Declaración de las Prácticas de Certificación

ABANCERT

Versión: 1.0

Fecha Vigencia: 07 de diciembre 2021

Contenido

RESUMEN DE LOS DERECHOS FUNDAMENTALES CONTENIDOS EN ESTA CP

ESTE TEXTO CONTIENE UNA VISIÓN CLARA DE LOS OBJETIVOS, DERECHOS Y OBLIGACIONES QUE RIGEN EN LA RELACIÓN JURÍDICA CON ABANCERT.

- Esta CP y los documentos afines regulan todo lo relativo a la solicitud, emisión, aceptación, renovación y revocación de certificados entre otros muchos aspectos vitales para la vida del certificado y el régimen jurídico que se establece entre el Titular, ABANCERT, los usuarios y terceros.
- Tanto la CP como los demás documentos afines y complementarios son publicados y puestos a disposición para los solicitantes, Titulares y Usuarios en la dirección de Internet: http://www.abancert.cl/assets/doc/DeclaracionPracticasCertificacion.pdf para que conozcan las normas y reglas aplicables a su sistema de certificación.
- ABANCERT emite varios tipos de certificados, por lo que el Solicitante de un certificado deberá conocer las condiciones de uso establecidas en la CPS y en las correspondientes Políticas de Certificación específicas de ese tipo de certificado, de manera que pueda proceder correctamente a la solicitud y uso del certificado.
- Es necesario que el Titular tome los resguardos de custodiar las claves privadas de su certificado. Al respecto, si llegara a ocurrir alguna de las causas de revocación del certificado establecidas en esta CPS (Indicadas en Puntos 4.2.1), es necesario que realice al instante la solicitud o petición de revocación como propietario del certificado, informando inmediatamente a ABANCERT, para que de esta manera proceda a su revocación, de manera de evitar el uso ilegítimo del certificado por parte de un tercero no autorizado.
- El Titular debe hacer un uso correcto del certificado, y será de su exclusiva responsabilidad la utilización del certificado de forma diferente a los usos previstos en la CPS.
- Es obligación del Usuario o Titular, comprobar en el repositorio de certificados publicado en: https://www.abancert.cl/CertificadoEstado.aspx por ABANCERT, que el certificado en el que pretende confiar, es válido y no ha caducado o ha sido revocado.
- En la CPS se establece la responsabilidad de ABANCERT y de los Usuarios o Titulares, así como las limitaciones ante posibles daños y perjuicios.
- Para más información, consulte nuestra página web en la dirección https://www.abancert.cl o contáctese al correo: contacto@abancert.cl.

1. INTRODUCCIÓN

1.1. PRESENTACIÓN

El presente documento constituye el Estatuto de Prácticas de Certificación (Certificate Practice Statement) del servicio de certificación de ABANCERT, al cual se hará referencia mediante el acrónimo de su denominación en inglés CPS.

1.2. IDENTIFICACIÓN

El presente documento se denomina “Declaración de las prácticas de Certificación de ABANCERT” y puede localizarse en la siguiente dirección: http://www.abancert.cl/assets/doc/DeclaracionPracticasCertificacion.pdf

1.3. COMUNIDAD DE USUARIOS Y APLICACIONES

Los certificados de Firma Electrónica Avanzada, FEA, permiten que las personas puedan firmar electrónicamente transacciones y documentación de esta clase. Identifica al usuario o titular de forma única y podrá utilizarse en aquellas aplicaciones que precisen firma electrónica mediante certificados digitales X.509 v3 emitidos bajo la Política Firma Electrónica Avanzada. Este certificado permitirá firmar solo ajustándose a lo establecido en la ley 19.799 y su reglamento.

El usuario o Titular de este tipo de certificados podrá ser cualquier persona natural, siempre que aplique a los criterios establecidos en la presente Práctica de Certificación (CPS), la Ley 19.799 y su reglamento especificado en el Decreto 181.

Los certificados FEA podrán ser utilizados por usuarios o titulares pertenecientes a organismos del Estado para realizar actos, celebrar contratos y expedir cualquier documento, exceptuando las no aplicaciones que se mencionen en el artículo 6° de la Ley 19.799.

Firma y no repudio

El receptor de un mensaje o documento firmado con el certificado, puede usar la clave pública del emisor para verificar que este último ha usado su clave privada para firmar el mensaje o documento. Esto permite confirmar frente a un tercero, la identidad del emisor del mensaje o documento y la no alteración de este.

El mensaje o documento firmado puede corresponder a una transacción y documento electrónico con validez legal según la legislación vigente, en especial la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación.

Integridad

El uso de los servicios de certificados y de FIRMA ELECTRÓNICA AVANZADA permite asegurar al receptor de un mensaje o documento, que no ha sido alterado entre el envío y la recepción.

a. Autoridad Certificadora

ABANCERT actúa como Prestadora de Servicios de Certificación (PSC) y al emitir un certificado, relaciona una determinada clave pública y privada con un sujeto o entidad concretos. A su vez los desvincula al revocar dicho certificado, de conformidad con los términos de esta CPS.

b. Autoridad de Registro

Corresponde a una entidad intermedia entre la Autoridad de Certificación (AC) y los solicitantes, encargándose de la detección, comercialización y administración de las solicitudes de certificación. Siendo su principal función, comprobar fehacientemente la identidad, registrando los antecedentes, permitiendo establecer los atributos de los usuarios finales de ser sujetos a certificar.

La AC podrá valerse de una o varias Autoridades de Registro (AR) (internas o externas contratadas para este fin), quienes deberán llevar a cabo el proceso de comprobar fehacientemente la identidad del Solicitante.

c. Titular

El usuario o Titular del certificado será la persona que utiliza bajo su exclusivo control un certificado de firma electrónica - Art. 2, letra h) Ley 19799.

d. Solicitante

Solicitante será la persona que comparece personalmente ante la Autoridad Certificadora permitiendo la comprobación fehaciente de su identidad, para la solicitud del otorgamiento del certificado, según lo dispuesto en la CP, CPS y ley 19799.

e. Tercera Persona que Confía

Persona que utiliza bajo su exclusivo control un certificado de firma electrónica avanzada.

Cuando el usuario o titular decida voluntariamente confiar y hacer uso del certificado le será de aplicación la presente CPS.

f. Tipo de Certificado

El tipo certificado que se ofrecen dentro del ámbito de esta CPS están definidos en la POLÍTICAS DE CERTIFICACIÓN (CP) y disponible en https://www.abancert.cl/assets/doc/PoliticaCertificadosFEA.pdf. La CP regula la aplicabilidad del certificado en relación con una comunidad de usuarios, algunos usos y restricciones determinados con requerimientos de seguridad comunes.

g. Limitaciones de Uso

Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que éstos vayan cambiando.

