Declaración de Prácticas de Certificación

Presentado por:

PBS El Salvador

Octubre 2022

Lourdes Ramos
Gerente de Servicios de Impresión y Servicios Digitales
+503 7862-6104
+503 2246-3119
lourdes.ramos@grouppbs.com

PBS El Salvador
Final Boulevard Santa Elena y Boulevard
Orden de Malta, Edificio PBS
San Salvador, EL SALVADOR
tel + 503 2239 3000 | fax + 503 2239 3095
www.grouppbs.com

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	2.3
Fecha edición:	8/11/2022
Fichero:	PBS_DPC_ES_v2.3.docx

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Andrea Vargas Fecha: 27/10/2022	Nombre: Lourdes Ramos Fecha: 7/12/2022	Nombre: Mirian Judith Alas Escolero (Apoderada general administrativa con cláusulas especiales) Fecha: 8/12/2022

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	ABD	23/03/2022
2.0	Completo	Se incorpora el método de identificación a distancia. Se incorpora una nueva Autoridad de Certificación Subordinada. Actualizaciones menores gramaticales y de formato.	ABD	15/07/2022
2.1	Completo	Se incorporan referencias a lo largo del documento en relación con el método de identificación a distancia.	APV	27/10/2022

		Se añaden referencias relativas a la realización de auditoria por parte de PBS.		
2.2	Completo	Se incorporan referencias a lo largo del documento en relación con el método de identificación a distancia no asistido.	OPL	21/11/2022
2.3	Completo	Se incorporan referencias al documento relativas al proceso de emisión de certificados electrónicos vía API	OPL	7/12/2022

Índice

1 Introducción 13
1.1 Presentación 13
1.2 Nombre del documento e identificación 14
1.2.1 Identificadores de certificados 14
1.3 Participantes en los servicios de certificación 15
1.3.1 Proveedor de Servicios de certificación 15
1.3.1.1. Autoridad de Certificación Raíz El Salvador 15
1.3.1.2. PBS CA1 16
1.3.1.3 PBS CA2 16
1.3.2 Autoridad de Registro 16
1.3.3 Entidades finales 17
1.3.3.1 Suscriptores del servicio de certificación 18
1.3.3.2 Firmantes 18
1.3.3.3 Partes usuarias 19
1.3.4 Proveedor de Servicios de Infraestructura de Clave Pública 19
1.4 Uso de los certificados 19
1.4.1 Usos permitidos para los certificados 20

1.4.1.1 Certificado de Persona natural en QSCD 20
1.4.1.2 Certificado de persona natural perteneciente a empresa u organización en QSCD 20
1.4.1.3 Certificado de Persona Natural Profesional en QSCD 21
1.4.1.4 Certificado de persona natural funcionario público en QSCD 22
1.4.1.5 Certificado de Persona Natural Representante de Persona Natural en QSCD 23
1.4.1.6 Certificado de Persona Natural Representante de Persona Jurídica en QSCD 24
1.4.1.7 Certificado de Sello Electrónico en QSCD 24
1.4.1.8 Certificado de Facturación Electrónica de Persona Jurídica en QSCD 25
1.4.1.9 Certificado de Facturación Electrónica de Persona Natural en QSCD 26
1.4.1.10 Certificado de sello de tiempo electrónico 26
1.4.1.11 Certificado de VA-OCSP 27
1.4.2 Límites y prohibiciones de uso de los certificados 27
1.5 Administración de la política 28
1.5.1 Organización que administra el documento 28
1.5.2 El Salvador Datos de contacto de la organización 28
1.5.3 Procedimientos de gestión del documento 29
2 Publicación de información y depósito de certificados 29
2.1 Depósito(s) de certificados 29
2.2 Publicación de información del proveedor de servicios de certificación 29
2.3 Frecuencia de publicación 29
2.4 Control de acceso 30
3 Identificación y autenticación 30
3.1 Registro inicial 30
3.1.1 Tipos de nombres 30
3.1.1.1 **Certificado de persona natural ciudadano en QSCD** 30
3.1.1.2 **Certificado de persona natural perteneciente a empresa u organización en QSCD** 31
3.1.1.3 **Certificado de persona natural profesional en QSCD** 31
3.1.1.4 **Certificado de persona natural funcionario público en QSCD** 31
3.1.1.5 **Certificado de Persona Natural Representante de Persona Natural en QSCD** 32
3.1.1.6 **Certificado de Persona Natural Representante de Persona Jurídica en QSCD** 32
3.1.1.7 **Certificado de Sello Electrónico en QSCD** 32
3.1.1.8 **Certificado de Facturación Electrónica de Persona Jurídica en QSCD** 33

3.1.1.9 **Certificado de Facturación Electrónica de Persona Natural en QSCD** 33
3.1.1.10 **Certificado de sello de tiempo electrónico** 33
3.1.1.11 **Certificado de VA-OCSP** 33
3.1.2 Significado de los nombres 34
3.1.3 Emisión de certificados del set de pruebas y certificados de pruebas en general 34
3.1.4 Empleo de anónimos y seudónimos 34
3.1.5 Interpretación de formatos de nombres 34
3.1.6 Unicidad de los nombres 35
3.1.7 Resolución de conflictos relativos a nombres 35
3.2 Validación inicial de la identidad 36
3.2.1 Prueba de posesión de clave privada 36
3.2.2 Validación de la Identidad 36
3.2.2.1 **Entrevista de identificación al solicitante y la guía de dialogo de los operadores: método asistido** 40
3.2.3 Autenticación de la identidad de una organización, empresa o entidad mediante representante 41
3.2.4 Autenticación de la identidad de una Persona natural 43
3.2.4.1 **En los certificados** 43
3.2.4.2 **Validación de la Identidad** 44
3.2.4.3 **Vinculación de la Persona natural** 46
3.2.5 Información de suscriptor no verificada 46
3.2.6 Autenticación de la identidad de una RA y sus operadores 46
3.3 Identificación y autenticación de solicitudes de renovación 47
3.3.1 Validación para la renovación rutinaria de certificados 47
3.3.2 Identificación y autenticación de la solicitud de renovación 47
3.4 Identificación y autenticación de la solicitud de revocación, suspensión o reactivación 48
4 Requisitos de operación del ciclo de vida de los certificados 48
4.1 Solicitud de emisión de certificado 48
4.1.1 Legitimación para solicitar la emisión 48
4.1.2 Procedimiento de alta y responsabilidades 49
4.2 Procesamiento de la solicitud de certificación 49
4.2.1 Ejecución de las funciones de identificación y autenticación 49

4.2.2 Aprobación o rechazo de la solicitud 50
4.2.3 Plazo para resolver la solicitud 50
4.3 Emisión del certificado 50
4.3.1 Acciones de la CA durante el proceso de emisión 51
4.3.2 Notificación de la emisión al suscriptor 51
4.4 Entrega y aceptación del certificado 51
4.4.1 Responsabilidades de la CA 51
4.4.2 Conducta que constituye aceptación del certificado 52
4.4.3 Publicación del certificado 53
4.4.4 Notificación de la emisión a terceros 53
4.5 Uso del par de claves y del certificado 53
4.5.1 Uso por el firmante 53
4.5.2 Uso por el subscriptor 54
4.5.2.1 **Obligaciones del suscriptor del certificado** 54
4.5.2.2 **Responsabilidad civil del suscriptor de certificado** 54
4.5.3 Uso por el tercero que confía en certificados 55
4.5.3.1 **Obligaciones del tercero que confía en certificados** 55
4.5.3.2 **Responsabilidad civil del tercero que confía en certificados** 55
4.6 Renovación de certificados 56
4.7 Renovación de claves y certificados 56
4.7.1 Causas de renovación de claves y certificados 56
4.7.2 Procedimiento de renovación online de certificados 56
4.7.2.1 **Circunstancias para la renovación online** 56
4.7.2.2 **Quién puede solicitar la renovación online de un certificado** 56
4.7.2.3 **Aprobación o rechazo de la solicitud** 57
4.7.2.4 **Tramitación de las peticiones de renovación online** 57
4.7.2.5 **Notificación de la emisión del certificado renovado** 57
4.7.2.6 **Conducta que constituye aceptación del certificado renovado** 57
4.7.2.7 **Publicación del certificado renovado** 58
4.7.2.8 **Notificación de la emisión a terceros** 58
4.8 Modificación de certificados 58
4.9 Revocación, suspensión o reactivación de certificados 58

4.9.1 Causas de revocación de certificados 58
4.9.1.1 **Circunstancias que afectan a la información contenida en el certificado:** 58
4.9.1.2 **Circunstancias que afectan a la seguridad de la clave o del certificado:** 58
4.9.1.3 **Circunstancias que afectan al suscriptor o a la Persona natural identificada en el certificado:** 59
4.9.2 Causas de suspensión de un certificado 59
4.9.3 Causas de reactivación de un certificado 60
4.9.4 Quién puede solicitar la revocación, suspensión o reactivación 60
4.9.5 Procedimientos de solicitud de revocación, suspensión o reactivación 60
4.9.6 Plazo temporal de solicitud de revocación, suspensión o reactivación 61
4.9.7 Plazo temporal de procesamiento de la solicitud de revocación, suspensión o reactivación 61
4.9.8 Obligación de consulta de información de revocación o suspensión de certificados 61
4.9.9 Frecuencia de emisión de listas de revocación de certificados (LRCs) 62
4.9.10 Plazo máximo de publicación de LRCs 62
4.9.11 Disponibilidad de servicios de comprobación en línea de estado de certificados 62
4.9.12 Obligación de consulta de servicios de comprobación de estado de certificados 63
4.9.13 Requisitos especiales en caso de compromiso de la clave privada 63
4.9.14 Período máximo de un certificado digital en estado suspendido 63
4.10 Finalización de la suscripción 63
4.11 Depósito y recuperación de claves 64
4.11.1 Política y prácticas de depósito y recuperación de claves 64
4.11.2 Política y prácticas de encapsulado y recuperación de claves de sesión 64
5 Controles de seguridad física, de gestión y de operaciones 65
5.1 Controles de seguridad física 65
5.1.1 Localización y construcción de las instalaciones 66
5.1.2 Acceso físico 66
5.1.3 Electricidad y aire acondicionado 66
5.1.4 Exposición al agua 67
5.1.5 Prevención y protección de incendios 67
5.1.6 Almacenamiento de soportes 67
5.1.7 Tratamiento de residuos 67

