DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE FIRMA AVANZADA

CERTIFICADORA DEL SUR

HOJA DE VIDA

Versión	Paginas	Fecha	Motivo del Cambio	Autor	Aprobador
V_1.0		Julio 2020	Creación del Documento	Gabriel Toro Pradines	Cristián Echeverría
V_1.1		Diciembre 2021	Se revisa y modifica según Guía de Acreditación	Cristián Altamirano	Cristián Echeverría
VF_1.0		Diciembre 2021	Se revisa y modifica según Guía de Acreditación	Cristián Altamirano	Cristián Echeverría
VF_2.0		Abril 2022	Se revisa y modifica según guía de acreditación	Matías Toro	Cristián Echeverría
VF_3.0		Abril 2022	Se revisa y modifica según guía de acreditación	Flavio Tapia	Cristián Echeverría
VF_3.1		Agosto 2022	Modificaciones en el registro del titular, la autenticación y verificación de identidad del solicitante.	Flavio Tapia	Cristián Echeverría
VF_3.2		Septiembre 2022	Modificaciones en el registro del titular, la autenticación y verificación de identidad del solicitante.	Flavio Tapia	Cristián Echeverría
VF_3.3		Agosto 2023	Se revisa y modifica según revisión de economía	Flavio Tapia	Cristián Echeverría
VF_3.4		Octubre 2023	Se revisa y modifica según revisión de economía	Flavio Tapia	Cristián Echeverría
VF_3.5		Octubre 2023	Se revisa y modifica según revisión de economía	Flavio Tapia	Cristián Echeverría
VF_3.6		Noviembre 2023	Se revisa y modifica según revisión de economía	Flavio Tapia	Cristián Echeverría

VF_3.7		Noviembre 2023	Se revisa y modifica según revisión de economía	Flavio Tapia	Cristián Echeverría

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente documento contiene la Declaración de Prácticas de Certificación (CPS) referente a los certificados de firma electrónica emitidos por Certificadora del Sur SPA, la cual está regida por la ley 19.799 "SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA", su reglamento y normas técnicas asociadas, y la Política de Certificados (CPS).

1.1. VISIÓN GENERAL

La norma chilena Nch2805.Of2003 el numeral 3.1.3 establece que la autoridad certificadora debe tener procedimientos documentados para la gestión de las claves privadas utilizadas en la emisión de certificados. Estos procedimientos deben incluir, al menos, la generación, el almacenamiento, el uso, la realización de copias de seguridad y la destrucción segura de las claves privadas.

En este documento, Declaración de Prácticas de Certificación (CPS) de Certificadora del Sur, se establecen las reglas para la solicitud, validación, aceptación, entrega, emisión y revocación de los certificados de firma electrónica emitidos por una determina Autoridad Certificadora, y sus CA subordinadas, así también se establece el uso de los certificados firma electrónica emitidos y los dispositivos seguros de creación de las claves de firma electrónica, para la CA (HSM) y para el titular (Token).

La estructura de esta Declaración de Prácticas de Certificación considera lo estipulado por la norma chilena Nch2805.Of2003 en la que se referencia la norma IETF RFC 2527 "Internet X.509 Public Key Infraestructure Certificate Policy and Certification Practices Framework", además de ETSI TS 102 042 V1.1.1 y ETSI TS 102 042 V2.1.1, en conformidad a las Disposiciones transitorias, letra a) del Decreto 181, reglamento de la Ley 19799, como marco para este tipo de documentos.

1.2. IDENTIFICACIÓN DE LA ORGANIZACIÓN RESPONSABLE DE LAS PRÁCTICAS DE CERTIFICACIÓN

Empresa	Certificadora del Sur
RUT	77.058.910-K
Dirección de Correo Electrónico y sitio web	contacto@certificadoradelsur.cl www.certificadoradelsur.cl
Dirección	Lautaro 867. Los Ángeles.
Número Telefónico	+56 2 28404640
Representante legal	José Cristian Echeverría Briones

1.3. IDENTIFICACIÓN DE LAS PRÁCTICAS

Nombre	DECLARACION DE PRACTICAS – CERTIFICADORA DEL SUR
Versión Actual	3.7
Versión Anterior	3.6
Fecha Última Actualización	NOVIEMBRE 2023
OID (Object Identifier)	1.3.6.1.4.1.55784
URL de Publicación	www.certificadoradelsur.cl

1.4. COMUNIDAD Y APLICABILIDAD

En la infraestructura de clave pública de Certificadora del Sur se relacionan distintos solicitantes de un Certificado de Firma Electrónica Avanzada con roles y actividades bien definidas: usuario o titular de certificados de Firma Electrónica Avanzada, Autoridad Certificadora (CA), Autoridad de Registro (RA) y terceras partes que confían en los certificados de Firma Electrónica Avanzada emitidos por la Autoridad Certificadora.

1.4.1. AUTORIDADES DE CERTIFICACIÓN

Es la autoridad en quien confían los usuarios o titulares para proveer los servicios de certificación de Firma Electrónica Avanzada, es decir solicitantes, y terceras partes que confían en los certificados emitidos por ella. La autoridad certificadora asegura que se cumplan los requisitos de la presente política, operando y controlando el funcionamiento de los procesos de publicación, registro, emisión, revocación y verificación del estado de certificados de Firma Electrónica Avanzada.

Así también, la Autoridad Certificadora puede subordinar a ella misma, una o más Autoridades Certificadoras Intermedias para emitir certificados de Firma Electrónica Avanzada, bajo la misma política de certificados, la declaración de prácticas de certificación y los procedimientos de ejecución.

1.4.2. AUTORIDADES DE REGISTRO

Son las autoridades que una vez comprobada fehacientemente la identidad del solicitante, como lo establece el Art. N°12, letra e de la Ley 19799, reciben, procesan y verifican las solicitudes de emisión y revocación de certificados de Firma Electrónica Avanzada, asegurando que las solicitudes sean completas, exactas y debidamente autorizadas.

1.4.3. USUARIO O TITULAR

Son aquellas personas naturales que solicitan, a través de la presentación de antecedentes ante la respectiva autoridad de registro, y que una vez comprobada fehacientemente la identidad del

solicitante, como lo establece el Art. N°12, letra e de la Ley 19799, se les emite un certificado para Firma Electrónica Avanzada, el cual es aceptado por él.

1.4.4. SOLICITANTE

Son solicitantes quienes solicitan un certificado de Firma Electrónica para sí, antes de obtenerlo. En caso de que el certificado sea emitido exitosamente y aceptado por el solicitante, el solicitante pasa a tener la calidad de Usuario o Titular, en caso contrario mantiene la de Solicitante.