Estos certificados son válidos para asumir las responsabilidades económicas y compromisos en nombre propio, permitidos por la Ley 19.799 y en general serán válidos para los usos descritos en este documento.

No se permite un uso del certificado contrario a:

- La normativa chilena y a los convenios internacionales ratificados por el Estado Chileno
- Lo establecido en la CPS, en la Política de Certificación y en los contratos que se firmen entre la AC (Autoridad Certificadora) / AR (Autoridad de Registro) y el Titular.

Los certificados de ABANCERT no podrán ser alterados, deberán utilizarse tal y como son suministrados por la AC.

1.4. DETALLES DE CONTACTO

Atención: Atención Clientes ABANCERT
Román Díaz 1180, Providencia, Santiago de Chile.
E-mail: contacto@abancert.cl
E-mail: soporte@abancert.cl
Lunes a Viernes: 09:30 – 13:00 hrs. y de 15:00 – 17:00 hrs.

2. CONDICIONES GENERALES

2.1. OBLIGACIONES

2.1.1. OBLIGACIONES del PSC.

Obligaciones de ABANCERT, como prestadora de servicios de certificación son todas aquellas obligaciones impuestas por la presente CPS:

- Asegurar conformidad de sus procesos y actividades con las prácticas de certificación definidas en este documento y las respectiva CP.
- Emitir certificados haciendo uso de tecnologías y criptografía que permitan un adecuado proceso de certificación.
- Apoyar la emisión de certificados con las tecnologías que permitan el resguardo de las llaves privadas de los titulares de ABANCERT.
- Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley Nº 19.628, sobre Protección de la Vida Privada.
- Utilizar mecanismos de comprobación fehaciente de la identidad del solicitante y garantizar una identificación fidedigna.
- Almacenar la información obtenida del proceso de enrolamiento (ficha de registro, impresión huella dactilar, fotografía del titular y fotocopia de cedula de identidad por ambos lados) en un sistema de custodia documental manual.

Frente a los Titulares

- Notificar al Titular de la emisión de su certificado.
- Notificar al Titular de la revocación de su certificado.
- Mantener actualizados los registros de certificados vigentes y certificados revocados, en concordancia con la ley 19799.
- Revocar certificados que no cumplan con declaraciones de las CPS o de la CP correspondiente al tipo de certificado.

Frente a la tercera parte interesada

- Cumplir de manera sustancial con el contenido de esta CPS.
- Poner a disposición de los usuarios los certificados que componen la(s) cadena(s) de confianza de ABANCERT.

2.1.2. OBLIGACIONES DE LA AR

La AR asumirá las siguientes obligaciones de las cuales será responsable.

- Comprobar fehacientemente la identidad del Titular, conforme a los procedimientos que se establece en esta CPS y en las Políticas de Certificación, utilizando cualquiera de los medios admitidos en derecho, que para los certificados de FEA es la comparecencia personal y directa del solicitante.
- Mantener y garantizar existencia de registro electrónico de los antecedentes de los suscriptores a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley N.º 19.628, sobre Protección de la Vida Privada, Cumplir con las demás obligaciones legales, Art. 385 especialmente las establecidas en esta ley, su reglamento, y D.O. 09.01.2014 las leyes N.º 19.496, sobre Protección de los Derechos de los Consumidores, y N.º 19.628, sobre Protección de la Vida Privada.
- Almacenar de forma segura la documentación aportada, tanto para el proceso de emisión del certificado, como para el proceso de revocación.
- Llevar a cabo cualesquiera otras funciones que le correspondan, a través del personal que sea necesario en cada caso, conforme se establece en esta CPS.
- Aplicar medidas de seguridad adecuada y suficiente para salvaguardar la llave privada del titular, al momento de generación del certificado.

La AR deberá disponer a la PSC del expedito acceso a los antecedentes, archivos y procedimientos relacionados al enrolamiento y entrega de los

certificados, para una eventual investigación o sospecha de infracción de la CPS y/o de las Políticas de Certificación.

Todas las funciones atribuidas a la AR externa, podrán ser desempeñadas de forma directa por parte del PSC como AR interna.

2.1.3. OBLIGACIONES DEL SOLICITANTE

Los usuarios de los certificados de firma electrónica quedarán obligados, en el momento de proporcionar los datos de su identidad personal u otras circunstancias objeto de certificación, a brindar declaraciones exactas y completas. Además, estarán obligados a custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador, y a actualizar sus datos en la medida que éstos vayan cambiando.

2.1.4. OBLIGACIONES DEL TITULAR

- Conservar y utilizar correctamente el certificado.
- Custodiar el certificado, tomando las precauciones razonables para evitando su pérdida, evitando la revelación de clave privada a un tercero, evitando una mala utilización o uso no autorizado del certificado.
- Proteger diligentemente el uso de password y el dispositivo portable seguro (e-Token, Fips 140 - 2 Nivel 3) que cumpla con los estándares establecidos para la emisión de dicho certificado.
- Solicitar la revocación del certificado cuando se cumpla alguno de los supuestos previstos en el epígrafe titulado “REVOCACIÓN DE CERTIFICADOS” de la presente CPS.
- No revelar la clave privada ni el código de activación del certificado.
- Asegurarse de que toda la información contenida en el certificado es correcta y en conformidad al Art. 24 de la Ley 19.799 y notificar inmediatamente a la AR o PSC, según corresponda.
- Informar inmediatamente a la AR o el PSC acerca de cualquier situación que pueda afectar a la validez del certificado.
- Realizar un debido y correcto uso del certificado, según se desprende de esta CPS y de las Políticas de Certificación. Será responsabilidad del Titular el uso indebido que éste haga del Certificado Electrónico Avanzado, según lo indicado en el Art. 24 de la Ley 19799.

- Cualquier otra obligación que exija la ley 19.799, en esta CPS o de las Políticas de Certificación.

2.1.5. OBLIGACIONES DE LOS PROVEEDORES

- Las empresas Proveedoras de servicios deberán cumplir con las políticas de seguridad de la información, mantener un procedimiento para el tratamiento de riesgos y contratos que aseguren la oportuna entrega de servicios con ABANCERT.

2.1.6. OBLIGACIONES DE LAS TERCERAS PARTES INTERESADAS

- Las terceras partes interesadas que pretendan confiar y usar los certificados emitidos por el PSC deberán verificar la validez de las firmas emitidas por los Titulares.
- En el supuesto de que los usuarios o terceras partes interesadas, no realicen la verificación de los certificados a través del OCSP (Estado de un certificado en línea) o la CRL (Lista de certificados revocados), el PSC no se hace responsable del uso y confianza que hagan de estos certificados.

