

**POLÍTICA DE CERTIFICACIÓN
FIRMA ELECTRÓNICA AVANZADA**

ABANCERT

Versión: 1.2

Fecha Vigencia: Noviembre 2023

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

Contenido

1. IDENTIFICACIÓN DE LA POLÍTICA DE CERTIFICACIÓN	4
1.1. PRESENTACIÓN	4
1.2. IDENTIFICACIÓN	4
1.3. ACRÓNIMOS	4
2. TITULAR DEL CERTIFICADO	4
3. PROCEDIMIENTO.....	5
3.1. SOLICITUD DE CERTIFICADO	5
3.2. COMPROBACIÓN DE LAS SOLICITUDES DE CERTIFICADOS	5
3.3. APROBACIÓN DE LA SOLICITUD	5
3.4. RECHAZO DE LA SOLICITUD	5
3.5. EMISION Y ENTREGA DEL CERTIFICADO	6
3.5.1. Entrega:	6
3.6. ACEPTACIÓN DEL CERTIFICADO POR PARTE DEL TITULAR	8
3.7. PUBLICACIÓN DEL CERTIFICADO	9
3.7.1. Formulario Solicitud de FIRMA ELECTRÓNICA AVANZADA (AR)	12
3.7.2. Datos de Facturación	12
3.7.3. Perfil de CRL.....	13
3.7.4. Identificación de CRL.....	14
4. USO DE LOS CERTIFICADOS.....	17
4.1. COMUNIDAD DE USUARIOS	17
4.2. APLICABILIDAD	17
4.2.1. Firma y No Repudio	17
4.2.2. Integridad	17
4.3. DETALLES DE CONTACTO	18
4.4. USOS NO AUTORIZADOS.....	18
5. PRIVACIDAD Y PROTECCIÓN DE LOS DATOS	18
5.1. TIPOS DE INFORMACIÓN A PROTEGER.....	18
5.2. TIPOS DE INFORMACIÓN QUE PUEDE ENTREGARSE	19
5.3. INFORMACIÓN DEL CERTIFICADO	19
5.4. ENTREGA DE INFORMACIÓN SOBRE LA REVOCACIÓN DEL CERTIFICADO	19
5.5. ENTREGA DE INFORMACIÓN EN VIRTUD DE UN PROCEDIMIENTO JUDICIAL	19
5.6. ENTREGA DE INFORMACIÓN A PETICIÓN DEL TITULAR	19

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

- 6. REVOCACIÓN DE CERTIFICADOS20**
 - 6.1. Circunstancias de Revocación del Certificado20**
 - 6.1.1. Efectos de la Revocación.....20
 - 6.2. Procedimiento de Revocación21**
 - 6.2.1. Recepción de Solicitudes de Revocación21
 - 6.2.2. Decisión de Revocar.....21
 - 6.2.3. Comunicación y Publicación de la Revocación21
 - 6.3. SUSPENSIÓN DE CERTIFICADOS22**
- 7. ADMINISTRACIÓN DE LA ESPECIFICACIÓN DE LA CP22**
 - 7.1. Proveedores22
 - 7.2. Auditorias23
 - 7.3. Comité de Seguridad de la Información23
 - 7.4. Controles23
 - 7.5. Riesgos23
 - 7.6. Cultura de Seguridad23
 - 7.7. Mantenimiento de la Infraestructura23
 - 7.8. Plan de Seguridad24
 - 7.9. Plan de administración de llaves.....24
 - 7.10. Responsabilidad sobre los activos.....24
 - 7.11. Control de Acceso.24
- 8. JERARQUÍA DE NORMAS24**
- 9. REVISIÓN.....25**

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

1. IDENTIFICACIÓN DE LA POLÍTICA DE CERTIFICACIÓN

1.1. PRESENTACIÓN

El presente documento constituye la Política de Certificación de ABANCERT correspondiente a los Certificados de FIRMAELECTRÓNICA AVANZADA, a la cual se hará referencia mediante el acrónimo de su denominación en inglés CP.