1.4.5. TERCERA PARTE QUE CONFÍA

Persona natural o jurídica, que confía en un certificado de Firma Electrónica Avanzada y utiliza la clave pública de un usuario o titular. Los usuarios o titulares que utilicen los certificados emitidos bajo la Política de Certificados de Certificadora del Sur, deben conocer y estar en conformidad con lo establecido en ellas, Certificadora del Sur pone a disposición de los usuarios o titulares los certificados de componen la(s) cadena(s) de confianza.

1.4.6. ALCANCE DE LA DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN

La comunidad confía en los certificados emitidos por la Autoridad Certificadora conforme a la función y finalidad para los cuales se han emitido bajo la Declaración de Prácticas de Certificación, y a la presente Política de Certificación.

Así también, el ámbito de acción de los certificados de Firma Electrónica Avanzada emitidos a usuario o titulares se restringen al uso específico para el cual ha sido emitido el certificado.

1.4.7. FINALIDAD Y USO DE LOS CERTIFICADOS

Los certificados de firma electrónica avanzada son emitidos a personas, mayores de edad que no sean calificadas como interdictos, para firmar y encriptar y cifrar correos electrónicos. No obstante lo indicado, un certificado de firma electrónica avanzada puede ser utilizado para otros fines, siempre que las Partes que Confían sean capaces de confiar razonablemente en el Certificado y que ese uso no esté prohibido por la ley, por esta CP, por cualquier CPS bajo la cual haya sido emitido el Certificado y cualquier acuerdo con los Usuarios o Titulares.

1.4.8. USO PROHIBIDO

Los Certificados deben ser utilizados solo en la medida que su uso sea consistente con la ley 19799 “sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma”, y en particular deberán ser utilizados sólo hasta el punto que ésta lo permita, no se permite el uso del certificado contrario a la normativa chilena y a los convenios internacionales ratificados por el Estado Chileno y a lo establecido por la CPS y la Política de Certificación de la misma.

Los Certificados de CA no se pueden utilizar para cualquier función, excepto las funciones propias de CA. Por otra parte, los Certificados de usuario o titular final no deberán ser utilizados como Certificados de CA.

1.5. Organización que administra la Declaración de Practicas de Certificación

1.5.1. Datos de Contacto de la Organización

Empresa	Certificadora del Sur
Dirección de Correo Electrónico	contacto@certificadoradelsur.cl www.certificadoradelsur.cl
Dirección	Lautaro 867. Los Ángeles.
Número Telefónico	+56 2 28404640

1.5.2. Persona que determina la idoneidad de la CPS

En conformidad al Art. N° 15 la Entidad Acreditadora debe velar porque los requisitos que se observaron al momento de otorgarse la acreditación y las obligaciones que impone la ley, este reglamento y las normas técnicas se cumplan durante la vigencia de la acreditación. En este sentido, los cambios que se realicen tanto a la CP como CPS y otros documentos, deben ser también revisados por la Entidad Acreditadora.

El Gerente General de Certificadora del Sur, en conjunto Oficial de Seguridad de la Información de Certificadora del Sur, deberán velar por el fiel cumplimiento de la presente Política de Certificados y los demás documentos, los que deben ser sometidos a revisiones y auditorias, y cuando se detecte cualquier cambio se debe comunicar a la Entidad Acreditadora.

2. Disposiciones Generales

2.1. Obligaciones

2.1.1. Obligaciones de la Autoridad Certificadora Raíz

La autoridad certificado raíz deberá firmar los certificados intermedios, o de CA subordinada, de firma electrónica, y que compartan esta declaración de prácticas de certificación, estableciendo de esta manera, una cadena jerárquica de confianza determinada entre ellas.

La Autoridad Certificadora Raíz debe emitir un certificado raíz autofirmado para sí misma, en su calidad de Autoridad Certificadora. Este certificado de raíz tendrá una vigencia de 15 años, y su clave privada será generada utilizando algoritmos reconocidos por la industria.

Utilizando el certificado raíz de la autoridad certificadora raíz se firmaran los certificados de las autoridades intermedias suscritas a estas prácticas de certificación, los cuales tendrán una

vigencia igual o inferior a la de la autoridad certificadora raíz, y sus claves privadas serán generadas utilizando algoritmos conocidos por la industria, la autoridad certificadora raíz podrá anticipadamente emitir un nuevo certificado intermedio para sus autoridades certificadora intermedias debido a cambios tecnológicos, de seguridad, normativos, de continuidad operacional.

La Autoridad Certificadora deberá cumplir lo establecido en estas Prácticas de Certificación. Las obligaciones de la Autoridad Certificadora de firma electrónica Avanzada serán:

a) Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano;

b) 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;

c) 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;

d) Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten;

e) En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;

f) Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores;

g) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que dará a los datos de los certificados, especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;

h) En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere;

i) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento concursal de liquidación o que se encuentre en cesación de pagos, y

j) Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada.

2.1.2. OBLIGACIONES DE LA AUTORIDAD DE REGISTRO

La respectiva autoridad de registro deberá acreditar fehacientemente la identidad del solicitante.

Las obligaciones de la autoridad de registro serán:

- Identificar y comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica" (Art. 12, letra e) de la Ley N° 19.799).
- Enviar información fidedigna a la Autoridad Certificadora correspondiente
- Almacenar en forma segura, y durante a lo menos seis años que exige la Ley N° 19.799, la documentación aportada en el proceso de emisión de un certificado.

2.1.3. OBLIGACIONES DEL USUARIO O TITULAR

El Usuario o Titular 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, notificando inmediatamente a la AR o PSC según corresponda, en conformidad al Art. 24 de la Ley 19.799.

Además, velará por el correcto uso y resguardo de su llave privada, así como también podrá solicitar la revocación o suspensión de los certificados en cualquier momento, siempre que la causa de revocación o suspensión se ajuste a las causas de revocación detalladas en la Política de Certificados, y en la presente Declaración de Prácticas de Certificación que dependen de esta Política.

Deberá además conocer la Política de Certificados y las respectivas Declaraciones de Prácticas de Certificación que pudiesen aplicárseles.