2.1.6.1 CONFIANZA DE LAS FIRMAS

Toda persona puede confiar en una firma electrónica emitida mediante un certificado ABANCERT, debiendo tener las siguientes consideraciones:

a. Si la parte que confía, ha adoptado las medidas adecuadas para determinar la fiabilidad de la firma y en particular, si ha verificado que el certificado usado para firmar poseía una cadena de confianza.

b. Si la parte que confía, confirmó si la firma estaba en entredicho o había sido revocada, según el punto 4 de esta CPS.

c. Si la parte que confía, confirmó las políticas y procedimientos que rigen la actividad con relación a las firmas generadas mediante certificados emitidos por ABANCERT, que se especifican en esta CPS y en las Políticas de Certificación, publicadas en: https://www.abancert.cl/assets/doc/PoliticaCertificadosFEA.pdf

2.2. RESPONSABILIDAD

2.2.1. Responsabilidad del PSC

La PSC no será responsable de los daños derivados de errores u omisiones de las obligaciones por parte del titular.

El PSC no será responsable de la incorrecta utilización de los certificados ni de cualquier daño indirecto que pueda resultar de su mal uso.

Previa acción a cualquier emisión de certificado, El PSC no será responsable por el retraso o la no ejecución de cualquiera de las obligaciones de esta CPS a consecuencia de un acto de fuerza mayor, caso fortuito o en general, cualquier circunstancia que la PSC no pueda poseer control razonable, como por ejemplo: Desastres naturales, guerra, estado de sitio, alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico, de comunicación o básico, virus informáticos, estado de emergencia sanitaria, pandemias, endemia, estados de excepción y/o catástrofes en general.

Será responsabilidad del Titular de disponer de todos los elementos técnicos necesarios para el normal funcionamiento y uso de del Certificado.

El PSC no será responsable del contenido de los documentos suscritos electrónicamente mediante cualquier certificado.

El PSC se compromete a mantener vigente y disponer un seguro de responsabilidad civil que cubra el valor mínimo exigido por el Art. 14, inciso 4 de la Ley 19799.

2.2.2. Responsabilidad de la AR

La AR responderá de las funciones que le correspondan conforme a esta CPS y, en especial, asumirá toda la responsabilidad por la correcta comprobación fehaciente de la identidad del solicitante, con las mismas limitaciones que se establecen en el apartado 2.1.2 de esta CPS con relación al PSC.

2.2.3. Responsabilidad del Titular

El Titular es responsable de custodiar el Certificado, tomando las precauciones razonables para evitar su pérdida, modificación o uso no autorizado y garantizar su seguridad, así como la del procedimiento para el cual se emiten, especialmente cuidando de no divulgar las claves privadas, especialmente si existe la posibilidad de extravío, hurto o sustracción indebida.

2.3. RESPONSABILIDAD FINANCIERA

Las responsabilidades que afecta la operación de ABANCERT están establecidas y limitadas a lo establecido en el artículo 14 de la Ley 19.799.

2.4. INTERPRETACIÓN Y EJECUCIÓN

2.4.1. Ley Aplicable.

ABANCERT cumple con las obligaciones establecidas por la Entidad Acreditadora, a los requerimientos de la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación” – EA-103 Versión 2.4 establecida por la Entidad Acreditadora. vigente, a lo establecido en la Ley 19.799 de 2002, ley 19.799 de 2007, el Decreto 181 de 2002, modificación del Decreto 181 de 2012, y los reglamentos que los modifiquen o complementen.

2.4.2. Subrogación, Novación y Notificaciones

El PSC se reserva el derecho de transmitir en el futuro todas las obligaciones y derechos que se deriven de esta CPS a un tercero para que éste continúe prestando el servicio de certificación. "En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad." Esta CPS seguirá siendo el documento que regule las relaciones entre las partes mientras no se cree un nuevo documento por escrito.

El PSC podrá modificar cualquiera de las cláusulas de la presente CPS en los términos previstos en esta CPS, "siempre que no afecte derechos del titular (consumidor) en relación a la Ley 19496 y Ley 1968. Este caso se puede presentar en caso de perder la acreditación, según causas del Artículo 19, letra b) de la Ley 19799”.

2.4.3. Tasas de Registro por la Expedición y Renovación de certificados.

El costo por la emisión o renovación de los certificados serán puestas a disposición de los solicitantes, usuarios o titulares por el PSC, la cual podrá establecer promociones especiales, ofertas o similares que modifiquen las tarifas previamente establecidas.

2.5. PUBLICACIÓN Y DEPÓSITO DE LA CPS

El contenido de esta CPS, así como de toda la información que se publique, estará disponible a título informativo en la dirección de Internet: https://www.abancert.cl/assets/doc/DeclaracionPracticasCertificacion.pdf y los originales estarán depositados en las oficinas del PSC.

2.6. SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

La seguridad de los equipos es resultado del análisis de las medidas de seguridad que mantiene nuestros proveedores de servicios en respuesta a la probabilidad e impacto de amenazas producto de omisiones o brechas de seguridad", según lo dispuesto en los requisitos de seguridad dispuestos en los dominios PS01 al PS07, que determinan los niveles de seguridad que dispone el PSC.".

2.7. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

2.7.1. Confidencialidad de las Claves de Firma Electrónica Avanzada

El Operador AR, entregará un dispositivo criptográfico y pondrá a disposición una interfaz o aplicativo, donde ABANCERT entregará al titular credenciales únicas y provisorias que le permita acceder al servicio de descarga de la firma electrónica, luego de realizada la descarga por el Titular deberá crear su clave propietaria del certificado, quedando a total control y administración de su Firma Electrónica en su dispositivo criptográfico “token FIPS 140-2 Nivel 3”. En caso de dudas se entregará el soporte y asistencia por el operador de la AR."

2.7.2. Confidencialidad en la Prestación de Servicios de Certificación

La información de los titulares de certificados es de carácter confidencial (Art. 23 párrafo 2° de la ley 19.799), por lo tanto, estos datos e información serán tratados por ABANCERT de acuerdo a las obligaciones según lo dispuesto por Artículo 12 b) de la ley N.°19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma.