Este documento enmarca los preceptos aplicados al procedimiento de la emisión de los Certificados de FIRMA ELECTRÓNICA AVANZADA por ABANCERT.

1.2. IDENTIFICACIÓN

Esta CP puede localizarse en la siguiente dirección de Internet:
<http://www.abancert.cl/assets/doc/DeclaracionPracticasCertificacion.pdf>

1.3. ACRÓNIMOS

Sigla	Descripción
AC	Autoridad Certificadora
AR	Autoridad de Registro
CP	Política de Certificación (Sigla en inglés)
CPS	Prácticas de Certificación

2. TITULAR DEL CERTIFICADO

Sera sujeto a ser Titular del Certificado de Firma Electrónica Avanzada, quienes certifiquen ser persona natural, que tengan Cédula de Identidad vigente, emitida por el Servicio de Registro Civil e Identificación de Chile, permitiendo a esta PCS comprobar fehacientemente la identidad del Titular.

El certificado es personal e intransferible, por tanto, todo acto ejecutado con el propio certificado será considerado como un acto propio del titular.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

3. PROCEDIMIENTO

3.1. SOLICITUD DE CERTIFICADO

El solicitante deberá llenar y enviar el formulario de solicitud del Certificado que estará a su disposición en la dirección de Internet: <https://www.abancert.cl> . El envío de los datos solicitados en este formulario supondrá su consentimiento para ser registrado como solicitante de un Certificado ABANCERT de FIRMA ELECTRÓNICA AVANZADA. La solicitud de este certificado no implicará en ningún caso su obtención si no se llegan a cumplir por parte del solicitante las cláusulas y condiciones establecidos en la CPS y en la Política de Certificación para los Certificados de FIRMA ELECTRÓNICA AVANZADA.

Asimismo, con el envío del formulario, el solicitante se compromete ante la AR, proporcionar 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 CP.

3.2. COMPROBACIÓN DE LAS SOLICITUDES DE CERTIFICADOS

Una vez el titular comparezca presencialmente en la AR, con los datos entregados se procederá a verificar la información recibida para su aprobación.

3.3. APROBACIÓN DE LA SOLICITUD

Una vez comprobada fehacientemente la identidad del Titular y validado el proceso de comprobación de solicitud de forma satisfactoria, la AR procederá a la aprobación de la solicitud, quedando dicha solicitud en estado de poder emitir y entregar el Certificado.

3.4. RECHAZO DE LA SOLICITUD

Si la AR decidiera rechazar la solicitud del Certificado, dicha decisión será comunicada de forma inmediata al Titular y a su vez, formalizada a través de correo electrónico.

En caso de encontrar defectos, el usuario deberá entregar los datos correctos para generar una nueva solicitud vía WEB.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

3.5. EMISION Y ENTREGA DEL CERTIFICADO

Una vez aceptada por la AR la Solicitud del Certificado, se llevará a cabo el proceso de enrolamiento del Titular, los requisitos para la emisión y entrega del Certificado son:

- Presencialidad del Titular en dependencias de ABANCERT.
- Acreditar el pago o importe del certificado.
- Para el caso de los Notarios, Conservadores y Archiveros Judiciales titulares, suplentes e interinos, debe presentar certificación que acredite su cargo de la condición de tales, emitido por el secretario de la Corte de Apelaciones respectiva.