Certificadora del Sur dispondrá de un acceso para conocer la Política de Certificados y las respectivas Declaraciones de Prácticas de Certificación, las cuales están disponibles en el siguiente enlace:

https://www.certificadoradelsur.cl/website/descargas.jsp

El Usuario o Titular deberá, además:

- Conocer y aceptar las condiciones (vigencia y propósito) del Certificado de Firma Electrónica, lo cual se hace efectivo a través de la aceptación mediante firma y huella dactilar con tinta estampada en el Formulario de Entrega de Certificado de Firma Electrónica avanzada que será emitido para él.
- Notificar a la Autoridad Certificadora o la Autoridad de Registro de cualquier cambio en los antecedentes proporcionados durante su solicitud.
- Conocer la presente Declaración de Prácticas de Certificación, las que estarán disponibles en el siguiente enlace:
  https://www.certificadoradelsur.cl/website/descargas.jsp
- Realizar su solicitud conforme a estas Prácticas de Certificación
- Verificar que la información del certificado de firma electrónica esté correcta y sea consistente con la entregada durante su registro; en caso de encontrar información errónea o inexacta deberá dar aviso inmediatamente a la Autoridad de registro.
- No revelar la clave de acceso a la clave privada del certificado de firma electrónica.
- Informar a la respectiva Autoridad de Registro de cualquier situación que pueda afectar la validez de los certificados y/o compromiso de la clave privada.
- Solicitar la revocación o suspensión del certificado de firma electrónica en caso de ser necesario.
- Cualquier otra obligación que derive de la ley, el reglamento y las prácticas de certificación asociadas al tipo de firma electrónica que se le ha emitido.
- Deberá tener en cuenta el propósito y las limitaciones del uso de los certificados de Firma Electrónica descritos en la presente declaración de prácticas de certificación asociadas al Certificado de firma electrónica avanzada que está utilizando.
- Deberá hacerse responsable de la custodia de su token criptográfico correspondiente a la marca Watchdata modelo PROXKey que cumple con el estándar de seguridad FIPS 140-2 nivel 3 en el que será almacenado su certificado digital, en el caso de que el Usuario o Titular se presente con otro Token criptográfico de mercado, Certificadora del Sur proporcionará un token criptográfico marca Watchdata modelo PROXKey para el almacenamiento de su nuevo Certificado de Firma Electrónica Avanzada.
- Conocer la clave de acceso a su token criptográfico para poder hacer uso de su certificado digital.

2.1.4. OBLIGACIONES DEL SOLICITANTE Y DEL USUARIO O TITULAR

Los solicitantes de los certificados de firma electrónica avanzada quedarán obligados, en el momento de proporcionar los datos de su identidad, a brindar declaraciones exactas y completas de los mismos. 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.

2.1.5. OBLIGACIONES DE LAS TERCERAS PARTES QUE CONFÍAN

Quién confía en el certificado de Firma Electrónica Avanzada emitido por la Autoridad Certificadora Intermedia deberá conocer las normas legales, verificar la autenticidad, validez y las condiciones del certificado de Firma Electrónica Avanzada en que está confiando.

Certificadora del Sur pone a disposición de Terceras Partes que Confían los siguientes enlaces:

Normas Legales

https://www.certificadoradelsur.cl/website/descargas.jsp

La verificación de las firmas electrónicas emitidas por la Certificadora, se puede realizar en el siguiente enlace:

https://solicitudes.certificadoradelsur.cl/solicitudes/certificado.jsp.

2.1.6. CONFIANZA EN LOS CERTIFICADOS

Los usuarios o titulares que confían en un certificado de Firma Electrónica Avanzada deberán conocer las normas legales, verificar la autenticidad, validez y las condiciones del certificado de Firma Electrónica Avanzada en que está confiando.

Normas Legales

https://www.certificadoradelsur.cl/website/descargas.jsp

2.2. OBLIGACIONES LEGALES DE LA ORGANIZACIÓN

La organización responsable de la Política tiene las siguientes obligaciones, de acuerdo a esta Política, las Declaraciones de Prácticas de Certificación, y la ley 19799 “sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma”:

a) Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios o titulares de manera sencilla y en idioma castellano;

b) Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos vigentes, suspendidos, revocados, traspasados y homologados y los que queden sin efecto. A dicho registro podrá accederse por medios electrónicos de manera continua y regular.

c) Conservar los datos del registro público antes señalado por a lo menos durante seis años desde la emisión inicial de los certificados.

d) En el caso de cesar voluntariamente en su actividad, deberá comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por la organización y, 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;

e) Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten;

f) En el otorgamiento de certificados de Firma Electrónica Avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;

g) Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores;

h) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vaya a cesar su actividad, y comunicarle el destino que vaya a dar a los datos de los certificados especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;

i) En caso de cancelación de la inscripción en el registro de prestadores acreditados, comunicar inmediatamente esta circunstancia a cada uno de los usuarios o titulares y traspasar los datos de sus certificados a otro prestador, si el usuario o titular no se opusiere;

j) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos, y

k) Cumplir con las demás obligaciones legales, especialmente las establecidas en la ley N° 19.799, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores y Nº 19.628, sobre Protección de la Vida Privada.

2.2.1. LIMITACIÓN DE RESPONSABILIDAD

En ningún caso la Autoridad Certificadora será responsable de los daños que tengan origen en el uso indebido o fraudulento de un certificado de Firma Electrónica Avanzada.

Un certificado de Firma Electrónica Avanzada provisto por la Autoridad Certificadora podrá establecer límites en cuanto a los posibles usos del certificado contenidos en la ley 19799 “sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma”, en cuyo caso, la Autoridad Certificadora quedará eximida de cualquier responsabilidad por el uso que se dé a dichos certificados y que excedan tales límites.

La Autoridad Certificadora quedará exenta de responsabilidad en caso que no pueda cumplir con las obligaciones señaladas en el presente documento por fuerza mayor o caso fortuito. Se entenderá que existe fuerza mayor en caso de que, por cambios regulatorios en leyes o reglamentos que no puedan ser anticipados, así como estados de excepción en el territorio de Chile, se vean interrumpidos o modificados los servicios de la PSC. Existirá caso fortuito cuando los servicios de la Autoridad Certificadora se interrumpan o modifiquen por catástrofes naturales, tales como terremotos o epidemias, o por circunstancias que afecten las instalaciones, conectividad o personal de la misma, entre ellos: daños informáticos producidos por programas o elementos imprevisibles de acuerdo a los estándares de la industria, interrupción prolongada de servicios y suministros básicos, entre otros.

La Autoridad Certificadora no será responsable de los daños derivados del uso malicioso del certificado digital por parte de su Titular.

La Autoridad Certificadora no será responsable de la incorrecta utilización de los certificados y las llaves, ni de cualquier daño indirecto que pueda resultar de la utilización del certificado, o de la información suministrada por la Autoridad Certificadora. En particular, el lucro cesante y la pérdida de ingresos o pérdida de datos serán considerados daños indirectos y no darán lugar a indemnización alguna.