2.7.3. Protección de Datos

La información de los titulares de certificados es de carácter confidencial (Art. 23 párrafo 2° de la ley 19.799), ABANCERT de acuerdo a las obligaciones y lo dispuesto por Artículo 12 b) de la ley N.°19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma, donde se estipula que la PSC debe mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para ese efecto, y no podrá utilizarlos para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley N.º 19.628, sobre Protección de la Vida Privada y lo relativo al Titular en su rol de consumidor, las disposiciones de la ley N.º 19.496, Sobre Protección a los Derechos de los Consumidores.

2.7.4. Tipos de Información que debe mantenerse Confidencial y Privada

ABANCERT no utilizará la información de los titulares para otros fines que los exclusivos y relacionados con sus actividades de certificación, ni compartirá esta información con terceros.

En relacionado a lo anterior, ABANCERT, como política general, no entrega información personal de sus clientes.

Sin perjuicio de lo anterior, los certificados emitidos por ABANCERT contienen información de identificación del titular, y el contenido del certificado está definido en la Ley N.º 19.799.

El certificado de firma electrónica avanzado contiene los siguientes campos obligatorios de información de los titulares:

- RUT
- Correo electrónico
- Nombre titular
- Tipo de certificado
- Empresa emisora de certificado PSC
- Datos de la acreditación de ABANCERT (Declaración del emisor)

2.7.5. Tipos de Información que no se considera Confidencial ni Privada

ABANCERT declara que los Certificados, la revocación de Certificados y la información contenida en ellos, no se consideran Información Confidencial/Privada. Asimismo, se establece que dicha información es tratada de conformidad con el artículo 12 b) de la ley 19.799.

2.8. DERECHOS DE PROPIEDAD INTELECTUAL

El PSC es titular de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta CPS. Se prohíbe, por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son titularidad exclusiva del PSC sin la autorización expresa por su parte. No obstante, no necesitará autorización del PSC para la reproducción del Certificado cuando la misma sea necesaria para la utilización del Certificado por parte del usuario legítimo y con arreglo a la finalidad del Certificado, de acuerdo con los términos de esta CPS.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. REGISTRO INICIAL

3.1.1. Tipos de Nombres

Los certificados de la CA de ABANCERT están basados en la estructura x509 v3 que contiene los datos expresados en notación DN (Distinguished Name), donde un DN se compone a su vez de diversos campos. Los DN correspondientes al campo SUJETO y ASUNTO de ABANCERT consiste en los elementos que se especifican en el Cuadro siguiente.

Atributo	Valor
País (C) =	“CL”
Organización (O) =	ABANCERT
Unidad Organizacional (UO) =	Autoridad Certificadora
Estado o provincia (S) =	Región Metropolitana
Localidad (L) =	Santiago
Dirección de correo electrónico (E) =	contacto@abancert.cl
Nombre Común (CN) =	ABANCERT FIRMA ELECTRÓNICA AVANZADA

En el caso de los datos del titular, los certificados también contienen los datos expresados en notación DN (Distinguished Name) en los campos del SUJETO y ASUNTO, ambos contienen los elementos que se especifican en el cuadro siguiente:

Cuadro – Atributos del DN en los Certificados del Titular Usuario Final

Atributo	***Valor***
País (P) =	"CL"
Organización (O) =	El atributo de la organización se usa como sigue: • El nombre de la empresa del Titular.
Unidad Organizacional (UO) =	Puede contener el departamento organizacional al que pertenece el Titular, por ejemplo, Gerencia.
Estado o Provincia (S) =	Indica el Estado o Provincia o Región.
Localidad (L) =	Indica la Ciudad del Titular.
Nombre Común (CN) =	Este atributo comprende: • Nombre (para los Certificados Individuales).
Dirección de correo electrónico (E) =	Dirección de correo electrónico para los Certificados.
Limitaciones	Contiene los límites establecidos por la AC en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles por tercero.

3.1.2. Singularidad de los Nombres

ABANCERT garantiza que los DN del Sujeto son únicos dentro del dominio de una AR específica a través de elementos del proceso de inscripción del Titular.

3.1.3. Autenticación de la Identidad de la Organización

ABANCERT comprueba la información de la organización ingresada por el solicitante del certificado para efectos de facturación y de la incorporación de la información en el Certificado que son requeridos para el atributo del campo Organización y Unidad Organizacional.

3.2. Solicitud de Certificado

3.2.1. Registro Inicial

El Solicitante deberá llenar el formulario dispuesto por el PSC en su página WEB para la solicitud del certificado. El ingreso de los datos solicitados en este formulario supondrá su consentimiento para ser registrado como Titular de un certificado ABANCERT. La solicitud de este certificado no implicará en ningún caso su obtención del mismo si no llegan a cumplirse por parte del solicitante las cláusulas y condiciones establecidos en la CPS o en la Política de Certificación para los certificados de Firma Electrónica Avanzada.
En el mismo acto el solicitante proporcionará a la AR toda la información que necesite, bien para registrar al Solicitante como Titular, o con la finalidad de incluirla en el certificado, de acuerdo con los requisitos establecidos en esta CPS.

3.2.2. Autenticación de la Identidad del Titular

Para que la AR pueda comprobar fehacientemente la identidad, el Titular deberá estar presencialmente y acreditar todas las menciones básicas del certificado, para lo cual deberá presentar los siguientes documentos:

- Cédula Nacional de Identidad chilena vigente.
- Tratándose de la FIRMA ELECTRÓNICA AVANZADA en que se vayan a incluir antecedentes en el campo Organización y Unidad Organizacional, se solicitara los documentos que acrediten tales calidades.

3.2.3. Confirmación de la Identidad del Titular

La AR solicitará al titular que presente su Cédula de Identidad Chilena, original, vigente y en buen estado, con los datos de la CI se procederá a consultar la validación de los datos en el servicio de Registro Civil e Identificación, el Titular deberá entregar todas las facilidades necesarias para la realizar las validaciones que correspondan, permitiendo comprobar fehacientemente su identificación.

3.2.4. Aceptación de la Solicitud

Una vez superado el proceso de comprobación de solicitud de forma satisfactoria, siempre y cuando no existan circunstancias que de alguna manera afecten a la seguridad del servicio de certificación, la AR procederá a la aprobación de la solicitud.

3.2.5. Rechazo de la Solicitud

Si la AR rechazara la solicitud del certificado (Información no corresponde al titular, cedula de identidad vencida, en mal estado o bloqueada), dicha decisión será comunicada de forma inmediata al Titular y a su vez, formalizada a través de correo electrónico. Si el rechazo es subsanable en forma, el usuario deberá entregar los datos correctos para generar una nueva solicitud vía WEB.