3.5.1. Entrega:

- a) El operador AR, solicitará al titular presentar su Cédula de Identidad Chilena original y en buen estado, con la cual validará visualmente que la persona que comparece corresponde a la que se identifica.
- b) Con el número y serie de la Cédula de Identidad, se consultará vía web al Servicio de Registro Civil e Identificación y/o una plataforma de servicio externo de un Bureau la verificación de los datos entregados, obteniendo la verificación de estado de fallecido o de defunción del Titular, además del estado de vigencia y bloqueo de la Cédula de Identidad.
- c) El operador AR, tomará fotografía digital al titular.
- d) El Operador AR entregará al titular el “Contrato de Suscripción de FEA” en dos (2) copias, debiendo estampar su huella dactilar y su firma en ambos ejemplares (este acto es manual y no se utilizan dispositivos tecnológicos), quedando una copia en poder del cliente y otra en dependencias de ABANCERT. Este contrato será almacenado físicamente en dependencias de ABANCERT y su respaldo digital será guardado en un directorio de acceso restringido y respaldado semanalmente.
- e) 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.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

- f) Por último, se debe registrar en el sistema de inventario interno, la salida del dispositivo portable seguro, registrando el número de serie de cada elemento y la información del registro del Titular que dio origen al certificado que fue entregado Ej: Fecha, Rut, Nombre.

El Titular se obliga a:

- a) Descargar y almacenar el certificado en los dispositivos autorizados por la EC y que han sido validados por esta, de acuerdo con lo establecido en la Ley 19799 "Sobre Documentos Electrónicos, Firma Electrónica Y Servicios De Certificación De Dicha Firma". La descarga y almacenamiento del certificado será realizada por el titular (asesorado por el operador AR), en un dispositivo portable seguro (token, Fips 140-2 Nivel 3), en las dependencias de ABANCERT.
- b) El dispositivo portable seguro cuenta con un mecanismo que lo inhabilita en caso de reiterados intentos fallidos de acceso (hasta 15 intentos).
- c) El Titular declarará en el "Contrato de Suscripción de FDA" que el uso de la clave privada correspondiente a su certificado y el conocimiento del PIN de acceso al dispositivo portable seguro (token, Fips 140-2 Nivel 3), serán de su total responsabilidad.
- d) No revelar la clave privada de seguridad del dispositivo en donde se encuentra almacenado el Certificado.
- e) Custodiar el Certificado, de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, 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 en cualquier otro documento que el titular conserve o transporte, especialmente si existe la posibilidad de extravío, hurto o sustracción indebida.
- f) Notificar de inmediato la pérdida, robo o falsificación del Certificado que contiene, así como el conocimiento por otras personas, contra su voluntad, del código de activación o de las claves privadas, solicitando la revocación del Certificado en conformidad con el procedimiento que se establece en la CPS.
- g) Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en el epígrafe titulado "REVOCACIÓN DE CERTIFICADOS" de la CPS.
- h) Destruir o borrar el Certificado que quede en desuso o que haya sido sustituido por otro a utilizar con los mismos fines.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

- i) La EC se reserva el derecho a negarse a emitir Certificados cuando concurra cualquier causa justificada, por lo que no podrá exigirse responsabilidad alguna por este motivo.

Responsabilidad de la PSC

- a) La PSC no será responsable de los daños derivados de errores u omisiones de las obligaciones por parte del titular.
- b) La PSC no será responsable de la utilización incorrecta de los certificados, ni de cualquier daño indirecto que pueda resultar de su uso.
- c) Previa acción al pago o emisión de certificado, El PSC no será responsable por el retraso o la no ejecución de cualquiera de las obligaciones de esta CP 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.
- d) Será responsabilidad del Titular como usuario, de disponer de todos los elementos técnicos necesarios para el normal funcionamiento y uso de del Certificado.
- e) La EC no será responsable del contenido de los documentos suscritos electrónicamente mediante cualquier certificado.
- f) La PSC se compromete a mantener vigente y disponer un seguro de responsabilidad civil que cubra el valor mínimo exigido por la normativa vigente de ley de Firma Electrónica Avanzada.

3.6. ACEPTACIÓN DEL CERTIFICADO POR PARTE DEL TITULAR

La entrega del Certificado, tomar su fotografía, la firma e impresión de huella dactilar (este acto es manual y no se utilizan dispositivos tecnológicos) durante el enrolamiento, implica la aceptación del Certificado por parte del titular.