5.1.8 Copia de respaldo fuera de las instalaciones 67
5.2 Controles de procedimientos 67
5.2.1 Funciones fiables 68
5.2.2 Número de personas por tarea 68
5.2.3 Identificación y autenticación para cada función 69
5.2.4 Roles que requieren separación de tareas 69
5.2.5 Sistema de gestión PKI 69
5.3 Controles de personal 69
5.3.1 Requisitos de historial, calificaciones, experiencia y autorización 69
5.3.2 Procedimientos de investigación de historial 70
5.3.3 Requisitos de formación 71
5.3.4 Requisitos y frecuencia de actualización formativa 71
5.3.5 Secuencia y frecuencia de rotación laboral 71
5.3.6 Sanciones para acciones no autorizadas 71
5.3.7 Requisitos de contratación de profesionales 71
5.3.8 Suministro de documentación al personal 72
5.4 Procedimientos de auditoría de seguridad 72
5.4.1 Tipos de eventos registrados 72
5.4.2 Frecuencia de tratamiento de registros de auditoría 73
5.4.3 Período de conservación de registros de auditoría 73
5.4.4 Protección de los registros de auditoría 73
5.4.5 Procedimientos de copia de respaldo 74
5.4.6 Localización del sistema de acumulación de registros de auditoría 74
5.4.7 Notificación del evento de auditoría al causante del evento 74
5.4.8 Análisis de vulnerabilidades 74
5.5 Archivos de informaciones 75
5.5.1 Tipos de registros archivados 75
5.5.2 Periodo de Conservación de registros 75
5.5.3 Protección del archivo 76
5.5.4 Procedimientos de copia de respaldo 76
5.5.5 Requisitos de sellado de fecha y hora 76
5.5.6 Localización del sistema de archivo 76

5.5.7 Procedimientos de obtención y verificación de información de archivo 76
5.6 Renovación de claves 77
5.7 Compromiso de claves y recuperación de desastre 77
5.7.1 Procedimientos de gestión de incidencias y compromisos 77
5.7.2 Corrupción de recursos, aplicaciones o datos 77
5.7.3 Compromiso de la clave privada de la entidad 77
5.7.4 Continuidad del negocio después de un desastre 77
5.8 Terminación del servicio 78
6 Controles de seguridad técnica 79
6.1 Generación e instalación del par de claves 79
6.1.1 Generación del par de claves 79
6.1.1.1 **Generación del par de claves del firmante** 79
6.1.2 Envío de la clave privada al firmante 80
6.1.3 Envío de la clave pública al emisor del certificado 80
6.1.4 Distribución de la clave pública del Proveedor de Servicios de certificación 80
6.1.5 Tamaños de claves 80
6.1.6 Generación de parámetros de clave pública 81
6.1.7 Comprobación de calidad de parámetros de clave pública 81
6.1.8 Generación de claves en aplicaciones informáticas o en bienes de equipo 81
6.1.9 Propósitos de uso de claves 81
6.2 Protección de la clave privada 81
6.2.1 Estándares de módulos criptográficos 81
6.2.2 Control por más de una persona (n de m) sobre la clave privada 81
6.2.3 Depósito de la clave privada 82
6.2.4 Copia de respaldo de la clave privada 82
6.2.5 Archivo de la clave privada 82
6.2.6 Introducción de la clave privada en el módulo criptográfico 82
6.2.7 Método de activación de la clave privada 83
6.2.8 Método de desactivación de la clave privada 83
6.2.9 Método de destrucción de la clave privada 83
6.2.10 Clasificación de módulos criptográficos 83
6.2.11 Clasificación de módulos criptográficos 83

6.3 Otros aspectos de gestión del par de claves 83
6.3.1 Archivo de la clave pública 84
6.3.2 Períodos de utilización de las claves pública y privada 84
6.4 Datos de activación 84
6.4.1 Generación e instalación de datos de activación 84
6.4.2 Protección de datos de activación 84
6.5 Controles de seguridad informática 84
6.5.1 Requisitos técnicos específicos de seguridad informática 85
6.5.2 Evaluación del nivel de seguridad informática 85
6.6 Controles técnicos del ciclo de vida 86
6.6.1 Controles de desarrollo de sistemas 86
6.6.2 Controles de gestión de seguridad 86
6.6.3 Clasificación y gestión de información y bienes 86
6.6.4 Operaciones de gestión 86
6.6.5 Tratamiento de los soportes y seguridad 87
Planificación del sistema 87
Reportes de incidencias y respuesta 87
Procedimientos operacionales y responsabilidades 87
6.7 Gestión del sistema de acceso 87
AC General 87
Generación del certificado 87
Gestión de la revocación 88
Estado de la revocación 88
6.8 Gestión del ciclo de vida del hardware criptográfico 88
6.9 Controles de seguridad de red 89
6.10 Controles de ingeniería de módulos criptográficos 89
6.11 Fuentes de Tiempo 89
6.12 Cambio de estado de un Dispositivo Seguro de Creación de Firma (SSCD) 89
7. Perfiles de certificados y listas de certificados revocados 90
7.1 Perfil de certificado 90
7.1.1 Número de versión 90
7.1.2 Extensiones del certificado 90

7.1.3 Identificadores de objeto (OID) de los algoritmos 90
7.1.4 Formato de Nombres 91
7.1.5 Restricción de los nombres 91
7.1.6 Identificador de objeto (OID) de los tipos de certificados 91
7.2 Perfil de la lista de revocación de certificados 91
7.2.1 Número de versión 91
7.2.2 Perfil de OCSP 91
8. Auditoría de conformidad 91
8.1 Frecuencia de la auditoría de conformidad 91
8.2 Identificación y calificación del auditor 91
8.3 Relación del auditor con la entidad auditada 92
8.4 Listado de elementos objeto de auditoría 92
8.5 Acciones a emprender como resultado de una falta de conformidad 92
8.6 Tratamiento de los informes de auditoría 93
9. Requisitos comerciales y legales 93
9.1 Tarifas 93
9.1.1 Tarifa de emisión o renovación de certificados 93
9.1.2 Tarifa de acceso a certificados 93
9.1.3 Tarifa de acceso a información de estado de certificado 93
9.1.4 Tarifas de otros servicios 93
9.1.5 Política de reintegro 93
9.2 Capacidad financiera 93
9.2.1 Cobertura 94
9.2.2 Otros activos 94
9.2.3 Cobertura para suscriptores y terceros que confían en certificados 94
9.3 Confidencialidad 94
9.3.1 Informaciones confidenciales 94
9.3.2 Informaciones no confidenciales 94
9.3.3 Divulgación de información de suspensión y revocación 95
9.3.4 Divulgación legal de información 95
9.3.5 Divulgación de información por petición de su titular 95
9.3.6 Otras circunstancias de divulgación de información 95

9.4 Protección de datos personales 96
9.5 Derechos de propiedad intelectual 98
9.5.1 Propiedad de los certificados e información de revocación 98
9.5.2 Propiedad de la Declaración de Prácticas de Certificación 99
9.5.3 Propiedad de la información relativa a nombres 99
9.5.4 Propiedad de claves 99
9.6 Obligaciones y responsabilidad civil 99
9.6.1 Obligaciones de PBS 99
9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados 100
9.6.3 Rechazo de otras garantías 101
9.6.4 Limitación de responsabilidades 101
9.6.5 Cláusulas de indemnidad 102
9.6.5.1 Cláusula de indemnidad de suscriptor 102
9.6.5.2 **Cláusula de indemnidad de tercero que confía en el certificado** 102
9.6.6 Caso fortuito y fuerza mayor 102
9.6.7 Ley aplicable 102
9.6.8 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación 103
9.6.9 Cláusula de jurisdicción competente 103
9.6.10 Resolución de conflictos 103
10. Anexo I - Acrónimos 104

PBS El Salvador
Final Boulevard Santa Elena y Boulevard
Orden de Malta, Edificio PBS
San Salvador, EL SALVADOR
tel + 503 2239 3000 | fax + 503 2239 3095
www.grouppbs.com

1 Introducción

1.1 Presentación

Este documento declara las prácticas de certificación de firma electrónica de Productive Business Solutions El Salvador, S.A. de CV, en adelante "*PBS El Salvador*".

Los certificados electrónicos de firma electrónica certificada que se emiten son los siguientes:

- **De Persona Natural**
  - Certificado de persona natural ciudadano en QSCD
  - Certificado de persona natural perteneciente a empresa u organización en QSCD
  - Certificado de persona natural profesional en QSCD
  - Certificado de persona natural funcionario público en QSCD

- **De Persona Natural Representante**
  - Certificado de Persona Natural Representante de Persona Natural en QSCD
  - Certificado de Persona Natural Representante de Persona Jurídica en QSCD

- **De Sello Electrónico**
  - Certificado de Sello Electrónico en QSCD

- **De Facturación Electrónica**
  - Certificado de Facturación Electrónica de Persona Jurídica en QSCD
  - Certificado de Facturación Electrónica de Persona Natural en QSCD

- **De Dispositivos**
  - Certificado de Sello de Tiempo Electrónico
  - Certificado de VA-OCSP

1.2 Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación de PBS El Salvador".

