Cualificado de Creación de Firma
ETSI	European Telecommunications Standards Institute o Instituto Europeo de Normas de Telecomunicaciones
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
LRC	Listas de Revocación de Certificados
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios

NTP	Network Time Protocol
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
PDS	Texto de divulgación
PIN	Personal Identification Number. Número de identificación personal
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure. Infraestructura de clave pública
PSC	Prestador de Servicios Electrónicos de Certificación / Confianza
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
TSA	Autoridad de Sellado de Tiempo
TSU	Unidad de Sellado de Tiempo