La aceptación del Certificado deberá realizarse de forma expresa, ante un representante 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.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

3.7. PUBLICACIÓN DEL CERTIFICADO

Una vez aceptado el Certificado por parte del titular, la EC procederá a la publicación, 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 Contenido del Certificado versión x509 v3.

Perfil de Certificado de la Política de FIRMA ELECTRÓNICA AVANZADA

Certificado X509:	VERSIÓN DE CERTIFICADO
Versión: V3	
Número de serie: 3a00000004bc6b92bc46c3369d000000000004	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 INDIVIDUALIZACIÓN DE FIRMA ELECTRÓNICA AVANZADA
E = contactos@abancert.cl	
CN = ABANCERT FIRMA ELECTRONICA AVANZADA - E7	
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	
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	

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	
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		
[1]Punto de distribución CRL		
Nombre del punto de distribución:		
Nombre completo:		
Dirección URL=http://crl.abancert.cl/abancertcaFEA-e7.crl	PUNTO DE DISTRIBUCIÓN CRL Y OCSP	
[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		
Autenticación del cliente (1.3.6.1.5.5.7.3.2)	USO MEJORADO DE CLAVES	
Correo seguro (1.3.6.1.5.5.7.3.4)		
Nombre alternativo del titular		
Otro nombre:	NOMBRE ALTERNATIVO DEL TITULAR SE INCLUYE EL RUT SEGUN CODIFICACION LEY 19799	
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		
Otro nombre:	NOMBRE ALTERNATIVO DEL EMISOR SE INCLUYE EL RUT SEGUN CODIFICACION LEY 19799	
1.3.6.1.4.1.8321.2=RUT DEL EMISOR PSC		
2.5.29.32: Marcas = 0, Longitud = 148		
Directivas del certificado		
[1]Directiva de certificados:	DIRECTIVAS DEL CERTIFICADO Y DECLARACIÓN DEL EMISOR	
Identificador de directiva=1.3.6.1.4.1.56549.1		
[1,1]Información de certificador de directiva:		

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	
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 acreditado según R.A Exenta N°XXX de DD-MM-YY de la Subsecretaría de Economía		
Algoritmo de firma:		
Id. de objeto del algoritmo: 1.2.840.113549.1.1.13 sha512RSA	ALGORITMO DE FIRMA SHA512RSA	
Huella Digital: 972c8df4b3195cb219107051c74a9975a4583440	HUELLA DIGITAL	
Nombre Completo Titular Rut Titular	NOMBRE DESCRIPTIVO INCLUYE NOMBRE Y RUT DEL TITULAR DEL LA FEA	

Solo para el caso de los Notarios, Conservadores y Archiveros Judiciales, el campo OU = Unidad Organizacional, será conformado con más información en el atributo:

OU= Cargo"+ "+Nombramiento+" "+Dto:"+Número Resolución

Para el resto, el atributo quedara conformado con el dato de la Unidad Organizacional que proporcione e identifique el Titular.

Todas estas especificaciones y condiciones de uso del certificado estarán publicadas en:

<http://www.abancert.cl/assets/doc/DeclaracionPracticasCertificacion.pdf>

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

3.7.1. Formulario Solicitud de FIRMA ELECTRÓNICA AVANZADA (AR)

- Nombre del Titular
- Apellido Paterno del Titular
- Apellido materno del titular
- Cédula de identidad
- Serie de Cédula de Identidad
- Dirección
- Región
- Ciudad
- Comuna
- Correo Electrónico
- Repetir correo Electrónico
- Teléfono

3.7.2. Datos de Facturación

- Nombre de la empresa
- RUT de la empresa
- Dirección de la empresa
- Giro Empresa
- Correo Electrónico
- Ciudad
- Comuna