1.2.1 Identificadores de certificados

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

Certificados electrónicos de firma electrónica certificada:

Número OID	Tipo de certificados
	Persona Natural
1.3.6.1.4.1.57626.3.1.1	Certificado de persona natural ciudadano en QSCD
1.3.6.1.4.1.57626.3.1.1	Certificado de persona natural perteneciente a empresa u organización en QSCD
1.3.6.1.4.1.57626.3.1.1	Certificado de persona natural profesional en QSCD
1.3.6.1.4.1.57626.3.1.1	Certificado de persona natural funcionario público en QSCD
	Persona Natural Representante
1.3.6.1.4.1.57626.3.2.1	Certificado de Persona Natural Representante de Persona Natural en QSCD
1.3.6.1.4.1.57626.3.2.1	Certificado de Persona Natural Representante de Persona Jurídica en QSCD
	Sello Electrónico
1.3.6.1.4.1.57626.3.3.1	Certificado de Sello Electrónico en QSCD
	Facturación Electrónica
1.3.6.1.4.1.57626.3.6.1	Certificado de Facturación Electrónica de Persona Jurídica en QSCD
1.3.6.1.4.1.57626.3.6.1	Certificado de Facturación Electrónica de Persona Natural en QSCD
	Dispositivos
1.3.6.1.4.1.57626.3.4.1	Certificado de Sello de Tiempo Electrónico
1.3.6.1.4.1.57626.3.5.1	Certificado de VA-OCSP

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.

1.3 Participantes en los servicios de certificación

1.3.1 Proveedor de Servicios de certificación

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

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 del ETSI aplicables a la expedición y gestión de certificados principalmente, EN 319 401, EN 319 411-1 y EN 319 411-2, y los mejores estándares internacionales, 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, PBS El Salvador ha establecido una jerarquía de entidades de certificación:

1.3.1.1. Autoridad de Certificación Raíz El Salvador

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

Datos de identificación:

CN:	AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR
Huella digital:	09 d7 55 ab cb 51 d9 a9 50 05 10 6c cf bf 30 dc 8b 87 2f 2b
Válido desde:	martes, 8 de septiembre de 2020
Válido hasta:	viernes, 8 de septiembre de 2045
Longitud de clave RSA:	4.096 bits

1.3.1.2. PBS CA1

Se trata de la entidad 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 AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR.

Datos de identificación:

CN:	PBS CA1
Huella digital:	f4 de c1 99 49 92 4e 23 ac e9 da 75 12 3f 1d a2 96 8f fd 73
Válido desde:	miércoles, 2 de marzo de 2022
Válido hasta:	domingo, 1 de marzo de 2037
Longitud de clave RSA:	4.096 bits

1.3.1.3 PBS CA2

Se trata de la entidad 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 AUTORIDAD DE CERTIFICACION RAIZ EL SALVADOR.

Datos de identificación:

CN:	PBS CA2
Huella digital:	794564c0ab0c6477e737df72966e8c20b539ef51cc
Válido desde:	martes, 23 de agosto de 2022
Válido hasta:	sábado, 22 de agosto de 2037
Longitud de clave RSA:	4.096 bits

1.3.2 Autoridad de Registro

Una Autoridad de Registro de PBS El Salvador 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 del certificado.
- Gestionar la generación de claves y la emisión del certificado
- 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.

Podrán actuar como RA de PBS El Salvador:

- Cualquier entidad autorizada por PBS El Salvador.
- PBS El Salvador directamente.

PBS El Salvador formalizará contractualmente las relaciones entre ella misma y cada una de las entidades que actúen como Autoridad de Registro de PBS El Salvador.

La entidad que actúe como Autoridad de Registro de PBS El Salvador podrá autorizar a una o varias personas como Operador de la RA para operar con el sistema de emisión de certificados de PBS El Salvador en nombre de la Autoridad de Registro.

La Autoridad de Registro podrá delegar las funciones de identificación de los suscriptores y/o firmantes, previo acuerdo de colaboración en el que se acepte la delegación de estas funciones. PBS El Salvador deberá autorizar de manera expresa dicho acuerdo de colaboración.

También podrán ser Autoridades de Registro sujetas a esta Declaración de Prácticas de Certificación, las unidades designadas para esta función por los suscriptores de los certificados, como un departamento de personal, dado que disponen de los registros auténticos acerca de la vinculación de los firmantes con el suscriptor.

1.3.3 Entidades finales

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

Serán entidades finales de los servicios de certificación de PBS El Salvador las siguientes:

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

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 PBS El Salvador (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 – certificados de sello electrónico –, o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor – certificados de firma electrónica. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio electrónico de certificación es, por tanto, el cliente del Proveedor de Servicios de certificación, de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en las normas técnicas aplicables a la expedición de certificados electrónicos, en especial ETSI EN 319 411, secciones 5.4.2 y 6.3.4.e).

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 Certificada; siendo típicamente los empleados, representantes legales o voluntarios, así como otras personas vinculadas a los suscriptores; incluyendo las personas al servicio de la Administración, en los certificados de funcionario 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, así como todos aquellos datos exigidos por la ley, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por el Proveedor de Servicios electrónicos de certificación, por lo que las personas naturales identificadas en los correspondientes certificados son las únicas responsables de su protección y deberían considerar las implicaciones de perder una clave privada.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la autenticación, también se emplea el término más genérico de “Persona natural identificada en el 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 electrónicos.

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 de la Autoridad de Certificación.

1.3.4 Proveedor de Servicios de Infraestructura de Clave Pública

"Productive Business Solutions El Salvador, S.A. de CV" 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 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.pbssoluciones.com

1.4.1.1 Certificado de Persona natural en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.1.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma, es un certificado 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.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de certificación, y permite la generación de la “firma electrónica certificada”, es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:
El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.2 Certificado de persona natural perteneciente a empresa u organización en QSCD

Este certificado dispone del OID 1.3.6.1.4.1. 57626.3.1.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado emitido en dispositivo seguro de creación de firma, es un certificado 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.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organizationn), y permite la generación de la "firma electrónica certificada" es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:
El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.3 Certificado de Persona Natural Profesional en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.1.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma, es un certificado 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.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una entidad habilitante descrita en el campo “O” (Organization), y permite la generación de la “firma electrónica certificada” es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:
El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.4 Certificado de persona natural funcionario público en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.1.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2, lo cual se declara en el certificado. Este certificado emitido en dispositivo seguro de creación de firma, es un certificado 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.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación entre el firmante y una Institución descrita en el campo “O” (Organization), y permite la generación de la “firma electrónica certificada” es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:
El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.5 Certificado de Persona Natural Representante de Persona Natural en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.2.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de representante emitido en dispositivo seguro de creación de firma, es un certificado 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.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una persona natural en el campo “O” (Organization), y permite la generación de la “firma electrónica certificada” es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:
El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.6 Certificado de Persona Natural Representante de Persona Jurídica en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.2.1. Es un certificado que se emite para la firma electrónica certificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de representante emitido en dispositivo seguro de creación de firma, es un certificado 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.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una persona jurídica, entidad u organización en el campo “O” (Organization), y permite la generación de la “firma electrónica certificada” es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:
El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.7 Certificado de Sello Electrónico en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.3.1. Es un certificado que se emite de acuerdo con la política de certificación QCP-l-qscd con el OID 0.4.0.194112.1.3. Este certificado de sello electrónico emitido en dispositivo seguro de creación de firma, es un certificado 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.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de sello electrónico en dispositivo seguro de creación de firma garantizan la identidad del responsable del sello y de la entidad vinculada, incluidos en el certificado.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:
El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c) Key Encipherment

1.4.1.8 Certificado de Facturación Electrónica de Persona Jurídica en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.6.1. Es un certificado que se emite de acuerdo con la política de certificación QCP-l-qscd con el OID 0.4.0.194112.1.3. Este certificado de facturación electrónica emitido en dispositivo seguro de creación de firma, es un certificado 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.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de facturación electrónica en dispositivo seguro de creación de firma garantizan la identidad del responsable del certificado y de la entidad vinculada, incluidos en el mismo.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionarlo, identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:
El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c) Key Encipherment

Este certificado solo podrá ser utilizado para la facturación electrónica de la entidad suscriptora identificada en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos de conformidad con la normativa aplicable.

1.4.1.9 Certificado de Facturación Electrónica de Persona Natural en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.6.1. Es un certificado que se emite de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de facturación electrónica emitido en dispositivo seguro de creación de firma, es un certificado 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.

Funciona con dispositivos seguros de creación de firma y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de certificación, y permite la generación de la “firma electrónica certificada”, es decir, son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos.

La información de usos en el perfil de certificado indica lo siguiente:
El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a) Firma digital (Digital Signature, para realizar la función de autenticación)
b) Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
c) Key Encipherment

Este certificado solo podrá ser utilizado para la facturación electrónica del firmante identificado en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos de conformidad con la normativa aplicable.

1.4.1.10 Certificado de sello de tiempo electrónico

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.4.1, y se emite de acuerdo con la política de certificación QCP-l-qscd con el OID 0.4.0.194112.1.3.
Los certificados de sello de tiempo electrónico se tratan de certificados emitidos para la operación de autoridades de sellado de tiempo y hora, para la firma de los sellos de tiempo que éstas producen.

Estos certificados permiten la firma de los sellos de tiempo que se emiten, desde el momento que hayan obtenido un certificado de sello de tiempo electrónico válido y mientras éste se encuentre vigente.

La sincronización de los tiempos en PBS se realiza mediante un servicio servidor de tiempo NTP Stratum 3.