La Autoridad Certificadora no será responsable de los daños que se deriven de aquellas operaciones en que se hayan superado las limitaciones de uso que se señalan en la política de certificado y las Prácticas de Certificación de cada tipo de certificado.

La Autoridad Certificadora no será responsable de las eventuales inexactitudes en el certificado producto de errores en la información que haya sido presentada por el solicitante en su solicitud de certificado, cuando la comprobación fehaciente de la identidad del solicitante no se haga ante la propia Autoridad Certificadora.

2.3. OBLIGACIONES DE REPOSITORIO

La Autoridad Certificadora contará con un repositorio de Acceso Público, el que contendrá un registro del estado de todos los certificados emitidos vigentes, suspendidos, revocados, traspasados y homologados.

2.4. RESPONSABILIDADES

2.4.1. RESPONSABILIDAD PSC COBERTURA DE SEGUROS

Certificadora del Sur debe mantener un nivel razonable de cobertura de seguro por errores y omisiones, para lo cual mantendrá al menos el seguro de responsabilidad civil exigido en el Art. N° 14 de la Ley N° 19.799, para cubrir los daños causados por errores y omisiones.

2.4.2. RESPONSABILIDAD USUARIO O TITULAR

Los titulares de los certificados digitales se encuentran obligados a:

a) Comunicar cualquier error o inexactitud en el certificado.
b) Usar los datos de creación de firma asociados al certificado para fines legales, y no ilícitos.
c) No usar el certificado para actuar como certificador de firma electrónica.
d) Comunicar inmediatamente el compromiso, pérdida, hurto, robo, acceso no autorizado o extravío, falsificación de sus datos de creación de firma o certificado o cualquier circunstancia que pudiera ser causal de suspensión o revocación de un Certificado.
e) Solicitar la suspensión o revocación del certificado cuando se presente alguna de las causales indicadas para este efecto.
f) No usar los datos de creación de firma una vez que el certificado haya expirado o haya sido solicitada la suspensión o revocación.

2.4.3. RESPONSABILIDAD SOLICITANTE

Los solicitantes de certificados digitales de firma electrónica avanzada tendrán las siguientes obligaciones:

1. Entregar información fidedigna al momento de realizar la solicitud del certificado.
2. Ingresar personalmente la clave privada del certificado.
3. Pagar el precio convenido, aun cuando no se acepten o no se ocupen los certificados emitidos.

2.4.4. INDEMNIZACIÓN POR PARTE DE LOS USUARIOS O TITULARES

En la medida que la legislación vigente no lo prohíba, los Usuarios o Titulares tienen la obligación de indemnizar a la Autoridad Certificadora, en caso de:

- Uso indebido o fraudulento de los certificados digitales emitidos por la Autoridad Certificadora.
- Infracciones a los derechos de propiedad intelectual de la Autoridad Certificadora.

2.4.5. INDEMNIZACIÓN DE LAS PARTES QUE CONFÍAN

No aplica.

2.4.6. RELACIONES FIDUCIARIAS

No aplica.

2.5. INTERPRETACIÓN Y EJECUCIÓN

2.5.1. LEY APLICABLE

Ley 19.799, “SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA AVANZADA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA”, y su reglamento; así como también Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada y cualquier ley de la República de Chile podrán ser aplicadas según ejecución, interpretación, y validez de esta Política de Certificados.

2.5.2. DIVISIBILIDAD, SUPERVIVENCIA, FUSIÓN Y AVISO

La autoridad certificadora considerará una antelación mínima de dos meses al cese efectivo de la actividad", de acuerdo al Art. N° 12, letra c), g) y h) de la Ley 19.799, para notificar a los Usuarios o Titulares y terceros que confían en caso que exista divisibilidad de la autoridad certificadora, y tomará los resguardos necesarios de tal forma de no afectar la continuidad en las operaciones de los Usuarios o Titulares.

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 establece 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.

2.6. PROCEDIMIENTO DE RESOLUCIÓN DE DISPUTAS

Las disputas entre cualquier miembro de la comunidad sobre la que aplica la presente Declaración de Practicas de Certificación, se resolverán en función de los acuerdos que se

puedan haber suscrito entre las partes. En la medida que sea permitido por la legislación vigente, todos los acuerdos suscritos deberán contener una cláusula de resolución de conflictos.

2.7. TARIFAS

2.7.1. TARIFA DE EMISIÓN O RENOVACIÓN DE CERTIFICADOS

Los precios se encuentran publicados en:

https://www.certificadoradelsur.cl/website/documentos/politica_precios.pdf

2.7.2. TARIFA DE ACCESO AL CERTIFICADO

No Aplica.

2.7.3. TARIFA DE ACCESO A LA INFORMACIÓN DE REVOCACIÓN DEL CERTIFICADO

No Aplica.

2.7.4. TARIFA PARA OTROS SERVICIOS, COMO INFORMACIÓN DE LA POLÍTICA

No Aplica.

2.8. POLÍTICAS DE REEMBOLSO

Se aplican las normas de reembolso consideradas en la Ley N° 19.496, sobre protección del consumidor, respecto de las compras realizadas en forma electrónica.

2.9. PUBLICACIÓN Y REPOSITORIOS

2.9.1. PUBLICACIÓN DE LA INFORMACIÓN DE LA AUTORIDAD CERTIFICADORA

La Autoridad Certificadora publicará a través de su sitio web https://www.certificadoradelsur.cl/website/descargas.jsp, lo siguiente:

- La Política de Certificados
- Las presente Prácticas de Certificación

- La información respecto al estado de vigencia y validez de los certificados emitidos, suspendidos, revocados, traspasados y homologados
- Los certificados digitales correspondientes a la cadena de confianza de la Autoridad Certificadora
- La lista de los certificados revocados (CRL)
- La Declaración de Privacidad
- La Política de Precios
- La Política de Reembolso
- Material de soporte y manuales de uso de los certificados digitales
- Resolución de aprobación de Acreditación emitida por la Subsecretaria de Economía y Empresas de Menor Tamaño.
- Certificados de Raíz e Intermedios de Otras Autoridades Certificadoras.

Lo anterior corresponde a información de carácter público, la cual se mantendrá actualizada y no contará con ningún tipo de control de acceso.

2.9.2. FRECUENCIA DE LA PUBLICACIÓN

Para la documentación publicada referente a Políticas y Prácticas de Certificación, estas se publicarán nuevamente cada vez que exista un cambio en ellas, manteniendo la versión anterior e indicando la fecha de entrada en vigencia de la nueva Política y/o Práctica de Certificación.