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

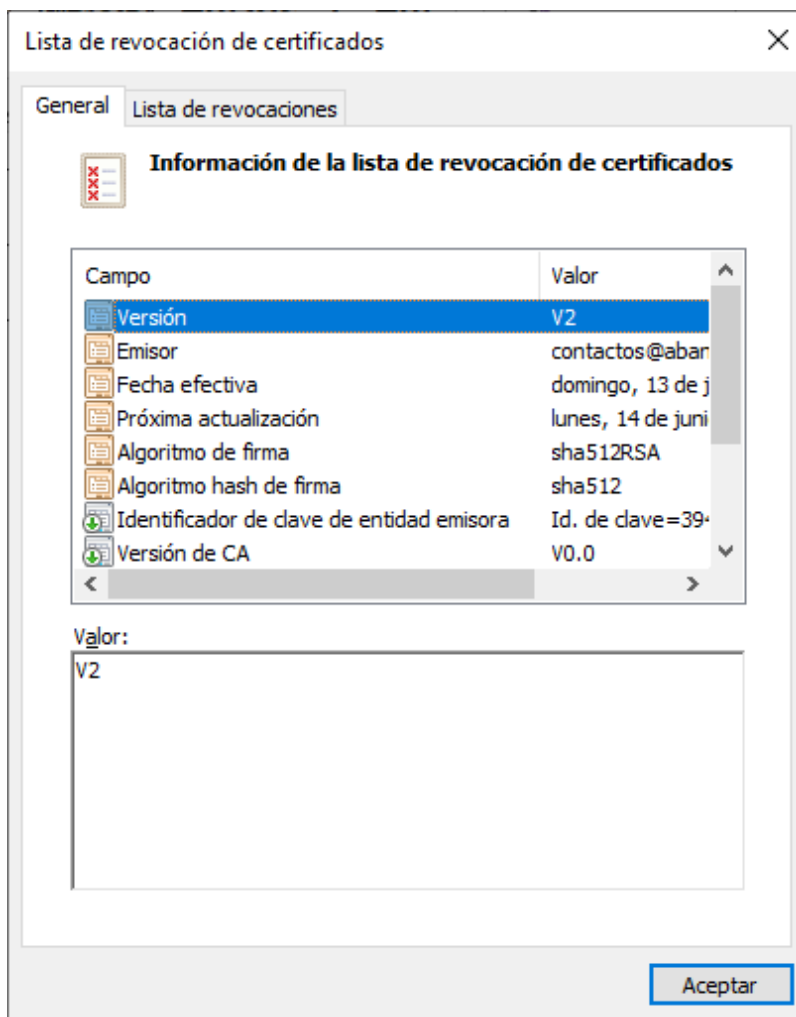
3.7.3. Perfil de CRL

Versión	V2
Emisor	E = contactos@abancert.cl CN = ABANCERT FIRMA ELECTRONICA AVANZADA - E7 OU = Autoridad Certificadora O = ABANCERT L = Santiago S = Region Metropolitana C = CL SERIALNUMBER = 77097633-2
Fecha efectiva	Se indica la fecha vigente según el formato: día, mes y año. Ejemplo: domingo, 13 de junio de 2021 16:23:34
Próxima actualización	Se indica la fecha vigencia según el formato: día, mes y año Ejemplo: lunes, 14 de junio de 2021 19:07:34
Algoritmo de firma	sha512RSA
Algoritmo has de firma	sha512
Versión de CA	V0.0
Número CRL	número secuencial
Huella digital	233ab3b020c18d0c5ff57f7030aba1f55f2270d5

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

3.7.4. Identificación de CRL

La lista de revocación se encuentra disponible en la dirección URL <http://crl.abancert.cl/abancertcaFEA-g2.crl> que es de Acceso Público.



ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

En este punto, se encuentra lista de certificados revocados o suspendidos.

Lista de revocación de certificados

General Lista de revocaciones

Certificados revocados:

Número de serie	Fecha de revocación
3a00000004bc6b92bc46c3369d0000...	domingo, 13 de junio de...