Este servidor, un Meinberg Lantime M300/GPS, con oscilador TCXO de alta estabilidad, receptor GPS, formado por una tarjeta GPS interna para sincronizarse simultáneamente con los satélites con los que tiene visibilidad en cada momento (entre 3 y 8), y protección anti-rayos.

1.4.1.11 Certificado de VA-OCSP

Este certificado dispone del OID 1.3.6.1.4.1.57626.3.5.1, y se emite de acuerdo con la política de certificación QCP-l-qscd con el OID 0.4.0.194112.1.3.

Los certificados de VA-OCSP son certificados emitidos para la operación de las Autoridades de Validación, respecto del servicio de validación de certificados mediante el protocolo OCSP (*Online Certificate Status Protocol*).

Estos certificados permiten la firma de las respuestas realizadas por el servidor de OCSP, a las peticiones de los usuarios para la verificación del estado de un certificado.

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 (LRC).

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

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

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

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

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

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 El Salvador 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
El Salvador
Correo electrónico: firmaelectronica.sv@grouppbs.com
Teléfono: +503 2239 3000
Página web: www.grouppbs.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 de información y depósito de certificados

2.1 Depósito(s) de certificados

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

Dicho servicio se encuentra disponible en el sitio web de PBS, durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de PBS, 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 proveedor de servicios de certificación

PBS publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos indistintamente del método de identificación, de los que se ha obtenido previamente el consentimiento de la Persona natural identificada en el certificado de acuerdo a los procedimientos de PBS
- 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.
- Los textos de divulgación (Policy Disclosure Statements - PDS), como mínimo en español.

2.3 Frecuencia de publicación

La información del Proveedor 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.

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, especialmente la información de estado de revocación.

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.
- 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.

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.509 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y 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 ciudadano en QSCD

Country Name (C)	País de residencia o nacionalidad del firmante
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número de documento de identificación del firmante
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE

3.1.1.2 Certificado de persona natural perteneciente a empresa u organización en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Nombre de la Empresa u Organización
Organizational Unit Name (OU)	Departamento al que pertenece el firmante o el tipo de vinculación con la Empresa
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante
Title	Título o puesto que la persona ocupa en la Empresa u Organización
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número de documento de identificación del firmante
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE

3.1.1.3 Certificado de persona natural profesional en QSCD

Country Name (C)	**País donde la organización o entidad solicitante del certificado está registrada**
Organization Name (O)	Nombre de la entidad habilitante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante
Title	Se especificará el título o especialidad del firmante.
Surname	Apellidos del firmante
Given Name	Nombre del firmante
Serial Number	Número de documento de identificación del firmante
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE

3.1.1.4 Certificado de persona natural funcionario público en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organizational Unit Name (OU)	Departamento al que pertenece el firmante o el tipo de vinculación con la Institución
Organization Name (O)	Se especificará el nombre de la Institución
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante
Title	Se especificará el cargo o puesto que la persona ocupa en la Institución
Surname	Apellidos del firmante

Given Name	Nombre del firmante
Serial Number	Número de documento de identificación del firmante
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE

3.1.1.5 Certificado de Persona Natural Representante de Persona Natural en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Nombre de persona natural representada
Organization Identifier	Número de documento de identificación de la persona a quien representa
Title	REPRESENTANTE LEGAL
Surname	Apellidos del representante
Given Name	Nombre del representante
Serial Number	Número de documento de identificación del representante
Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE

3.1.1.6 Certificado de Persona Natural Representante de Persona Jurídica en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Nombre de la organización de la que el firmante es representante
Organization Identifier	Número oficial de identificación de la organización o entidad representada por el firmante
Title	REPRESENTANTE LEGAL
Surname	Apellidos del representante
Given Name	Nombre del representante
Serial Number	Número de documento de identificación del representante
Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE

3.1.1.7 Certificado de Sello Electrónico en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Denominación (nombre “oficial” de la organización o entidad)
Organizational Unit Name (OU)	Denominación (nombre “oficial” de la unidad) del solicitante del sello (Ej: Subdirección de explotación)
Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello
Surname	Apellidos del firmante responsable firmante del sello
Given Name	Nombre del firmante responsable firmante del sello
Serial Number	Número de documento de identificación del responsable firmante del sello

Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES

3.1.1.8 Certificado de Facturación Electrónica de Persona Jurídica en QSCD

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Organization Name (O)	Denominación (nombre "oficial" de la organización o entidad)
Organizational Unit Name (OU)	Denominación (nombre "oficial" de la unidad) del solicitante del sello (Ej: Subdirección de explotación)
Organization Identifier	Número oficial de identificación de la organización o entidad a la que está vinculado el sello
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Description	Número de Registro de Contribuyente (NRC)

3.1.1.9 Certificado de Facturación Electrónica de Persona Natural en QSCD

Country Name (C)	País de residencia o nacionalidad del firmante
Surname	Apellidos del firmante responsable firmante del sello
Given Name	Nombre del firmante responsable firmante del sello
Serial Number	Número de documento de identificación del responsable firmante del sello
Common Name	NOMBRE DESCRIPTIVO DEL CREADOR DEL SELLO, ASEGURANDO QUE DICHO NOMBRE TENGA SENTIDO Y NO DÉ LUGAR A AMBIGÜEDADES
Description	Número de Registro de Contribuyente (NRC)

3.1.1.10 Certificado de sello de tiempo electrónico

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Locality Name (L)	Nombre de la LOCALIDAD donde resida el proveedor del servicio de certificación.
Organizational Unit Name (OU)	TSP-UNIDAD PRESTADOR
Organization Name (O)	NOMBRE ORGANIZACIÓN
Common Name (CN)	Sello de tiempo electrónico de [NOMBRE DEL PRESTADOR DE SERVICIO]
Organization Identifier (other name)	VATSV-[NIT DEL PRESTADOR DEL SERVICIO]"

3.1.1.11 Certificado de VA-OCSP

Country Name (C)	País donde la organización o entidad solicitante del certificado está registrada
Locality Name (L)	Nombre de la LOCALIDAD donde resida el titular del certificado. (No incluir información adicional al nombre de la localidad)
Organizational Unit Name (OU)	TSP-UNIDAD PRESTADOR
Organization Name (O)	NOMBRE ORGANIZACIÓN
Common Name (CN)	Autoridad de Validación de [NOMBRE DEL PRESTADOR DE SERVICIO]
Organization Identifier (other name)	VATSV-[NIT DEL PRESTADOR DEL SERVICIO]"

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 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 PBS. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y permitir al ente regulador su evaluación.

3.1.4 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.

3.1.5 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 Documento Único de Identidad (DUI), Pasaporte u otro número de identificación idóneo del firmante, reconocido en derecho.

3.1.6 Unicidad de los nombres

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

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 del Número de Identificación Fiscal, 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:

- Documento Único de Identidad (DUI), Pasaporte u otro identificador legalmente válido de la Persona natural.
- Número de Identificación Tributaria (NIT) u otro identificador legalmente válido del suscriptor.
- Tipo de certificado (OID de identificador de política de certificación).

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

3.1.7 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.

No existirá ninguna obligación 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 Proveedor de Servicios de electrónicos 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 en el marco de los organismos competentes para la realización de un arbitraje en El Salvador a los 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.

3.2 Validación inicial de la identidad

La identificación de los suscriptores se realizará mediante comparecencia personal o a distancia según corresponda, cuya identidad resulta fijada en el momento de la firma del contrato entre PBS y el suscriptor, momento en el que queda verificada la existencia del suscriptor mediante su documento oficial de identidad o las escrituras correspondientes, al igual que los poderes de actuación de la persona que presente como representante si fuese el caso. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

En el caso de personas naturales identificadas presencialmente, en certificados cuyo suscriptor sea una persona jurídica, sus identidades podrán validarse mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados siempre que aseguren que se han identificado presencialmente. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a PBS, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

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 certificados de sello, o por el firmante, en certificados de firma.

3.2.2 Validación de la Identidad

Para la solicitud de certificados, los Operadores de Registro de PBS, ya sean de manera asistida o no asistida:

Determínese como asistida la intervención síncrona del operador después de que el solicitante o titular haya realizado el proceso de video identificación a distancia, validando el operador los documentos, la evidencia de prueba de vida, de coincidencia del Selfie con los documentos de identidad, de revisión de las imágenes de los documentos y de los datos capturados del proceso requerido para la aprobación o rechazo de la emisión del certificado.

Y como no asistida la intervención asíncrona de dicho operador donde después de que el titular haya realizado su proceso de video identificación a través de la plataforma de identificación a distancia, la tecnología de dicha plataforma, realizará una evaluación de prueba de vida, de coincidencia del Selfie con los documentos de identidad, de revisión de las imágenes de los documentos y de revisión por los datos capturados del proceso, si estos cuatro parámetros son superados, de manera automática se emitirá el certificado. De lo contrario, si uno de estos parámetros no es superado a través de la respuesta que emita la plataforma, se deberá pasar al proceso asistido a través de un operador de la autoridad de registro para validar los datos y aceptar o rechazar la emisión del certificado.