Las CRL serán actualizadas y publicadas cada 24 horas, permaneciendo publicada la última versión de la CRL.

2.9.3. CONTROLES DE ACCESO

Para la información de carácter público, no se establecen controles de acceso de ningún tipo.

2.9.4. REPOSITORIOS

Certificadora del Sur es la encargada de mantener un repositorio en línea, con acceso público, donde se publicará:

- Distintas Políticas relevantes para la Infraestructura de Llave Pública
- Todos los certificados emitidos vigentes por la Autoridad Certificadora
- Todos los certificados revocados y suspendidos por la Autoridad Certificadora
- Todos los certificados traspasados y homologados por la Autoridad Certificadora
- Otra información relevante para la Infraestructura de Llave Publica

Este repositorio se ubicará en https://solicitudes.certificadoradelsur.cl/solicitudes/certificado.jsp

3. AUDITORÍA Y CUMPLIMIENTO

Certificadora del Sur reconoce y declara la importancia y el valor del resguardo que tiene para la organización identificar y proteger los activos de información a través de la implementación de un Sistema de Gestión de Seguridad de la Información orientado a definir las directrices que permitan resguardar la confidencialidad, integridad y disponibilidad de la información de la organización y de terceros, asegurando la continuidad del negocio en conjunto con el cumplimiento de las disposiciones legales vigentes.

Para asegurar dicho cumplimiento se consideran las Inspecciones Anuales Ordinarias e Inspecciones extraordinarias que realiza la Entidad Acreditadora (Art. N° 20 de la Ley N° 19.799).

Adicionalmente para velar por dicho sistema, Certificadora del Sur solicitará a entes externos la realización de auditorías de cumplimiento para fortalecer dicho proceso, según lo estime conveniente.

3.1. FRECUENCIA DE LA AUDITORIA DE CUMPLIMIENTO

La Entidad Acreditadora, en conformidad a la Ley 19799 realiza inspecciones anuales, por ende la periodicidad de las auditorías internas, externas y la revisión de la evaluación de riesgos y amenazas, serán ser realizadas anualmente.

3.1.1. IDENTIDAD Y EXPERIENCIA DEL AUDITOR

Certificadora del Sur podrá delegar la realización de esta auditoría a un ente calificado, al cual se le exigirá contar con experiencia comprobada en las materias a auditar.

3.1.2. RELACIÓN DEL AUDITOR CON LA PARTE AUDITADA

Estas evaluaciones serán llevadas a cabo por terceros, los cuales deben ser completamente independientes de Certificadora del Sur. Estas entidades externas no deben tener conflicto de interés sobre las materias auditadas.

3.1.3. TEMAS CUBIERTOS POR LA AUDITORIA

Todos los que Certificadora del Sur estime convenientes, en función del cumplimiento de la guía de acreditación, estándares internacionales, otro tipo de certificaciones, o materias financieras.

3.1.4. ACCIONES TOMADAS COMO RESULTADO DE LA AUDITORIA

Se solicitará a la entidad auditora que entregue un informe preliminar, sobre el cual Certificadora del Sur podría tomar acciones correctivas, sin ser obligatorio dependiendo del tipo de auditoría.

Sin prejuicio de lo anterior, Certificadora del Sur, de buena fe, hará todos los esfuerzos razonables para abordar un plan de acción que pueda mitigar, en un plazo de tiempo razonable, cualquier brecha o deficiencia que pudiera detectar esta auditoría.

Los tiempos de remediación se especificarán en el plan de trabajo.

3.1.5. COMUNICACIÓN DE RESULTADOS

Después de cualquier auditoria, los resultados deberán ser comunicados no más allá de diez días hábiles desde la finalización de la auditoria.

Certificadora del Sur será libre de publicar, o no, los informes de auditoría respectivos, así como las medidas de mitigación adoptadas sobre este informe, en caso que existieran.

3.2. PROCEDIMIENTOS DE AUDITORIA DE SEGURIDAD

3.2.1. TIPOS DE EVENTOS REGISTRADOS EN EL LOG DE AUDITORIA

A continuación, se detallan todos los eventos e incidentes que debe registrar la Autoridad Certificadora y Autoridad de Registro. Todos estos registros, electrónicos y manuales deben contener fecha y hora del evento o incidente.

Los eventos auditables son:

- Eventos Operacionales: Como mínimo se deberá registrar:
    - Generación de llaves propias de una Autoridad Certificadora y las llaves de las CA intermedias, o subordinadas
    - Inicio y detención de los sistemas y aplicativos
    - Cambio en los datos de Autoridades Certificadoras, o llaves
    - Eventos relativos al ciclo de vida del módulo criptográfico
    - Posesión de la data para activación de llaves
    - Evidencia y registro de destrucción de medios que contienen material de llaves, datos de activación, o cualquier otro tipo de información personal del órgano Usuario o Titular.
- Eventos relativos al ciclo de vida del certificado de Firma Electrónica Avanzada
- Eventos de empleados de confianza: Como mínimo se deberá registrar:
    - Inicio de sesión, e intentos erróneos de inicio de sesión.
    - Cierre de sesión
    - Creación, eliminación y cambio de contraseñas
    - Cambios en los privilegios de los usuarios o titulares con privilegios
- Informes de Compromisos, como inicio de sesión no autorizados a los sistemas o a la red.
- Operaciones con errores de lectura o escritura en los certificados y el repositorio.
- Incidentes de seguridad, esto es aquellos que amenacen la confidencialidad, integridad y disponibilidad de la información.

3.2.2. FRECUENCIA DE PROCESAMIENTO DEL LOG DE AUDITORIA

Los registros serán revisados cada vez que sea requerido a causa de alguna alerta basada en irregularidades, o incidentes, entro de los sistemas de la Autoridad Certificadora o Autoridad de Registro.

3.2.3. PERIODO DE RETENCIÓN DEL LOG DE AUDITORIA

Los registros deben ser retenidos por un periodo de 6 meses después de su procesamiento, y luego deben ser archivados.

3.2.4. PROTECCIÓN DEL LOG DE AUDITORIA

Certificadora del Sur implementa controles físicos y tecnológicos para proteger los archivos contra eliminación, modificación u otra manipulación.

3.2.5. PROCEDIMIENTO DE RESPALDO DEL LOG DE AUDITORIA

Certificadora del Sur realiza diariamente respaldos incrementales de los registros de auditoría.

3.2.6. SISTEMA DE RECOLECCIÓN DE LOGS DE AUDITORIA

No Aplica.

3.2.7. NOTIFICACIÓN DE MATERIAS CAUSA-EVENTO

Todos los incidentes deben ser reportados. Los eventos serán reportados en la medida que la Declaración de Prácticas de Certificación lo determinen.