Entrada de revocación

Campo	Valor
-------	-------

Valor:

Aceptar

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

Servicio Validación OCSP:

Vista representada en otro plano de la estructura y componentes de la lista de revocación:

Versión	V2	
Emisor	Email	E=contactos@abancert.cl
	Nombre Firmante de la CRL	CN=ABANCERT FIRMA ELECTRÓNICA AVANZADA - E7
	Unidad Organizacional	OU= Autoridad Certificadora
	Organización	O=ABANCERT
	Localidad (Ciudad)	L=Santiago
	Estado (Región)	S=Región Metropolitana
	País	C=CL
	SERIALNUMBER	SERIALNUMBER = 77097633-2
Fecha Efectiva	domingo, 13 de junio de 2021 18:27:15	
Próxima Actualización	lunes, 14 de junio de 2021 21:11:15	
Algoritmo de firma	Sha512RSA	
Algoritmo hash de la firma	Sha512	
Identificación de clave de entidad emisora	Id. de clave= 394e95d9b5a01d5223d2163e4a0c8687cdb81564	
Versión de CA	V0.0	
Número de la CRL	03	
Authority Key	Id. de clave=	

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	
	Certificados revocados	
Lista de Revocación		Número de Serie
		Fecha de Revocación
		Código de Razón de la lista de revocación de certificados

4. USO DE LOS CERTIFICADOS

4.1. COMUNIDAD DE USUARIOS

Los Certificados Digitales permiten que los usuarios puedan identificarse digitalmente en Internet. Identifica al usuario de forma única y podrá utilizarse en todas aquellas aplicaciones que precisen autenticación mediante certificados digitales X.509 v3. Adicionalmente, los certificados de personas permitirán firmar, cifrar y soportar no repudio de transacciones. El Titular de un tipo de Certificados podrá ser cualquier persona natural siempre que esté conforme a los criterios establecidos en las Prácticas de Certificación Específica (CPS) de cada tipo de certificado. Este certificado permitirá sólo firmar de acuerdo con lo establecido en la ley 19.799 y su reglamento.

4.2. APLICABILIDAD

4.2.1. 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 documento o mensaje. Esto permite probar la identidad del emisor del mensaje o documento y que este mensaje o documento no ha sido alterado, lo que en el futuro da lugar al NO repudio del acto, es decir, se entiende como la capacidad de probar que una acción o evento que ha tenido lugar, de modo tal, que este evento o acción no pueda ser repudiado más tarde.

El mensaje o documento firmado puede corresponder a una transacción y documento electrónico con validez legal según las normativas vigentes que dicen relación con la firma digital, de acuerdo a la ley 19.799.

4.2.2. Integridad

El uso de este sistema de claves asimétricas permite comprobar al receptor de un mensaje que el mismo no ha sido alterado entre el envío y la recepción.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

4.3. DETALLES DE CONTACTO

Atención.: Atención Clientes ABANCERT
 Román Díaz 117,
 Providencia. Santiago de Chile
 E-mail: contacto@abancert.cl Teléfono: (+56 2) 64658405
 Mesa ayuda certificación: (+56 2) 64658405
 Lunes a Viernes: 09:30 – 13:00 hrs. 15:00 – 17:00 hrs.

4.4. USOS NO AUTORIZADOS

Se deja constancia de que la finalidad de los certificados es identificar a una persona en un sistema de redes abiertas o cerradas y no son medios de pago. No obstante, los certificados regidos por esta POLÍTICA DE CERTIFICACIÓN pueden ser utilizados en operaciones que representen órdenes de pago o transferencias de dinero.

Estos certificados son válidos para asumir las responsabilidades económicas y compromisos en nombre propio permitidos por ley 19.799 "sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma" 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 y en la Política de Certificación.

Los certificados ABANCERT no pueden ser alterados, se deben utilizar tal y como son suministrados por la PSC, en caso de haber alguna alteración, estos quedan invalidados inmediatamente.

5. PRIVACIDAD Y PROTECCIÓN DE LOS DATOS

5.1. TIPOS DE INFORMACIÓN A PROTEGER

La información personal 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 Art. 12 b) de la ley N.º19.799 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

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

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 que establece Normas Sobre Protección a los Derechos de los Consumidores.