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 la verificación se procederá a través de un operador de registro o persona autorizada de la Autoridad de Registro de acuerdo con los siguientes métodos:

a. En presencia de la persona física o de un representante autorizado de la persona jurídica, quien deberá aportar el Documento Único de Identidad (DUI), Pasaporte u otro medio idóneo reconocido en derecho para su identificación.
b. Por medio del procedimiento de identificación a distancia a través del sistema de vídeo identificación remota de PBS o utilizando otros métodos de identificación a distancia que cumplan las condiciones y requisitos de seguridad determinados por la Unidad de Firma Electrónica. Para este fin, PBS tendrá dos opciones de identificación a distancia para la emisión del certificado.
   Siendo la primera la que permite el procesamiento no asistido de video identificación del titular del certificado a través una solución desatendida puramente digital que permite la identificación electrónica en tiempo real y evita la personación. En esta video identificación, el solicitante muestra sus documentos identificativos, se hacen capturas de pantalla de los mismos y se graba todo el proceso de identificación. A su vez, se permite también la intervención de un operador de registro en caso se necesitara para completar el proceso.
   La segunda opción de video identificación permitirá al solicitante muestre sus documentos identificativos, se hacen capturas de pantalla de los mismos y se graba todo el proceso de identificación, sin embargo, esta opción requiere de la asistencia del operador de la autoridad de registro después de la video identificación realizada para finalizar el proceso de emisión de certificado.
c. Por medio de un certificado electrónico de firma certificada, o sello electrónico, siempre y cuando el periodo de tiempo transcurrido desde la identificación realizada en el apartado a) de este apartado, sea menor a cinco (5) años.
d. Mediante identificaciones previas de los solicitantes de los certificados electrónicos, que ya constasen en PBS en virtud de una relación previa, siempre y cuando desde la

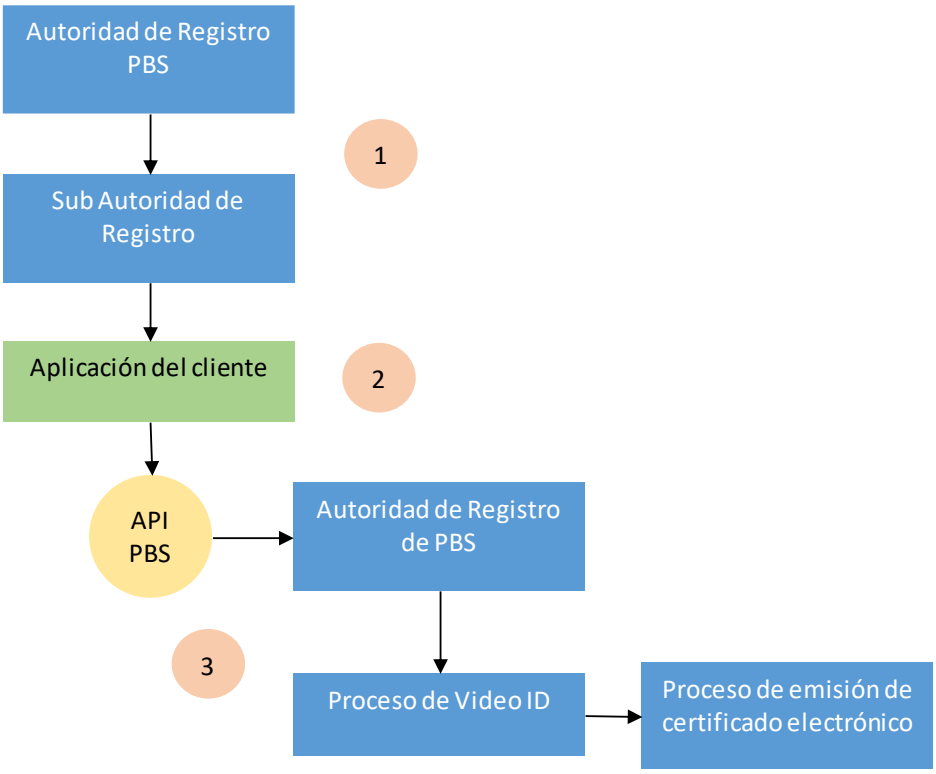
identificación realizada acorde a los procedimientos descritos en el apartado a) de este apartado, sea menor a cinco (5) años.

El proceso de emisión de certificados utilizando el método de identificación a distancia, en las soluciones que PBS posee, se podrá realizar de manera automatizada por las autoridades de registro que el proveedor de servicios de certificación cree. Este proceso podría realizarse a través de API (interfaz de programación de aplicaciones), lo cual es un intermediario de software que permite que dos aplicaciones se comuniquen entre sí. El flujo a seguir para este proceso se describiría de la siguiente manera:

El proveedor de servicios de certificación creará y habilitará una autoridad de registro subordinada (cliente) dentro de la plataforma de la autoridad de registro. Posterior a ello, PBS le facilitará a la sub autoridad unas credenciales y la información relativa a la API para que, a través de esta, PBS disponga los servicios de firma electrónica al cliente y este pueda conectarse y consumir, a través de su aplicación, los servicios de la autoridad de registro para la emisión de certificados electrónicos de PBS. Una vez el cliente se encuentre consumiendo los servicios de PBS, podrá ofrecerle al usuario final el proceso de video identificación y el de emisión de certificados electrónicos.

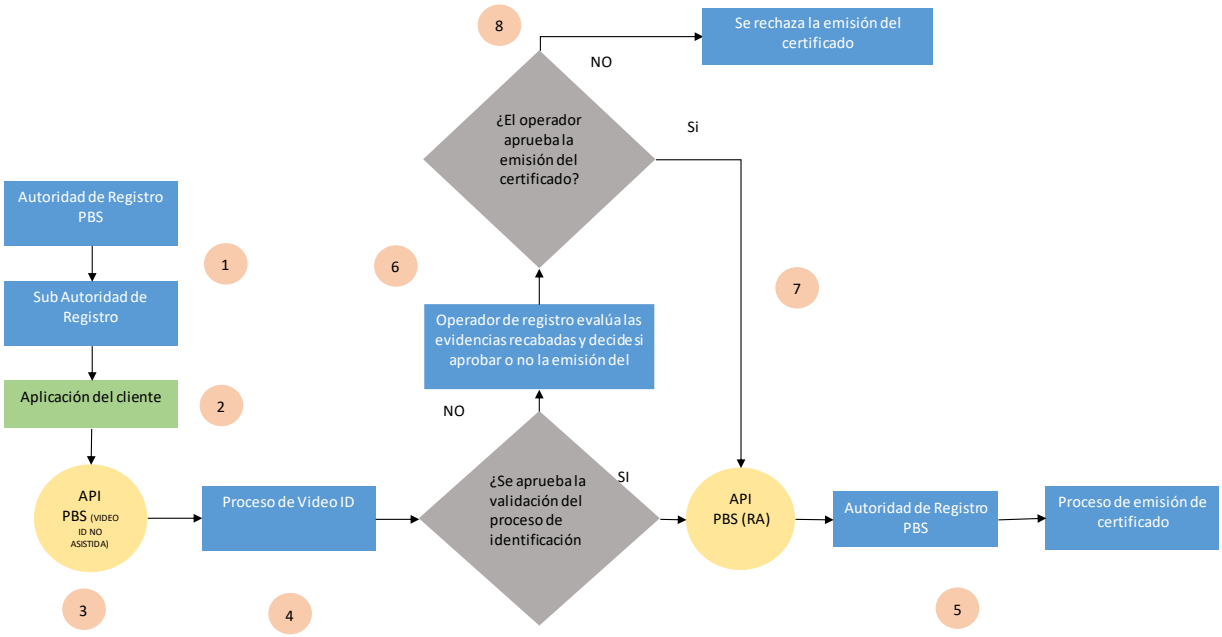
A continuación, se describen a detalle los pasos que sigue el proceso automatizado de la emisión de certificados electrónicos con el método de identificación a distancia a través de las soluciones que PBS posee:

Solución de video identificación asistida



1. La Autoridad de Registro de PBS crea en la plataforma una nueva autoridad de registro subordinada (cliente).
2. El cliente o la autoridad de registro subordinada posee una aplicación o interfaz en la cual ofrece sus servicios al público.
3. PBS dispone servicios a través de la API para que el cliente a través de su aplicación pueda conectarse y consumir los servicios de la autoridad de registro, en donde podrá poner a disposición del usuario el proceso de video identificación para que se pueda aprobar por un operador de registro el proceso de emisión del certificado electrónico.

Solución de video identificación no asistida



1. La Autoridad de Registro de PBS crea en la plataforma una nueva autoridad de registro subordinada (cliente).
2. El cliente o la autoridad de registro subordinada posee una aplicación o interfaz en la cual ofrece sus servicios al público.
3. PBS otorga API al cliente para que su aplicación pueda conectarse con los servicios de video identificación no asistida de PBS.
4. El cliente a través de su aplicación dispone el servicio del proceso de video identificación al usuario final.
5. Si la validación se aprueba, la aplicación del cliente, a través de la API de firma electrónica, dispone el servicio de la autoridad de registro para la emisión de los certificados electrónicos.
6. Si la validación no se aprueba, existiría la intervención de un operador de registro para validar si existen evidencias suficientes para proceder con la emisión del certificado electrónico.
7. Si existen evidencias suficientes para proceder a la emisión del certificado electrónico, la aplicación del cliente, a través de la API de firma electrónica, dispondría del servicio de la autoridad de registro para emitir el certificado.
8. Si no existen evidencias suficientes para proceder a la emisión del certificado electrónico, el operador rechaza la solicitud del certificado electrónico.

3.2.2.1 Entrevista de identificación al solicitante y la guía de dialogo de los operadores: método asistido

Proceso de entrevistas con el solicitante del certificado electrónico:

El operador de registro se pondrá en contacto con el solicitante para poder validar información que permita aclarar la emisión del certificado. La entrevista será guiada solicitante los siguientes datos mínimos:

1. Nombre completo del solicitante
2. Tipo de documento a presentar: DUI, Pasaporte o Carnet de residencia
3. Dirección de residencia
4. Ciudad de residencia
5. Código postal
6. Teléfono celular
7. Correo electrónico
8. Fotografías del documento de identidad anverso y reverso
9. Enviar enlace para realizar prueba de vida

El diálogo de los operadores de registro se basará en la solicitud del tipo de certificado y constará en poder evidenciar que la persona es quien dice ser y que la persona está viva, entre las preguntas que se realizarán se encuentran:

1. ¿Cuál es su nombre completo?
2. ¿Cuál es su dirección de residencia?
3. ¿Cuál es su número de documento de identidad?
4. ¿Cuál es su número de celular?
5. ¿Cuál es su correo electrónico?