3.3. Aceptación del Certificado

3.3.1. Aceptación del Certificado por parte del Titular

La entrega del Certificado, toma de fotografía, firma e impresión de huella dactilar en el "Contrato de Suscripción de FDA" (este acto es manual y no se utilizan dispositivos tecnológicos), implicará la aceptación del certificado por parte del Titular.

La aceptación del certificado deberá realizarse de forma expresa, por escrito y ante el encargado de la AR.

Aceptando el Certificado, el titular confirma y asume la exactitud del contenido de este, con las consiguientes obligaciones que de ello se derive frente a la AR, la EC o cualquier tercero que de buena fe confíe en el contenido del Certificado.

3.4. Emisión de Certificado

Una vez aceptada por la AR la Solicitud del certificado, se llevará a cabo el registro del solicitante.

Prerrequisitos:

- Entrega de la documentación requerida, correcta y completa.
- Exhibir Cédula de Identidad Nacional o Pasaporte vigente y en buen estado.

La AR se obliga a:

a. Comprobar fehacientemente la identidad del titular.

b. Entregará un dispositivo criptográfico y pondrá a disposición una interfaz o aplicativo, donde ABANCERT entregará al titular credenciales únicas y provisorias que le permita acceder al servicio de descarga de la firma electrónica, luego de realizada la descarga por el Titular deberá crear su clave propietaria del certificado, quedando a total control y administración de su Firma Electrónica en su dispositivo criptográfico. En caso de dudas se entregará el soporte y asistencia por el operador de la AR.

c. Disponer al Titular de una sesión segura, que le permita descargar y almacenar el certificado en un dispositivo portable seguro (token, Fips 140-2 Nivel 3), creando sus claves privadas al cual solo el Titular tendrá a su resguardo, todo este proceso será realizado en dependencias de ABANCERT.

El Titular se obliga a:

a. Dar cuenta de cualquier irregularidad que detecte en el sistema.

b. Presentar su carnet de identidad nacional válido y vigente.

c. Seguir correctamente el proceso solicitado por el operador AR para la emisión del certificado.

d. Revocar en caso de extravío o pérdida.

La AR se reserva el derecho a negarse a emitir certificados cuando concurra cualquier causa justificada, según lo que indica esta CPS en al punto 3.2.5, por lo que no podrá exigirse responsabilidad alguna por este motivo.

3.4.1. Publicación del Certificado

Una vez aceptado el Certificado por parte del Titular, la AR procederá a la publicación de la llave publica, en el Registro de Acceso Público.

La publicación de los datos del Certificado en el Registro de Acceso Público significa que ha sido aceptado para los terceros usuarios de buena fe, que confíen en el certificado.

3.4.2. Contenido del Certificado.

Versión x509v3

3.4.3. Perfil de Certificado de la Política de Firma Electrónica Avanzada

Certificado X509:	**VERSIÓN DE CERTIFICADO**
Versión: V3	
Número de serie: 6c00000002a736fd4a8f64647d000000000002	**IDENTIFICADOR ÚNICO DEL CERTIFICADO**
Algoritmo de firma:	**ALGORITMO DE FIRMA SHA512RSA**
Id. de objeto del algoritmo: 1.2.840.113549.1.1.13 sha512RSA	
Emisor:	**DATOS DE IDENTIFICACIÓN DEL EMISOR INCLUYENDO RUT DEL PSC Y INDIVIDUALIZACION**
E = contactos@abancert.cl	

CN = ABANCERT FIRMA ELECTRONICA AVANZADA - G2	**DE FIRMA ELECTRÓNICA AVANZADA**
OU = Autoridad Certificadora	
O = ABANCERT	
L = Santiago	
S = Region Metropolitana	
C = CL	
SERIALNUMBER = 77097633-2	
NotBefore: domingo, 13 de junio de 2021 16:51:20	**FECHAS DE CREACIÓN Y VIGENCIA DEL CERTIFICADO**
NotAfter: lunes, 13 de junio de 2022 16:16:19	
Sujeto:	**DATOS IDENTIFICADOR DE SUJETO INCLUYENDO EL RUT DEL TITULAR DE LA FEA**
E = nombrecorreo@correo.cl	
CN = Nombre Completo Titular	
OU = Unidad Organizacional	
O = Organización	
L = Localidad	
S = Región	
C = CL	
SERIALNUMBER= 12345678-9	
Algoritmo de clave pública:	**ALGORITMO DE CLAVE PÚBLICA RSA**
Id. de objeto del algoritmo: 1.2.840.113549.1.1.1 RSA	
Longitud de clave pública: 2048 bits	**LONGITUD DE CLAVE PÚBLICA 2048**
Identificador de clave del titular	
6422d2066817754fb5dc17c9da0d744fcd98b3d6	
2.5.29.15: Marcas = 1(Crítico), Longitud = 4	
Uso de la clave	

Firma digital, Sin repudio, Cifrado de clave, Cifrado de datos (f0)	
2.5.29.35: Marcas = 0, Longitud = 18	
Identificador de clave de entidad emisora	
Id. de clave=394e95d9b5a01d5223d2163e4a0c8687cdb81564	
2.5.29.31: Marcas = 0, Longitud = 32	
Puntos de distribución CRL	**PUNTO DE DISTRIBUCIÓN CRL Y OCSP**
[1]Punto de distribución CRL	
Nombre del punto de distribución:	
Nombre completo:	
Dirección URL=http://crl.abancert.cl/abancertcaFEA-g2.crl	
[1]Acceso a información de autoridad	
Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)	
Nombre alternativo:	
Dirección URL=http://ocsp.abancert.cl/ocsp	
Uso mejorado de claves	**USO MEJORADO DE CLAVES**
Autenticación del cliente (1.3.6.1.5.5.7.3.2)	
Correo seguro (1.3.6.1.5.5.7.3.4)	
Nombre alternativo del titular	**NOMBRE ALTERNATIVO DEL TITULAR SE INCLUYE EL RUT SEGUN CODIFICACION LEY 19799**
Otro nombre:	
1.3.6.1.4.1.8321.1=RUT DEL TITULAR DE FEA	
2.5.29.18: Marcas = 0, Longitud = 1c	
Nombre alternativo del emisor	**NOMBRE ALTERNATIVO DEL EMISOR SE INCLUYE EL RUT SEGUN CODIFICACION LEY 19799**
Otro nombre:	
1.3.6.1.4.1.8321.2=RUT DEL EMISOR PSC	