ABANCERT no utilizará la información para otros fines que los exclusivos y relacionados con sus actividades de certificación, ni compartirá esta información con terceros salvo lo señalado en los números siguientes.

5.2. TIPOS DE INFORMACIÓN QUE PUEDE ENTREGARSE

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.

5.3. INFORMACIÓN DEL CERTIFICADO

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)

5.4. ENTREGA DE INFORMACIÓN SOBRE LA REVOCACIÓN DEL CERTIFICADO

La información sobre el estado de vigencia o revocación de un certificado emitido por ABANCERT se encuentra publicada en: <https://www.abancert.cl/CertificadoEstado.aspx>

5.5. ENTREGA DE INFORMACIÓN EN VIRTUD DE UN PROCEDIMIENTO JUDICIAL

ABANCERT sólo entregará la información requerida en virtud de un procedimiento judicial o solicitud formal por orden de un tribunal del Poder del Estado Judicial Chileno.

5.6. ENTREGA DE INFORMACIÓN A PETICIÓN DEL TITULAR

ABANCERT administra información proporcionada por el propio solicitante y/o titular.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

6. REVOCACIÓN DE CERTIFICADOS

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

6.1. Circunstancias de Revocación del Certificado

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

- Solicitud del titular del certificado.
- Pérdida o inutilización por daños del soporte del certificado.
- Fallecimiento del titular o disolución de la persona jurídica que represente, en su caso.
- 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 al momento de solicitarlo no proporcionó los datos de la identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa.
- Que el titular del certificado no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificador.
- Por incumplimiento por parte de la AR, PSC o el Titular de las obligaciones establecidas en esta CP.
- Por incumplimiento por parte de la AR, EC o el titular de las obligaciones establecidas en esta CP.
- Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto de que se ponga en duda la fiabilidad del Certificado.
- Por resolución judicial ejecutoriada.
- Por la concurrencia de cualquier otra causa especificada en la presente CP o establecida en la CPS.

6.1.1. Efectos de la Revocación

El efecto de la revocación del certificado es el cese permanente de los efectos jurídicos de este conforme a los usos que le son propios e impide el uso legítimo del mismo.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

6.2. Procedimiento de Revocación

6.2.1. Recepción de Solicitudes de Revocación

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

- a. La solicitud de revocación será recibida vía correo electrónico a las siguientes direcciones:
 - contacto@abancert.cl,
 - soporte@abancert.cl,

ABANCERT podría disponer otros canales para la solicitar la revocación, el cual será debidamente descrito en su página web <https://www.abancert.cl>

Sólo el Titular del certificado puede utilizar alguno de los medios anteriores.

ABANCERT procederá a informar al titular que dispone de 48 horas para presentarse presencialmente ante ABANCERT y ratificar su solicitud de Suspensión/Revocación. El Titular deberá presentar su RUT para identificarse y la ratificación de revocación de certificado se formalizará a través un documento firmado, en donde deberá señalar el motivo de revocación.

- b. Mediante la presencia física del usuario en la AR, se validará la identidad de forma fehaciente 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 proceso de revocación se iniciará al ser recibida la solicitud y finalizará con la presencialidad del titular.

6.2.2. 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.

6.2.3. 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

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

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.

6.3. SUSPENSIÓN DE CERTIFICADOS

ABANCERT define que el proceso de Suspensión de Certificados será igual al proceso de Revocación descrito en este documento en ítem 6 del punto 6.2 y la habilitación de la suspensión corresponderá a la emisión de un nuevo certificado, descrito en el ítem 3 del punto 3.5 de este documento.

Se procederá la suspensión de la vigencia del certificado cuando se verifique alguna de las siguientes circunstancias:

- Solicitud del titular del certificado.
- Decisión del prestador de servicios de certificación en virtud de razones técnicas.