Se podrán realizar todas las preguntas o no, y esto será basado en la información que el titular haya provisto en el proceso de video identificación.

3.2.3 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 o entidades sin personalidad jurídica, públicas o privadas, que sean suscriptoras de certificados, podrán actuar como representantes de estas, 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 PBS, 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 3.2.2., de tal manera que:
    i. Si se identifica presencialmente ante un operador o persona autorizada de una Autoridad de Registro de PBS:
        - Mostrando su documento oficial de identificación (Documento Único de Identidad (DUI), 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 video identificación remota de PBS:
   - Mostrando su documento oficial de identificación (Documento Único de Identidad (DUI), 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 proporcionará la siguiente información y sus correspondientes soportes acreditativos:
   - Sus datos de identificación, como representante:
     - Nombre y apellidos
     - Lugar y fecha de nacimiento
     - Documento: DUI, Pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
   - Los datos de identificación del suscriptor al que representa:
     - Denominación o razón social.
     - Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.
     - Documento: NIT o documento acreditativo de la identificación fiscal de la entidad.
     - Documento: Documentos públicos 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 electrónica de la escritura notarial de apoderamiento, en los términos de la normativa notarial.

3. El operador o personal autorizado de la Autoridad de Registro de PBS 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 aportado.
     - Documentación que acredite su representación.

   - Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de PBS 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 video identificación remota.
     - Revisión del cotejo producido por el sistema de video 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 video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.
     - Documentación que acredite su representación.

4. El operador o personal autorizado de la Autoridad de Registro de PBS verificará la información suministrada para la autenticación y le devolverá cuando corresponda la documentación original aportada.

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

3.2.4 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.

3.2.4.1 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 3.2.2. de esta DPC, de tal manera que:

- (i) Si se identifica presencialmente ante un operador o persona autorizada de una Autoridad de Registro de PBS:
  - Mostrando su Documento Único de Identidad (DUI), pasaporte u otro medio idóneo reconocido en derecho.

- (ii) Si se identifica electrónicamente a través del sistema de video identificación remota usado por PBS:
  - Mostrando su Documento Único de Identidad (DUI), pasaporte u otro medio idóneo reconocido en derecho.
  - 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.

La información de identificación de las personas naturales identificadas en los certificados cuyo suscriptor sea una entidad 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.

3.2.4.2 Validación de la Identidad

Para la solicitud de certificados, el operador o personal autorizado de la Autoridad de Registro PBS 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 video identificación de PBS, el operador de registro comprobará la identidad de la persona natural de manera asistida o no asistida, 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 video identificación remota.
  - Revisión del cotejo producido por el sistema de video 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 video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.

Teniendo PBS la opción de video identificación no asistida la cual es una solución desatendida puramente digital que permite la identificación electrónica en tiempo real y evita la personación del titular con verificaciones de identidad totalmente automatizadas y en tiempo real, impulsadas exclusivamente por inteligencia artificial y aprendizaje automático. Pero a su vez, en caso fuera necesario, permite la intervención del operador de registro para finalizar el proceso de emisión de certificado. También PBS posee la opción de video identificación asistida que permite al solicitante muestre sus documentos identificativos, se hacen capturas de pantalla de los mismos y se graba todo el proceso de identificación, sin embargo, esta opción requiere de la asistencia del operador de la autoridad de registro después de la video identificación realizada para finalizar el proceso de emisión de certificado.

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica no se requiere la presencia física directa, debido a la relación ya acreditada entre la Persona natural y entidad, empresa u organización de derecho público o privado a la que está vinculada. Sin embargo, antes de la entrega de un certificado, la entidad,

empresa u organización de derecho público o privado suscriptora, por medio de su responsable de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la Persona natural identificada en el certificado mediante su presencia física.

Durante este trámite se confirma rigurosamente la identidad de la Persona natural identificada en el certificado. Por este motivo, en todos los casos en que se expide un certificado se acredita mediante un operador de registro, ya sea de manera asistida o no asistida, la identidad de la Persona natural firmante.

La Autoridad de Registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

3.2.4.3 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.

3.2.5 Información de suscriptor no verificada

PBS no incluye ninguna información de suscriptor no verificada en los certificados.

3.2.6 Autenticación de la identidad de una RA y sus operadores

Para la constitución de una nueva Autoridad de Registro, se realizan las verificaciones necesarias para confirmar la existencia de la entidad u organización de la que se trate. Para ello, se podrá utilizar exhibición de documentos o utilizar sus propias fuentes de información.

Igualmente, PBS directamente o a través de su Autoridad de Registro, verifica y valida la identidad de los operadores de las Autoridades de Registro, para lo cual estas últimas envían a PBS la documentación de identificación correspondientes al nuevo operador, juntamente con su autorización para actuar como tal.

PBS se asegura que los operadores de la Autoridad de Registro reciben la formación suficiente para el desarrollo de sus funciones, lo cual verifica con la evaluación correspondiente. Dicha formación y evaluación puede ser ejecutada por la Autoridad de Registro previamente autorizada por PBS.

Para la prestación de los servicios, PBS se asegura de que los operadores de Autoridad de Registro acceden al sistema mediante autenticación fuerte con certificado digital.

3.3 Identificación y autenticación de solicitudes de renovación

3.3.1 Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, el operador o personal autorizado de la Autoridad de Registro se comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la Persona natural identificada en el certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son:

- El uso del código “CRE” o “ERC” relativo al certificado anterior, o de otros métodos de autenticación personal, que consiste en información que sólo conoce la Persona natural identificada en el certificado, y que le permite renovar de forma automática su certificado, siempre que no se haya superado el plazo máximo legalmente establecido.
- El empleo del certificado vigente para su renovación y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

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.
La renovación de certificados no aplicará para aquellos certificados que fueron emitidos mediante la identificación a distancia de PBS. De tal manera que la solicitud de un certificado será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

3.3.2 Identificación y autenticación de la solicitud de renovación

Antes de renovar un certificado, el operador o personal autorizado de la Autoridad de Registro 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.

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

PBS o un operador o personal autorizado de la Autoridad de Registro autentica 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 de manera online mediante el uso del Código de Revocación (CRE o ERC) a través de la página web de PBS 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 PBS y/o Autoridades de Registro.
- Las autoridades de registro de PBS: deberán 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 pasa a estado de suspensión.

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 indistintamente del método de identificación empleado por PBS, sea Persona natural o jurídica, deberá firmar un contrato de prestación de servicios de certificación con PBS.

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

Cuando el solicitante es una persona distinta al suscriptor, debe existir una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados 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

PBS recibe solicitudes de certificados, realizadas por personas, 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 PBS. En el caso de certificados cuyo suscriptor sea una entidad, empresa u organización de derecho público o privado que actúe como una Autoridad de Registro de PBS, podrá gestionar directamente las solicitudes accediendo a los sistemas informáticos de PBS y generar los certificados correspondientes para la propia entidad, empresa u organización o para sus miembros.

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 3.2.4. 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

4.2.1 Ejecución de las funciones de identificación y autenticación

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

En caso afirmativo, PBS verifica la información proporcionada, verificando los aspectos descritos en la sección 3.2.

La documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado, incluso en caso de pérdida anticipada de vigencia por revocación.

4.2.2 Aprobación o rechazo de la solicitud

Tras realizar la identificación de la persona de manera presencial o a distancia, siguiendo las políticas y procedimientos de PBS, se procederá a su verificación. En caso de que los datos se verifiquen correctamente, PBS debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Autoridad de Certificación, de las Autoridades de Registro o de los suscriptores, PBS denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, la solicitud quedará denegada definitivamente.

Se notificará al solicitante la aprobación o denegación de la solicitud.

Podrá automatizarse 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

Las solicitudes de certificados se atienden 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.

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, PBS:

- Protege la confidencialidad e integridad de los datos de registro de que dispone provenientes tanto de la identificación realizada de manera presencial como de la realizada a distancia.
- 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 la propia PBS o sus Autoridades de Registro deducirlas o utilizarlas en ningún modo.

4.3.2 Notificación de la emisión al suscriptor

PBS notifica la emisión del certificado al suscriptor y/o a la Persona natural identificada en el certificado y el método de generación/descarga.

4.4 Entrega y aceptación del certificado

4.4.1 Responsabilidades de la CA

Durante este proceso, el operador o personal autorizado de la Autoridad de Registro PBS (ya sea asistido o no asistido, siendo el primero la intervención humana del mismo y el segundo, no asistido, la metodología de video identificación totalmente automatizada en tiempo real impulsada por inteligencia artificial) debe realizar las siguientes actuaciones:

- Independientemente del método de identificación realizado por PBS se deberá acreditar definitivamente la identidad de la Persona natural identificada en el certificado, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.4.

- 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 Proveedor 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 conserva los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a PBS, así como los originales cuando PBS precise de acceso a los mismos.

4.4.2 Conducta que constituye aceptación del certificado

Indistintamente del método de identificación utilizada para la emisión del certificado cuando se haga entrega de la hoja de aceptación en formato digital o físico según corresponda, dicha 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 se lleve a cabo a través del procedimiento automatizado definido por PBS, la aceptación del certificado por la Persona natural identificada en el mismo se produce mediante la firma del contrato de Prestación de Servicios de Certificación utilizando el propio certificado.

4.4.3 Publicación del certificado

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

4.4.4 Notificación de la emisión a terceros

PBS 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

PBS obliga a:

- Facilitar a PBS 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 la sección 0.
- Cuando el certificado funcione juntamente con un DCCF, reconocer su capacidad de producción de firmas electrónicas certificadas; 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, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 0.
- Comunicar a PBS, 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.