2.5.29.32: Marcas = 0, Longitud = 148	
Directivas del certificado	**DIRECTIVAS DEL CERTIFICADO Y DECLARACIÓN DEL EMISOR**
[1]Directiva de certificados:	
Identificador de directiva=1.3.6.1.4.1.56549.1	
[1,1]Información de certificador de directiva:	
Id. de certificador de directiva=CPS	
Certificador:	
https://www.abancert.cl	
[1,2]Información de certificador de directiva:	
Id. de certificador de directiva=Aviso de usuario	
Certificador:	
Texto de aviso=Certificado Firma Electrónica Avanzada. PSC acreditada según RAEX202200309, de 02 de marzo de 2022, de la Subsecretaría de Economía y Empresas de Menor Tamaño.	
Algoritmo de firma:	**ALGORITMO DE FIRMA SHA512RSA**
Id. de objeto del algoritmo: 1.2.840.113549.1.1.13 sha512RSA	
Huella Digital: d3303453e41b30c8527c5ce35e1d440cf61e0701	**HUELLA DIGITAL**
Nombre Completo Titular Rut Titular	**NOMBRE DESCRIPTIVO INCLUYE NOMBRE Y RUT DEL TITULAR DEL LA FEA**

4. REVOCACIÓN DE CERTIFICADOS

La revocación de certificados son mecanismos a utilizar en el supuesto de que por alguna causa establecida en la presente CPS se deje de confiar en el certificado antes de la finalización de su período de validez originalmente previsto.

4.1. Supuesto de Revocación

Los certificados deberán ser revocados cuando concurra alguna de las circunstancias siguientes:

- Solicitud voluntaria del Titular.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del Titular, incapacidad sobreviviente, total o parcial, extinción de la persona jurídica representada.
- Cese en su actividad del prestador de servicios de certificación salvo que los certificados expedidos por aquél, sean transferidos a otro prestador de servicios.
- Que el titular del certificado digital informe causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, uso de las claves privadas por persona distinta al titular o bien por cualesquiera otras circunstancias, incluidas las fortuitas.
- Por incumplimiento por parte de la AR, PSC o el Titular de las obligaciones establecidas en esta CPS.
- Por resolución judicial ejecutoriada, o por incumplimiento de las obligaciones del usuario establecidas en el artículo 24 de la ley 19799.
- Por la concurrencia de cualquier otra causa especificada en la presente CPS o establecida en la CP.

4.1.1. Efectos de la Revocación

El efecto de la revocación del certificado es la pérdida de fiabilidad del mismo, originando el cese permanente de la operatividad del Certificado conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.

La revocación de un certificado impide el uso legítimo del mismo por parte del Titular.

La revocación del certificado por causa no imputable al Titular originará la emisión de un nuevo certificado a favor del Titular por el plazo equivalente al restante para concluir el periodo originario de validez del certificado revocado.

La revocación del certificado tendrá como consecuencia la notificación a terceros mediante un correo electrónico, de que un certificado ha sido revocado, cuando se solicite la verificación del mismo.

4.2. Procedimiento de Revocación

4.2.1. Legitimación Activa

Deberán solicitar la revocación en cuanto tengan conocimiento de la concurrencia de alguna de las circunstancias contempladas en el apartado 4.1 anterior:

- El Titular del Certificado, así como la persona natural o jurídica representada por éste.
- La AR, respecto a aquellos certificados en cuya emisión haya participado.
- La persona jurídica que conste en el certificado.

En todo caso, el PSC podrá iniciar de oficio el procedimiento de revocación de certificados, en cualquiera de los casos previstos en el apartado 4.1 anterior.

4.2.2. Recepción de Solicitudes de Revocación

Se establece el siguiente procedimiento para la solicitud de revocación de un Certificado:

a. Notificación de la revocación, identificándose e indicando los motivos, por medio de uno de los siguientes mecanismos:
   Vía e-mail: contacto@abancert.cl
   Vía web en la dirección: https://www.abancert.cl

Sólo el Titular del certificado puede utilizar alguno de los medios anteriores.
En el caso de que la solicitud sea realizada por alguno de los medios detallados en el apartado anterior, ABANCERT procederá a Revocar el certificado.
El titular o usuario dispone de 48 horas desde su solicitud para presentarse ante ABANCERT para ratificar su solicitud de Suspensión/Revocación. El Titular deberá presentar su RUT para identificarse y se le hará entrega del formulario de ratificación de revocación de certificado, en donde se debe señalar el motivo de revocación debe ser firmado y estampada su huella dactilar.

b. Mediante la presencia física del usuario en la AR donde realizó la solicitud del Certificado, ratificando la revocación.
Cualquiera sea el mecanismo utilizado para solicitar la revocación, se deberá comprobar fehacientemente la identidad del solicitante, previo a dar curso a la revocación del certificado. Si la causa es por fallecimiento del Titular, se validará la información a través de algún bureau. Cualquier otra forma no contemplada será resuelta por la AR o PSC.
El inicio del proceso de revocación se realizará en forma inmediata al ser recibida la solicitud y con la presencialidad del titular.
Las conversaciones telefónicas que se mantengan podrán ser grabadas y registradas por ABANCERT a efectos probatorios. Pero deben ser ratificadas a través de un mail o presencia del Titular.

4.2.3. Decisión de Revocar

Una vez recibida y autenticada la solicitud de revocación, ABANCERT efectuará la revocación efectiva del Certificado. La decisión de revocar un Certificado corresponde a la AR.

4.2.4. Comunicación y Publicación de la Revocación

La decisión de revocar el certificado será comunicada por el PSC al Titular mediante e-mail.

Igualmente, se publicará la revocación del certificado en la CRL http://crl.abancert.cl/abancertcaFEA-g2.crl.

La revocación comenzará a producir efectos a partir de su publicación por parte del PSC, salvo que la causa de revocación sea el cese de la actividad del PSC, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

5. CADUCIDAD DE CERTIFICADOS

Los certificados caducarán por el transcurso del período operacional indicadas en las “fechas de creación (NotBefore)” y vigencia (NotAfter)” del mismo.
La caducidad producirá automáticamente la invalidez del certificado, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de certificación.
La caducidad de un certificado impide el uso legítimo del mismo por parte del Titular.

6. RENOVACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN

6.1. Renovación de Certificados

Este procedimiento se establece para los casos en que el certificado vaya a caducar y el Titular simplemente desee utilizar un certificado con las mismas características que tenía el que venía utilizando válidamente hasta entonces.

En este caso, el PSC emitirá un nuevo certificado y se generarán nuevas claves. Es requerido llevar a cabo nuevamente el proceso de verificación y validación de la identidad del Titular, según la CP que aplique.

Los certificados emitidos por ABANCERT tienen un plazo de vigencia de uno, dos o tres años. Se podrá acudir a los trámites que se establecen en este documento para la renovación de los servicios de certificación de ABANCERT si ocurren las situaciones que a continuación se detallan.