3.2.8. ANÁLISIS DE VULNERABILIDADES

La plataforma tecnológica completa de la Infraestructura de Llave Publica de Certificado del Sur, debe ser sometida a análisis de vulnerabilidades cada vez que existan cambios en sus componentes.

3.2.9. ARCHIVO DE LOS REGISTROS

Los archivos deberán cumplir con las normas de confidencialidad, privacidad y protección de datos a que se hace referencia en esta Declaración de Practicas de Certificación.

3.2.9.1. TIPO DE EVENTOS REGISTRADOS EN EL ARCHIVO DE REGISTROS

Las Autoridades Certificadoras y Autoridades de Registro deben mantener los siguientes archivos:

- Información relativa al ciclo de vida del certificado
- Información de Solicitud de certificados
- Todos los datos de auditoria
- Documentación y registros que sustentan la validación de los certificados

3.2.9.2. PERIODO DE RETENCIÓN PARA EL ARCHIVO DE REGISTROS

La Autoridad Certificadora asegurará que toda la información concerniente al proceso de emisión de certificados, su revocación y publicación se mantendrá disponible durante 6 años. Luego de ese periodo se procederá a archivar en formato digital. Podrían existir otras normas para el periodo de archivo de registros, las cuales estarán especificadas en la presente Declaración de Prácticas de Certificación.

3.2.9.3. PROTECCIÓN DEL ARCHIVO DE REGISTROS

Los archivos deben contar con medios de protección, de tal forma que solamente las personas autorizadas de la Autoridad Certificadora tengan acceso a ellos.

Los archivos deben estar protegidos contra accesos no autorizados, modificaciones, eliminaciones, etcétera.

3.2.9.4. PROCEDIMIENTO DE RESPALDO DEL ARCHIVO DE REGISTROS

Certificadora del Sur realiza diariamente respaldos incrementales de los registros de auditoría.

3.2.9.5. REQUERIMIENTOS PARA ACCESO A ARCHIVO DE REGISTROS

Todos los accesos a las entradas de certificados, revocación, y listas de revocación deben tener fecha y hora.

3.2.9.6. SISTEMA DE RECOLECCIÓN DE ARCHIVO DE REGISTROS

Para velar por la seguridad de los sistemas, activos y procedimientos del PSC, Certificadora del Sur implementa un sistema automatizado de recolección de bitácoras operacionales de los diferentes componentes de la plataforma. Los registros capturan fecha y hora del suceso, máquina y usuario de sistema, aplicativo y mensaje del aplicativo pertenecientes al suceso. Se registran entre otros, los siguientes sucesos:

- Peticiones válidas e inválidas enviadas hacia servicios WEB
- Comandos ejecutados en los terminales de los servidores

- Actividades realizadas por los operadores a nivel de la Autoridad de Registro y automáticas que forman parte de los procesos de atención.
- Actividades automáticas y manuales ejecutadas, fallidas y exitosas, realizadas a nivel de la Autoridad Certificadora
  - ✓ Asignación de permisos de operadores
  - ✓ Desasignación de permisos de operadores
  - ✓ Cambios de configuración
  - ✓ Emisión de las listas CRL
  - ✓ Eventos de ciclo de vida de los certificados personales de Firma Electrónica Avanzada
  - ✓ Eventos de ciclo de vida de los certificados raíces e intermedios de la Autoridad Certificadora
  - ✓ Activación de la conexión entre la Autoridad Certificadora y el dispositivo HSM que protege las llaves privadas de esta
  - ✓ Desactivación de la conexión entre la Autoridad Certificadora y el dispositivo HSM que protege las llaves privadas de esta
- Resultados de ejecución de tareas de respaldo.

3.2.9.7. PROCEDIMIENTO PARA OBTENER Y VERIFICAR INFORMACIÓN DEL ARCHIVO DE REGISTROS

Únicamente personal autorizado de Certificadora del Sur pueden tener acceso al archivo. La integridad de la información se verificará cuando el archivo necesite ser restaurado.

4. OTRAS MATERIAS LEGALES

4.1. POLÍTICA DE PRIVACIDAD

Las operaciones que se realicen en el marco de esta política de certificado se sujetaran a lo dispuesto en la Ley 19.628, sobre protección de la vida privada y a la Política de Privacidad de Certificadora del Sur detallada en el documento “Política de Privacidad del PSC _ VF_2.0”, como se indica a continuación.

4.1.1. INFORMACIÓN PERSONAL RECOPILADA

Certificadora del Sur solicita los usuarios o titulares la información necesaria para emitir un certificado digital, de acuerdo a esta CPS y la CP, lo que es informado en forma previa al mismo usuario o titular.

No se solicita a quienes visitan el sitio información alguna adicional a la señalada, salvo lo relativo a la información de contacto, en el caso de consultas y suscripción a listas de correo.

A las personas que realizan consultas, se le solicitarán una serie de datos personales que le serán informados en el mismo formulario, esta información es solicitada con el objetivo de poder contactarlo y dar respuesta a su requerimiento.

Dentro de los datos solicitados a los usuarios o titulares, se encuentra el correo electrónico, el que es utilizado para enviar información sobre los servicios asociados a certificación digital entregados por la organización.

4.1.1.1. DATOS SENSIBLES

No se solicita a los usuarios o titulares la entrega de datos sensibles.

4.1.1.2. DATOS PERSONALES RELATIVOS A OBLIGACIONES DE CARÁCTER ECONÓMICO, FINANCIERO, BANCARIO

No se solicita a los usuarios o titulares la entrega de datos personales relativos a obligaciones de carácter económico, financiero, bancario.

4.1.1.3. INFORMACIÓN ESTADÍSTICA SOBRE LA VISITA

Certificadora del Sur puede recopilar información estadística sobre las visitas realizadas a su sitio web, esta información no identifica personalmente al visitante, sino solo registra una visita al sitio web.

Dentro de la información estadística que puede ser recopilada, se encuentra:

- Número de personas que visita el sitio por día
- Dirección IP del equipo desde donde se hace la consulta
- Secciones visitadas dentro del sitio web
- Dominio(s) desde el cual accede el visitante
- Navegador y Sistema Operativo utilizado

El Usuario o Titular y el solicitante pueden oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión, seleccionando esa opción al terminar el proceso de enrolamiento.

4.1.2. TRATAMIENTO DE DATOS

4.1.2.1. FINALIDAD

Solo se utiliza los datos entregados por los usuarios o titulares, para la emisión, renovación, suspensión o revocación de un certificado digital. Se informa a los solicitantes y Usuarios o Titulares la información recopilada por la organización, y el tratamiento de que será objeto.