PBS obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante 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 firmante es una entidad final y no un Proveedor 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 Proveedor de Servicios de certificación ni en ningún otro caso.

4.5.2 Uso por el subscriptor

4.5.2.1 Obligaciones del suscriptor del certificado

PBS obliga contractualmente al suscriptor a:

- Facilitar a la Autoridad 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 emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Comunicar a PBS, 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 PBS, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del Proveedor de Servicios de certificación de PBS.

4.5.2.2 Responsabilidad civil del suscriptor de certificado

PBS 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 Proveedor 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 Proveedor 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

PBS 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 digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas, producidas en un dispositivo seguro de creación de firma (DSCF) tienen la consideración legal de firmas electrónicas certificadas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.
- 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.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de PBS, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la PBS.

4.5.3.2 Responsabilidad civil del tercero que confía en certificados

PBS 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.

No aplicará la renovación de un certificado cuando se hubiera sido emitido mediante la identificación a distancia de la persona. De tal manera que la solicitud de un certificado será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

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.

Se consideran al menos dos posibilidades para la renovación de certificados:

- Proceso de renovación presencial, que se efectuará del mismo modo que la emisión de un nuevo certificado.
- Proceso de renovación online (a través de internet), que se detalla a continuación.

4.7.2 Procedimiento de renovación online de certificados

4.7.2.1 Circunstancias para la renovación online

Solamente se podrá proceder a la renovación online del certificado si se cumplen las condiciones siguientes:

- La Autoridad de Registro y/o PBS dispone del servicio de renovación online.
- El certificado con el que se firma la renovación esté vigente, es decir, no haya caducado, no esté revocado ni suspendido.

4.7.2.2 Quién puede solicitar la renovación online de un certificado

Cualquier firmante podrá pedir la renovación online de su certificado si se cumplen las circunstancias descritas en el punto anterior.

El firmante podrá formalizar su solicitud accediendo al servicio de renovación online de certificados en la página web de PBS.

4.7.2.3 Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, PBS aprobará la solicitud de renovación del certificado y proceder a su emisión y entrega.

PBS notifica al solicitante la aprobación o denegación de la solicitud.

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

4.7.2.4 Tramitación de las peticiones de renovación online

La solicitud de una renovación del certificado se realizará de acuerdo con lo siguiente:

- Cuando el certificado digital de un usuario esté próximo a caducar, PBS podrá enviar una o más notificaciones distribuidas en el tiempo, invitándole a su renovación.
- El firmante se conectará al servicio de renovación de la página web de PBS y procederá a la solicitud de renovación.
- El firmante firmará la renovación de su certificado válido.
- Se procederá a la generación del nuevo par de claves y generación e importación del certificado, respetando los siguientes condicionantes:
- 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 del usuario sobre sus propias claves, no pudiendo la propia PBS o sus Autoridades de Registro deducirlas o utilizarlas.

4.7.2.5 Notificación de la emisión del certificado renovado

PBS notifica la emisión del certificado al suscriptor y a la Persona natural identificada en el certificado.

4.7.2.6 Conducta que constituye aceptación del certificado renovado

El certificado se considerará aceptado al firmar electrónicamente la renovación.

4.7.2.7 Publicación del certificado renovado

PBS publica el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

4.7.2.8 Notificación de la emisión a terceros

PBS 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

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

Un certificado será revocado cuando concurre alguna de las siguientes causas:

4.9.1.1 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.

4.9.1.2 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.
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.
e) 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.

4.9.1.3 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 PBS y el suscriptor.
b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la Persona natural 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.

4.9.1.4 Otras circunstancias:

a) La terminación del servicio de certificación de la Entidad 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:
    1. La naturaleza y el número de quejas recibidas.
    2. La identidad de las entidades que presentan las quejas.
    3. La legislación relevante vigente en cada momento.
    4. 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 PBS 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, PBS 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 PBS 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.

4.9.5 Procedimientos de solicitud de revocación, suspensión o reactivación

La entidad que precise revocación, suspensión o reactivación un certificado puede solicitarlo directamente a PBS o a la Autoridad de Registro del suscriptor o realizarlo él mismo a través del servicio online disponible en la página web de PBS. La solicitud de revocación, suspensión o reactivación deberá incorporar la siguiente información:

- Fecha de solicitud de la revocación, suspensión o reactivación.
- Identidad del suscriptor.
- Nombre y título de la persona que pide la revocación, suspensión o reactivación.
- Información de contacto de la persona que pide la revocación, suspensión o reactivación.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, por PBS, 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 PBS en la dirección: https://www.pbssoluciones.com

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 PBS.

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 PBS.

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 PBS o en su caso de la Autoridad de Registro. Si se realiza a través del servicio online, será inmediata.

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 la Entidad de Certificación de PBS.

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

PBS CA1

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

PBS CA2

- http://crl1.uanataca.com/public/pki/crl/PBSCA2.crl
- http://crl2.uanataca.com/public/pki/crl/PBSCA2.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 (LRCs)

PBS 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.

4.9.10 Plazo máximo de publicación de LRCs

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún 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 PBS, que se encuentra disponible las 24 horas de los 7 días de la semana en el web:

- *https://download.hightech-corp.com/PBSCA.cer*

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

- *Autoridad de Certificación Raíz (AUTORIDAD DE CERTIFICACIÓN RAIZ EL SALVADOR):*
  - http://crl1.firmaelectronica.minec.gob.sv/crl/arl_minec.crl
  - http://crl2.firmaelectronica.minec.gob.sv/crl/arl_minec.crl

- *Autoridad de Certificación Intermedia 1 (PBS CA1):*
  - http://crl1.uanataca.com/public/pki/crl/PBSCA1.crl
  - http://crl2.uanataca.com/public/pki/crl/PBSCA1.crl

- *Autoridad de Certificación Intermedia 2 (PBS CA2):*
  - http://crl1.uanataca.com/public/pki/crl/PBSCA2.crl
  - http://crl2.uanataca.com/public/pki/crl/PBSCA2.crl

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

PBS 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.

4.9.13 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada 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.

4.9.14 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.

PBS 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

PBS 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.

5 Controles de seguridad física, de gestión y de operaciones

PBS y UANATACA, S.A., han suscrito un contrato de prestación de servicios de tecnología en el que UANATACA provee la infraestructura de clave pública (PKI) que sustenta el servicio de confianza de PBS.

En el presente apartado, se describen los sistemas de seguridad con que cuenta el Centro de Procesamiento de Datos donde se aloja el sistema que contiene la infraestructura de clave pública PKI del servicio de la Autoridad de Certificación de Información de PBS.

La Infraestructura de Clave Pública PKI de la Autoridad de Certificación de PBS, está ubicada en un rack / armario aislado físicamente del resto de infraestructuras hospedados en el Centro de Procesamiento de Datos del proveedor de servicios de tecnología ADAM Ecotech (en lo sucesivo ADAM).

El Centro de Procesamiento de Datos de producción y contingencia se encuentra ubicado en una instalación segura dentro del edificio de ADAM. El mismo ha sido diseñado con tecnología TIER 3, el cual permite tener un esquema redundante para garantizar la continuidad en la operación y disponibilidad de los sistemas y cuenta con los controles de seguridad que se definen a continuación.

5.1 Controles de seguridad física

Se han 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 a 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.

5.1.1 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.

Se 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

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) 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 donde se llevan a cabo procesos de certificación 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 los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.1.3 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.

5.1.4 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.

5.1.5 Prevención y protección de incendios

Las instalaciones y activos 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

Se realiza el uso de 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

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 ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1 Funciones fiables

Se ha identificado, de acuerdo con la 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 Registro:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor y emitir certificados electrónicos.
- **Oficial de Revocación:** Persona responsable de realizar los cambios en el estado de un certificado, principalmente proceder con la suspensión y revocación de los mismos.
- **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.

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.

5.2.2 Número de personas por tarea

Se 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 de Certificación, y en general cualquier manipulación del dispositivo de custodia de las claves de las Autoridades de certificación 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 certificación.
- 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

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.

Se asegura de que el personal de registro es confiable para realizar las tareas de registro. El Administrador de Registro recibe formación para realizar las tareas de validación de las peticiones.

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.

No se 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.

En todo caso, las Autoridades de Registro podrán establecer procesos de comprobación de antecedentes diferentes, siempre preservando las políticas establecidas, siendo responsables por la actuación de las personas que autoricen en sus operaciones.

5.3.2 Procedimientos de investigación de historial

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.

PBS obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales en cumplimiento de la normativa vigente en materia de protección de datos personales.

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.

5.3.3 Requisitos de formación

Se 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 PBS. 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

Se 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.

5.3.5 Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6 Sanciones para acciones no autorizadas

Se 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.

5.3.7 Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados. Cualquier acción que

comprometa la seguridad de los procesos aceptados podría, 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, la entidad 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.

5.3.8 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.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de eventos registrados

Se 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 AC 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 AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- 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 de la Entidad 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

Se revisan 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.

5.4.3 Período de conservación de registros de auditoría

Se almacena la información de los logs durante un periodo de entre 1 y 15 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 AC.

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

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 backup de los logs.

PBS 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, 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 PBS.

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

Se 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 PBS (o por las entidades de registro):

- 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 Entidad 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.
- 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.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

PBS y/o las Autoridades de Registro según corresponda, serán responsables del correcto archivo de todo este material.

5.5.2 Periodo de Conservación de registros

Se archivan los registros especificados anteriormente durante al menos 15 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 15 años o el periodo que establezca la legislación vigente desde su cambio de estado.

5.5.3 Protección del archivo

Se 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.

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

5.5.4 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, se (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

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

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

5.5.7 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. Se proporcionan tanto 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 AC 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 AC. Se generará una nueva AC 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

Se han 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.