6.1.1. Requisitos Previos

Deberán concurrir los siguientes:

- Que el Titular posea o hubiese poseído en el anterior periodo, un certificado emitido por ABANCERT.
- Que el Titular desee la renovación del servicio de certificación y lo solicite en debido tiempo y forma, siguiendo el proceso 6.1.3 que se específica a tal efecto.
- Que el PSC no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación del certificado.
- Que el Titular se someta a los trámites correspondientes para la emisión de un certificado como cualquier otro Solicitante que solicita su certificado por primera vez.
- Que la solicitud de renovación de servicios de prestación se refiere al mismo tipo de certificado emitido inicialmente.

6.1.2. Cómo Solicitar la Renovación

El Titular que solicite la renovación de los servicios de certificación deberá solicitarlo enviando un e-mail a contacto@abancert.cl identificándose e indicando los motivos.

El Titular o usuario del certificado se someterá al régimen general de revisión de datos e identidad, bajo el mismo proceso utilizado para la emisión de nuevos certificados, permitiendo esta manera a ABANCERT comprobar fehacientemente la identidad del Solicitante o Titular. El certificado cuya vigencia ha expirado no es necesario revocarlo, debido a que por restricciones de fecha no puede dar continuidad a su uso.

6.1.3. Procedimiento de Renovación de Certificados

Cuando el PSC reciba la solicitud del Titular en debida forma, procederá con la revisión de los antecedentes e iniciara el proceso de validación, comprobando fehacientemente la identidad del solicitante.

Con la renovación de los servicios de certificación se entenderán que se mantienen los derechos, obligaciones y responsabilidades tanto de Titular como de PSC y AR, según se establece en los correspondientes contratos, la CPS y de las Políticas de Certificación aplicables.

6.2. Nueva emisión de Certificados

Este procedimiento se establece para los casos en que el certificado de un Titular sea declarado revocado por la existencia de inexactitudes en el Certificado y se emite un nuevo certificado.

6.2.1. Requisitos Previos

Se podrá acudir a los trámites que se establecen en este documento para la nueva emisión de certificados de ABANCERT si concurren a la vez los requisitos generales que a continuación se detallan:

- La solicitud la debe llevar a cabo el Titular del antiguo certificado.
- El origen de la solicitud debe basarse en la renovación del certificado por inexactitudes en el mismo.
- La solicitud debe realizarse en debida forma, siguiendo las instrucciones y normas que ABANCERT específica a tal efecto.
- La solicitud de una nueva emisión del certificado debe referirse al mismo tipo de certificado emitido inicialmente.

6.2.2. Cómo Solicitar la Nueva emisión

El antiguo Titular que solicite la nueva emisión de los servicios de certificación deberá llenar un formulario que se encuentra en: https://www.abancert.cl

El Titular deberá manifestar en dicho formulario, bajo su responsabilidad, cuáles de los datos que constaban en su certificado ya revocado no son ciertos o han variado de alguna forma.

La AR revisará la validez formal de la solicitud de nueva emisión y enviará a la AC una solicitud para la creación de un nuevo certificado a nombre del Titular. A continuación, la propia AR PSC, realizará la validación de la identidad y de los datos del certificado que hayan variado, solicitando la presencia física del solicitante y requiriendo la exhibición de cuantos documentos originales considere necesarios.

Para la validación definitiva de los nuevos datos del certificado, y para la entrega de éste, se aplicará el mismo procedimiento que para la primera emisión.

6.2.3. Procedimiento de Nueva emisión de Certificados

Una vez presentada la documentación necesaria, la AR examinará si procede o no la nueva emisión del certificado, distinguiendo tres supuestos:

a) **Defectos subsanables en la presentación.** En este caso, la AR deberá comunicar al Solicitante tal error o defecto.

b) **Defectos no subsanables en la presentación.** En este caso, la AR deberá comunicar al Titular que solicita la nueva emisión, estas circunstancias, denegándole la posibilidad de nueva emisión del certificado.

c) **La documentación presentada es la necesaria y concurren los requisitos exigibles.** En este caso, la AR entregará al Titular el nuevo certificado, entendiéndose que se mantienen los derechos, obligaciones y responsabilidades tanto del Titular como de PSC y AR, según se establece en los correspondientes contratos, la CPS y de las Políticas de Certificación aplicables.

7. EXTINCIÓN DEL PSC

En orden a causar el menor daño posible tanto en los Titulares como a los Usuarios del sistema de certificación ante una hipotética desaparición del PSC se establecen las siguientes medidas:

- Comunicar la extinción mediante el envío de un correo electrónico o una notificación mediante correo ordinario certificado dirigido a todos los titulares o usuario cuyos certificados permanezcan en vigor y la publicación de un anuncio en dos diarios de tirada nacional. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.
- Establecer, cuando ello fuera posible, un acuerdo con otro prestador de servicios con la intención de transmitir todas sus obligaciones y derechos dentro del sistema de certificación con la intención de continuar el servicio. Si se produce la subrogación, a la cual el titular o usuario da su consentimiento de manera expresa, esta CPS seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito.
- Proceder, en caso de no haberse podido llevar a cabo transferencia de derechos y obligaciones a otro PSC, a la revocación de todos los certificados una vez transcurrido el plazo de dos meses desde la comunicación.
- Indemnizar adecuadamente a aquellos titulares o usuarios que lo soliciten cuando sus certificados sean revocados con anterioridad al plazo previsto de vigencia, pactándose como tope para la indemnización el coste efectivo del servicio, descontando a prorrata el coste por los días transcurridos desde el inicio del contrato hasta la fecha de resolución, o la emisión de un nuevo certificado en la otra PSC que tomo la responsabilidad, con un periodo de vigencia hasta la fecha de vigencia del certificado original.
- Cualquier otra obligación que venga impuesta por la ley 19799.

8. CONTROLES DE SEGURIDAD

Con el objeto de reforzar la seguridad técnica, física, de procedimientos y de capacitación del personal, el PSC dispone de un reglamento interno de funcionamiento que regula todos estos aspectos, el cual es entregado a los empleados de Abancert al momento de firmar su contrato.

Los requerimientos básicos de seguridad que ha de observar el PSC son los siguientes:

- El software y la información del PSC correrá en una estación de trabajo dedicada a tal fin, con las providencias y medidas necesarias para protegerlo contra ataques de la red interna y por sobre todo de la red externa.
- La clave de firma del PSC tendrá una longitud de 2048 bits.
- Al menos una copia de los Backups del equipo del PSC deberá ser respaldados en medios externos al PSC.