4.1.2.2. BASE JURÍDICA DEL TRATAMIENTO

La Ley N° 19.628 es la base jurídica del tratamiento de datos, tal como se indica en el Contrato Marco suscrito por el usuario o titular.

4.1.2.3. RESPONSABLE DEL REGISTRO DE DATOS

La organización es la responsable del registro de datos.

4.1.3. TRATAMIENTO DE DATOS

Solo se utiliza los datos entregados por los usuarios o titulares, para la emisión, renovación, suspensión o revocación de un certificado digital. Se informa a los solicitantes y Usuarios o Titulares la información recopilada por la organización, y el tratamiento de que será objeto.

4.1.4. ELIMINACIÓN DE DATOS

El sitio web mantiene la custodia de los datos entregados por el titular por el período que señala la Ley N° 19.799 (6 años), luego de lo cual se eliminan.

Los usuarios o titulares pueden solicitar la modificación de los datos almacenados, cuando sean erróneos, inexactos, equívocos o incompletos, y solicitar la eliminación de las bases de datos utilizadas por la organización para enviar correos electrónicos con información sobre certificados digitales.

La página web no indica que esta eliminación tenga costo alguno para el usuario o titular.

4.1.5. DERECHOS DE LOS TITULARES DE DATOS

- Solicitar la rectificación de los datos personales almacenados
- Solicitar la eliminación de su correo electrónico de la base de datos de correos electrónicos para el envío de información a usuarios o titulares.
- Solicitar la eliminación de sus datos una vez transcurridos 6 años desde la emisión del certificado digital para el cual fueron entregados.

4.1.6. INFORMACIÓN DIVULGADA POR LA ORGANIZACIÓN

4.1.6.1. INFORMACIÓN CATALOGADA COMO CONFIDENCIAL

La Autoridad Certificadora y la Autoridad de Registro deberán considerar como confidencial la información entregada por los Usuarios o Titulares y solicitantes de certificados, y solo podrá ser utilizada para los propósitos de certificación y lo especificado en la Política de Certificación y en estas Prácticas de Certificación.

La información catalogada como confidencial es protegida por la organización de manera razonable y diligente, de acuerdo a los estándares de seguridad utilizados en la industria. Los documentos que describen los controles de seguridad no técnicos (es decir, controles físicos, de

procedimiento y de personal) utilizados por la organización para realizar de forma segura las funciones de archivo, protección y auditoría de la seguridad de la información se mantienen reservados, y su cumplimiento es auditado al menos de forma anual.

4.1.6.2. INFORMACIÓN CATALOGADA COMO NO CONFIDENCIAL

La Autoridad Certificadora podrá entregar la información especificada en el certificado de Firma Electrónica Avanzada, la cual está definida en la Ley 19.799 sobre documentos electrónicos, Firma Electrónica Avanzada y los servicios de certificación de dicha firma.

4.1.6.3. DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN, O SUSPENSIÓN DE CERTIFICADOS

La Autoridad Certificadora publicara el estado de vigencia de los certificados emitidos, suspendidos, revocados, traspasados y homologados de los certificados de firma electrónica avanzada emitidos por ella a través de cualquiera de sus CA. Esta información será publicada en el sitio web de la Autoridad Certificadora. La información de revocación se podrá consultar a través de:

- Lista de revocación de cada CA subordinada, la cual será publicada en https://www.certificadoradelsur.cl/crl/c3.crl
- Servicio de Consulta de Estado de Certificados mediante OCSP (Online Certificate Status Protocol)

4.1.6.4. ENTREGA DE INFORMACIÓN POR SOLICITUD JUDICIAL

Los usuarios o titulares de firma electrónica avanzada, aceptan que Certificadora del Sur tendrá derecho a revelar información privada en los siguientes casos:

- La revelación es solicitada en citaciones y órdenes judiciales
- La revelación es necesaria en términos de participación en un proceso judicial, administrativo o de otra índole legal que involucre a la organización, respecto de los certificados digitales que han sido emitidos.

4.1.7. ENTREGA DE INFORMACIÓN A SOLICITUD DEL USUARIO O TITULAR

El propietario de la información podrá solicitar la entrega de información relativa a los procesos asociados únicamente a la solicitud, entrega, aceptación, instalación y revocación de su propio certificado de firma electrónica.

4.1.8. OTRAS CIRCUNSTANCIAS DE ENTREGA DE INFORMACIÓN

INFORMACIÓN DEL CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA

Los Certificados de Firma Electrónica Avanzada se emitirán bajo el estándar X.509v3 y deberán incluir la siguiente información individual:

Campo	Descripción/Observación	Valor de Ejemplo
Versión (version)	Version correspondiente a estándar X.509 del certificado de firma electrónica del titular	V3(0X2)
Número de Serie (SerialNumber)	Numero único dado por la Autoridad Certificadora de Firma Electrónica Avanzada	486de6cf17fa0de9
Algoritmo de Firma (Signature)	Identificador del Algoritmo y función de Hash utilizada por la Autoridad Certificadora, al firmar el certificado de Firma Electrónica Avanzada	SHA-256 with RSA Encryption
Emisor (Issuer)	Nombre Distintivo (DN) del emisor	CN= Firma Electronica Avanzada Certificadora del Sur OU= Terminos de Uso en https://www.certificadoradelsur.cl O=Certificadora del Sur C=CL
Vigencia	Fecha y hora de inicio y fin de la vigencia del certificado de firma electrónica, en formato UTC. Para certificados de Firma Electrónica Avanzada el certificado tiene como máximo 3 años de vigencia	[FECHA DE INICIO] No antes 3/7/2020 12:06:46 (hora estándar de Chile) [FECHA DE EXPIRACIÓN] 3/7/2023 12:06:46 (hora estándar de Chile)
Sujeto (Titular)	Nombre Distintito del Titular. Initials se utilizará para incorporar el Rut del Titular.	CN = Jose Cristian Echeverria Briones E = echeverria@certificadoradelsur.cl Initials = 11960129-0 C = CL
Clave Pública	Clave pública del titular del certificado	RSA encryption (1.3.6.1.4.1.55784.1.4.2.1) Largo = 2048 bits o superior

Extensión – Uso de Clave	Uso de Clave RSA	Digital Signature, Non-Repudiation, Key Encipherment
Extensión – Uso extendido de Clave	Uso de Clave RSA	Client Authentication Email Protection
Extensión – Nombre Alternativo del Sujeto	Nombre alternativo del titular, el cual contiene el valor del Rut del Titular	Otro nombre: 1.3.6.1.4.1.8321.1=30 0c 0c 0a 31 33 38 34 35 32 38 30 2d 38
Extensión – Nombre Alternativo del Emisor	Nombre alternativo del PSC, el cual contiene el valor del Rut del PSC	Otro nombre: 1.3.6.1.4.1.8321.2=30 17 a0 02 1b 00 a1 11 30 0f a0 03 02 01 00 a1 08 30 06 1b 04 6e 75 6c 6c
Extensión – Lista de Revocación & Punto de Publicación	URL de la lista de distribución	https://www.certificadoradelsur.cl/crl/c3.crl

4.2. DERECHOS DE PROPIEDAD INTELECTUAL

Todos los documentos generados por la Autoridad Certificadora son propiedad de su autor.