7. ADMINISTRACIÓN DE LA ESPECIFICACIÓN DE LA CP

La PSC podrá modificar las estipulaciones de la presente CP, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación, y serán publicadas en régimen de vigencia, siempre y cuando sean aprobadas por la Entidad Acreditadora del Ministerio de Economía.

7.1. Proveedores

Las empresas y consultores que presten servicios deberán cumplir con las políticas, estándares y procedimientos detallados en el contrato de servicio específico, ítems que pueden ser evaluados en cualquier momento por ABANCERT y que se ajusten a la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación”, en su versión vigente.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

7.2. Auditorias

Con el fin de velar por el correcto uso de los recursos de su propiedad, ABANCERT se reserva el derecho de auditar a la AR en todo momento y sin previo aviso, como también solicitar auditorías de seguridad externas sobre los procesos de la PSC o como es dictaminado por norma, entregar la información para el proceso de revisión anual ordinario de la Entidad Acreditadora, resguardando 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 y que se ajusten a la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación”, en su versión vigente.

7.3. Comité de Seguridad de la Información

La misión del Comité de Seguridad de la Información es resolver las Políticas de Seguridad de la Información, sus ajustes y modificaciones, y estará formado por personal de la alta administración de la empresa. La Política de Seguridad de la información deberá ser revisada anualmente por el Comité de Seguridad y sus cambios validados por el Gerente General.

Las principales funciones del Comité están detalladas en el punto 5 del documento “PS02 - Política de Seguridad de Información de la Organización”.

7.4. Controles

El PSC dispone de controles internos de funcionamiento que regulan los aspectos que refuerzan la seguridad técnica, física, de procedimientos y de capacitación del personal los que están especificados en el punto 8 del documento “PO02 - Declaración de las Prácticas de Certificación”.

7.5. Riesgos

ABANCERT realiza la gestión de riesgos a través de su Política de Gestión de Riesgos.

7.6. Cultura de Seguridad

La forma en la que se lleva a cabo a través de lo especificado en el punto 7.9 del documento “PS02 - Política de Seguridad de Información de la Organización”.

7.7. Mantenimiento de la Infraestructura

ABANCERT cuenta con mantenimiento de los servicios de infraestructura contratados a un proveedor que cumple con las obligaciones y requisitos de la “Guía de Evaluación Procedimiento de Acreditación de Prestadores de Servicios de Certificación”, en su versión vigente, esto permite que puedan ser

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

aplicadas las mejoras de los procesos de Capacity planning que se lleven a cabo por el área de tecnología y que apruebe el SGSI.

7.8. Plan de Seguridad

Mediante el Plan de Seguridad se trabaja en los ámbitos de acción durante el año con el objetivo de proveer protección a los recursos de información según lo definido en el requisito 4.11. PS04 - Plan de seguridad de sistemas.

7.9. Plan de administración de llaves

En el documento “PS06 - Plan de Administración de llaves”, se define el plan de administración de las llaves criptográficas para ABANCERT, con el fin de resguardarlas y administrarlas durante su ciclo de vida.

7.10. 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.

7.11. 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”.

8. JERARQUÍA DE NORMAS

En todo lo no expresamente previsto por la presente Política de Certificación (CP) será de aplicación lo señalado en la CPS de ABANCERT. Los requisitos legales que la PSC debe cumplir están especificados en el punto 4.2 del documento “PS02 - Política de Seguridad de Información de la Organización”.

ABANCERT	Política de Certificación Firma Electrónica Avanzada	
Rev. 1.2	Fecha Vigencia: Noviembre de 2023	

9. REVISIÓN

Versión	Fecha	Revisión	Observaciones
1.0	07 de dic.2021	1.0	Primer documento.
1.1	Nov.2023	1.0	Segundo documento.
1.2	Ago.2024	1.0	Tercer documento. Modifica ítem 6.3.
Elaborado por: ABANCERT – Equipo de trabajo			Fecha: diciembre de 2021

**** FIN ****