9. AUDITORÍAS

Con el fin de velar por el correcto uso de los recursos de su propiedad, ABANCERT se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos.
En referencia a las revisiones de la seguridad de la información, se considera revisiones independientes, evaluaciones del cumplimiento de las políticas y normas de seguridad y evidencia que compruebe del cumplimiento.

10. RIESGOS

ABANCERT realiza la gestión de riesgos a través de su Política de Gestión de riesgos que se detalla en el requisito PS01.

11. CARACTERÍSTICAS DE LOS CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS

11.1. Características del Certificado

Los certificados podrán ser emitidos en diversos tipos de soportes, siempre que estos se ajusten a las Políticas de Certificación: e- token, disco local, etc. Los e-tokens serán emitidos únicamente en las instalaciones donde se ubica el PSC y la AR.

Los certificados tendrán una validez de uno, dos o tres años a partir de su fecha de validez inicial.

11.2. Listas de Certificados Emitidos por ABANCERT

Los certificados una vez emitidos, su parte publica estará disponible para consultar su estado en la siguiente url: https://www.abancert.cl/CertificadoEstado.aspx

Los certificados revocados por el PSC serán publicados en un repositorio disponible públicamente. Esta operación será realizada por personal autorizado a partir de los ficheros generados por el PSC.

El listado de certificados revocados (CRL) estará a disposición de los usuarios en la página web del PSC:

http://crl.abancert.cl/abancertcaFEA-g2.crl

Los Usuarios de certificados pueden consultar en cualquier momento el estado de un Certificado determinado, por lo siguientes mecanismos:

Realizando consultas en línea mediante el servicio OCSP publicado en: http://ocsp.abancert.cl/ocsp

Realizando la solicitud correspondiente a través del correo contacto@abancert.cl.

12. ADMINISTRACIÓN DE ESPECIFICACIONES

12.1. Procedimiento de Modificación de la CPS y de las CP

El PSC podrá modificar las estipulaciones de la presente CPS y de su CP específicas, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación y siempre que toda modificación se justifique desde el punto de vista jurídico, técnico y comercial.

Tanto las modificaciones a las CPS y CP, serán publicadas en régimen de vigencia, una vez sean aprobadas por la Entidad Acreditadora del Ministerio de Economía.

12.2. Procedimiento de Publicación de las modificaciones

El PSC podrá modificar las estipulaciones de la presente CPS y de su CP específicas, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación y no se afecten los derechos del consumidor según la ley 19496 y, siempre y cuando, toda modificación se justifique desde el punto de vista jurídico, técnico y comercial.

Las modificaciones efectuadas sobre la CPS o las CP se darán a conocer a los interesados, en la página web del PSC https://www.abancert.cl y en las oficinas del PSC y de la AR.

A estos efectos, en dicha página web, se hará una referencia expresa y fácilmente localizable a la existencia de dicha modificación, durante un período de treinta días.

De igual modo, se procederá a sustituir la versión anterior de la CPS o de las CP por la nueva.

En la página Web del PSC se incluirá un listado de control de las sucesivas versiones que sobre la CPS o las CP puedan originarse, desde que se podrá tener acceso tanto a la versión actual y operativa como a las versiones anteriores con una antigüedad no superior a un año.

12.3. Comité de Seguridad de la Información

ABANCERT ha establecido una Estructura Organizacional de Seguridad que contempla la definición de funciones específicas en el ámbito de la seguridad, que da pie al Comité de Seguridad de la Información.

12.4. Procedimientos de difusión de Interna

ABANCERT comunica la información relevante definida por el Sistema de Gestión de Seguridad de la Información, a las personas de la organización, a través de mecanismos que aseguran la capacitación permanente de las distintas políticas y procedimientos que le atañan.

12.5. Mantención de la Infraestructura

ABANCERT cuenta con servicios de infraestructura contratados a un proveedor que cumple con los requisitos mínimos exigidos por la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación” publicados por la Entidad Acreditadora del ministerio de Economía en su versión vigente.

12.6. Procedimiento de Notificación de las Publicaciones

En caso de que las modificaciones efectuadas en la CPS o en las Políticas de Certificación incidan directamente en los derechos y obligaciones de los Titulares y/o Solicitantes, así como cuando dichas modificaciones alteren la operatividad de los certificados por parte de los usuarios, deberán notificarse dichas modificaciones a los Titulares y/o Solicitantes con un período de antelación de quince días a la aplicación de los cambios efectuados.
El transcurso de dicho período sin que medie comunicación escrita por parte del Titular y/o Solicitante, en contra de las citadas modificaciones implicará su aceptación. La no aceptación de las modificaciones de esta CPS o de las Políticas de Certificación realizadas por el PSC, tendrá como consecuencia el término de la relación comercial con el Titular/Solicitante.
Se considerará como medio eficaz para la realización de notificaciones el correo electrónico y enviado a la dirección proporcionada por el Titular y/o Solicitante.

12.7. Plan de Seguridad

El Plan de Seguridad permite trabajar en el transcurso del año en aquellos ámbitos de acción establecidos, con el objetivo de proveer protección a los recursos de información, según lo definido en la política de seguridad de Información de la Organización.

12.8. Plan de administración de llaves

En el documento ubicado en la carpeta PS06-PLAN DE ADMINISTRACIÓN DE LLAVES se encuentra el detalle del Plan de administración de llaves en el cual se definen las acciones sobre las llaves criptográficas de ABANCERT, de manera de resguardarlas y administrarlas durante su ciclo de vida.

12.9. Responsabilidad sobre los activos.

ABANCERT mantiene un inventario de activos el cual es revisado periódicamente y que se encuentra en el archivo “Inventario de Activos y Riesgos”.

La Gerencia de ABANCERT es el propietario de sus activos y debe entregar los recursos necesarios para gestionarlos y así proveer productos y soluciones de Firma Electrónica (Certificados Digitales) de forma segura y eficiente.

12.10. Control de Acceso.

En ABANCERT el control de acceso a la información es de alta importancia, por lo que se regula en base a lo establecido en la “Política de control de acceso” ubicada en la Carpeta “00_DREF-DOCUMENTOS REFERENCIADOS”.

13. REFERENCIAS

La presente CPS está basada principalmente en la propuesta de estándar para la redacción de políticas y prácticas de certificación, del grupo de trabajo del IETF PKIX y ETSI TS 102 042.

14. Revisión

Versión	Fecha	Revisión	Observaciones
1.0	07 dic.2021	1.0	Primer documento.

Elaborado por: ABANCERT – Equipo de trabajo	Fecha: diciembre de 2021

**** FIN ****