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 con las políticas de seguridad y gestión de incidentes, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres.

5.7.3 Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de PBS, 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.

5.7.4 Continuidad del negocio después de un desastre

Se restablecerán 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.

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.

5.8 Terminación del servicio

Se asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del Proveedor de Servicios de certificación. En este sentido, se garantiza un mantenimiento continuo de los registros definidos en el apartado 5.5.1, por el tiempo establecido en el apartado 5.5.2 de esta Declaración de Prácticas de Certificación.

No obstante lo anterior, si procede se 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 o la previsión legal que corresponda.

Antes de terminar sus servicios, se desarrolla 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 Firmantes/Suscriptores, Tercero que confían y otras AC's 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 la AC en el procedimiento de emisión de certificados.
- 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.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- 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 Organismo Supervisor Nacional, con una antelación mínima de 90 días hábiles, 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 Organismo Supervisor Nacional, 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

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 de la entidad de certificación intermedia "PBS CA1" ha sido creada por la entidad de certificación raíz "AUTORIDAD DE CERTIFICACIÓN RAIZ EL SALVADOR" de acuerdo con los procedimientos de ceremonia de PBS, 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 CISA. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por PBS.

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

PBS CA1	4.096 bits	15 años
• Certificados de entidad final	2.048 bits	Hasta 5 años
• Certificados de la Unidad de Sello de tiempo (TSU)	2.048 bits	Hasta 5 años

Los documentos Texto de Divulgación (PKI Disclosure Statement-PDS) de todos los perfiles de certificados electrónicos indicados en el presente documento, se encuentran accesibles bajo el enlace https://www.pbssoluciones.com

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 PBS. Las claves no generadas en un QSCD, serán generadas por el firmante. Nunca se generan claves fuera de un QSCD para ser enviadas al firmante.

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

En certificados en dispositivo seguro de creación de firma la clave privada se genera y se almacena debidamente protegida en el interior de dicho dispositivo. 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.

En certificados en archivo p12 la clave privada del firmante se genera y se almacena en el sistema informático que utiliza este firmante cuando realiza la solicitud del certificado, por lo que en este caso no existe envío de clave privada, garantizando el control exclusivo de la clave por parte del usuario

6.1.3 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.

6.1.4 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.

El certificado de las Autoridades de Certificación Raíz y Subordinadas estará a disposición de los usuarios en la página web de PBS.

6.1.5 Tamaños de claves

- 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.

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 CA 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 digital, el no repudio y cifrado de datos.

6.2 Protección de la clave privada

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

6.2.1 Estándares de módulos criptográficos

En relación con los módulos que gestionan claves de PBS y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

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 AC. 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

No se almacenan copias utilizables por medios propios de las claves privadas de los firmantes.

6.2.4 Copia de respaldo de la clave privada

PBS realiza copia de seguridad de las claves privadas de las CA 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 es posible realizar backups de las claves, ya que no es posible su exportación. Si estas se encuentran en un HSM, es posible realizar backups de un bloob 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 AC son archivadas por un periodo de **15 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 también se guardará copia de la clave privada asociada al certificado de cifrado.

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 PBS.

6.2.7 Método de activación de la clave privada

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos de producción de PBS.

6.2.8 Método de desactivación de la clave privada

La clave privada de PBS 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 AC 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 PBS se seguirán los pasos descritos en el manual del administrador del equipo criptográfico 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 PBS. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante en hardware y podrán ser destruidas mediante una aplicación informática especial en las dependencias de las RA o de PBS.

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

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

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 PBS 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, se 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 subordinadas, 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

PBS emplea sistemas fiables para ofrecer sus servicios de certificación. PBS 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, 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 backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

6.5.1 Requisitos técnicos específicos de seguridad informática

Cada servidor incluye las siguientes funcionalidades:

1. Control de acceso a los servicios de las Autoridades de Certificación subordinadas y gestión de privilegios.
2. Imposición de separación de tareas para la gestión de privilegios.
3. Identificación y autenticación de roles asociados a identidades.
4. Archivo del historial del suscriptor, de las Autoridades de Certificación subordinadas y datos de auditoria.
5. Auditoria de eventos relativos a la seguridad.
6. Auto-diagnóstico de seguridad relacionado con los servicios de las Autoridades de Certificación subordinadas.
7. 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 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 PBS son fiables.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por PBS 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

PBS 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 por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

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

6.6.3 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.

6.6.4 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.

6.6.5 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

El departamento de Sistemas 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.

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 económica que supone la resolución de la incidencia.

Procedimientos operacionales y responsabilidades

Se definen 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.

6.7 Gestión del sistema de acceso

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

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.

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.

6.8 Gestión del ciclo de vida del hardware criptográfico

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.

PBS 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.

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

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

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

La configuración del sistema de PBS, 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.

6.9 Controles de seguridad de red

PBS 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.

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

6.11 Fuentes de Tiempo

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

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

PBS en el caso de modificación del estado de la certificación de los dispositivos seguros de creación de firma (SSCD), procederá de la siguiente manera:

- PBS 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.
- En el supuesto de finalización del periodo de validez o pérdida de la certificación, PBS no utilizará dichos SSCD para la emisión de nuevos certificados electrónicos, bien sea en nuevas emisiones como eventualmente en posibles renovaciones.
- Procederá de inmediato a cambiar a de dispositivos SSCD con certificación válida.
- 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 electrónicos emitidos en estos dispositivos y reemplazarlos emitiéndolos en SSCD válidos.

7. Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

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

La documentación relativa a los perfiles de la norma EN 319 412 puede solicitarse a PBS.

7.1.1 Número de versión

PBS emite certificados 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, 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 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 por el Organismo Supervisor Nacional y se encuentra sometida a las revisiones de control que este organismo considere necesarias.

8.1 Frecuencia de la auditoría de conformidad

Se 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 Unidad de Firma Electrónica del MINEC por tal de dar conformidad relativa a la ley de firma electrónica y demás normativa y guías aplicables.

8.3 Relación del auditor con la entidad auditada

Se declara que no existe ningún conflicto de intereses que pueda desvirtuar su actuación entre la Unidad y 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 electrónicos así como, los métodos de identificación previstos por la legislación de el Salvador tanto presenciales como a distancia
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

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, 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 Comité de Seguridad de PBS 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.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Seguridad de PBS 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 de emisión o renovación de certificados

Se 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

No se ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3 Tarifa de acceso a información de estado de certificado

No se 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

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

PBS ha constituido una fianza que mantiene vigente en los términos previstos en los artículos 9 y 10 del Reglamento de la Ley de Firma Electrónica.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura para suscriptores y terceros que confían en certificados

PBS ha constituido una fianza que mantiene vigente en los términos previstos en los artículos 9 y 10 del Reglamento de la Ley de Firma Electrónica.

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales:

- 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 Proveedor 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 la Autoridad 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 la Entidad de Certificación.

- El nombre y los apellidos de la Persona natural identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- 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 (LRCs), 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

PBS 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.

Se indicarán estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5 Divulgación de información por petición de su titular

Se 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.

9.3.6 Otras circunstancias de divulgación de información

Sin estipulación.

9.4 Protección de datos personales

PBS garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales especialmente en lo referente al artículo 5 de la ley de firma electrónica de El Salvador.
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 la política de privacidad aplicable a todos los servicios de certificación de PBS en el que se detalla toda la información necesaria con respecto al tratamiento de datos personales realizado por PBS

Finalidad del tratamiento
PBS 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 PBS, la cual se encuentra disponible en el siguiente enlace: https://www.pbssoluciones.com

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

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.

Los datos serán obtenidos directamente de los solicitantes de los certificados.

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 soporte.sv@grouppbs.com

Transferencia de datos

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

Datos tratados y conservación

Las categorías de datos personales tratados por PBS, 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, vídeos y/o cuando corresponda el patrón biométrico facial, con la finalidad de poder llevar a cabo el proceso de vídeo identificación de PBS.

Los datos personales se conservarán hasta la finalización de la relación contractual y posteriormente, durante los plazos legalmente exigidos acorde a cada caso. Como norma general, los datos personales relativos al servicio se conservarán durante 15 años desde la revocación del certificado correspondiente.

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 soporte.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

9.5.1 Propiedad de los certificados e información de revocación

Únicamente PBS 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 electrónicos y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por PBS contienen un aviso legal relativo a la propiedad de los mismos.

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 PBS 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.

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 PBS

PBS 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 con las indicaciones contenidas en este documento.

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

PBS 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 los textos de divulgación (PDS) de cada uno de los certificados adquiridos.

El documento de texto de divulgación, también denominado PDS, cumple el contenido del anexo A de la ETSI EN 319 411-1, documento el cual puede ser transmitido por medios

electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

PBS vincula a suscriptores, poseedores de claves 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 las secciones 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados

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

PBS como mínimo, garantiza al suscriptor:

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

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

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4.
- 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, PBS garantiza al suscriptor y al tercero que confía en el certificado:

- 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 de la Entidad de Certificación, con los límites que se establezcan.

9.6.3 Rechazo de otras garantías

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

9.6.4 Limitación de responsabilidades

PBS limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados por la Entidad de Certificación.

9.6.5 Cláusulas de indemnidad

9.6.5.1 Cláusula de indemnidad de suscriptor

PBS incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad 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 a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- 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

PBS incluye en el texto de divulgación o PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad 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

PBS incluye en el texto de divulgación o PDS, cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7 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.

9.6.8 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, la Entidad de Certificación vela porque, al menos los 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

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 salvadoreños.

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

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

10. Anexo I - Acrónimos

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
DSCF	Dispositivo Seguro de Creación de Firma
SSCD	Secure Signature Creation Device. Dispositivo Seguro 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