Los documentos definidos como públicos pueden ser reproducidos respetando las restricciones indicadas en cada uno de ellos.

Se definen como documentos públicos los siguientes:

- Política de Certificados
- Declaración de Prácticas de Certificación
- Política de privacidad

5. IDENTIFICACIÓN Y AUTENTICACIÓN

5.1.1. REGISTRO INICIAL

5.1.1.1. TIPOS DE NOMBRES

Los certificados de firma electrónica contienen un campo llamado Distinguished Name, o DN (Nombre Distinguido) en el campo Subject (Asunto).

Dentro del campo Subject, se incluye un campo llamado Common Name, o CN (Nombre Comun).

El valor autenticado del Nombre Común, es el nombre completo del solicitante de certificado de firma electrónica, para el caso de los certificados de firma electrónica avanzada.

Cada titular de un certificado de firma electrónica será identificado a través de su nombre completo (nombres, apellido paterno y apellido materno), el cual es entregado por el SRCEI.

La información del nombre del titular quedará en el certificado de firma electrónica en el campo "CN – Common Name", se respetarán las mayúsculas, minúsculas y tildes de acuerdo a la Cedula de Identidad facilitado por el solicitante al momento de ser validado.

Finalmente, en el campo C, se incluirá el país en forma ISO 9660, email incorporará el email que el usuario ingrese, y el rol único nacional del titular a través del campo "Initials", el cual se ingresará de forma manual de acuerdo al Cedula de Identidad facilitado por el solicitante al momento de ser validado.

Todos estos campos se representan a través de la definición del Nombre Distintivo (Distinguished Name) se lo especificado en el estándar X.500 y X.520.

Common Name (CN)	[NOMBRE Y APELLIDOS]
Country (C)	[CL]
Email (Email)	[EMAIL DEL TITULAR]
Initials	[RUN DEL TITULAR]

5.1.1.2. VERIFICACIÓN GENERAL

Los datos del Common Name serán digitados directamente por un funcionario de Certificadora del Sur, una vez validado el solicitante.

Los datos de la solicitud del solicitante y el certificado de firma electrónica serán verificados por el personal que Certificadora del Sur defina para estos efectos, donde la información mínima a certificar será la siguiente:

- Información entregada por el SRCEI, referente a los nombres, apellido paterno, apellido materno y rol único nacional
- Email

5.1.2. NECESIDAD DE NOMBRES SIGNIFICATIVOS

Los certificados deberán contener nombres significativos con una semántica comúnmente entendible, que permitan identificar inequívocamente al solicitante del certificado.

5.1.3. REGLAS PARA INTERPRETAR VARIAS FORMAS DE NOMBRES

No aplica.

5.1.4. UNICIDAD DE LOS NOMBRES

Como regla general, los nombres de los titulares de certificados de firma electrónica avanzada no siempre serán únicos, sin embargo, los titulares de certificados de firma electrónica avanzada siempre pueden ser identificados de forma única a través de su Rut (cedula de identidad).

Es posible para un titular de certificado de firma electrónica avanzada, tener dos o más certificados, con el mismo nombre en el campo Common Name.

5.1.5. PROCEDIMIENTO DE RESOLUCIÓN DE DISPUTAS DE RECLAMOS DE NOMBRES

No aplica.

5.1.6. RECONOCIMIENTO, AUTENTICACIÓN Y FUNCIÓN DE LAS MARCAS REGISTRADAS

No Aplica.

5.1.7. MÉTODO PARA PROBAR LA POSESIÓN DE LA LLAVE PRIVADA

El titular de certificado de firma avanzada debe demostrar que es poseedor de la llave privada contenida en el Token, esto lo puede demostrar firmando algún documento con dicho certificado de firma avanzada.

5.1.8. AUTENTICACIÓN DE LA IDENTIDAD DE LA ORGANIZACIÓN

No Aplica.

5.2. IDENTIFICACIÓN Y AUTENTICACIÓN DE IDENTIDAD DE UN SOLICITANTE

El solicitante que quiera obtener un certificado de firma electrónica avanzada debe presentarse físicamente en las instalaciones de la empresa con su cedula nacional de identidad completando un formulario de solicitud de firma electrónica avanzada, dicha solicitud generará un numero de solicitud la que deberá ser firmada y se estampará la huella dactilar con tinta por el solicitante y se verificará la vigencia de la cedula de identidad ante el Registro Civil. Una vez realizado

correctamente el proceso de verificación fehaciente de identidad, se procederá a registrar los datos de la persona, para que así se genere una solicitud, la que será enviada con la clave pública provista por el usuario a la CA, para que Certificadora del Sur firme y se genere el certificado de firma avanzada. La llave privada será almacenada en un dispositivo criptográfico (token) que cumpla con la normativa técnica vigente a la fecha.

Una vez realizado correctamente el proceso de verificación fehaciente de identidad, el operador de registro procederá a registrar los datos de la persona, y generara una solicitud de creación de certificado avanzado o CSR, en este momento el Titular generará su clave del certificado lo que le permitirá tener el control absoluto de su certificado, esta clave será enviada a la CA, para que la CA firme la solicitud CSR y se genere el certificado de firma avanzada; tanto la llave privada como la llave publica serán almacenadas en un dispositivo criptográfico (Token) que será de propiedad del Titular y sobre el cual tendrá el control absoluto, dicho Token cumple con la normativa técnica vigente a la fecha.

5.3. REKEY O REEMISIÓN DE LLAVES

La autoridad Certificadora no emitirá o re-emitirá llaves para el Titular, así como tampoco renovará certificados por termino de vigencia, debido a que las llaves deben ser generadas por acción del Usuario o Titular.

Para renovar certificados, el titular deberá realizar una nueva solicitud.

5.3.1. REKEY DESPUÉS DE LA REVOCACIÓN

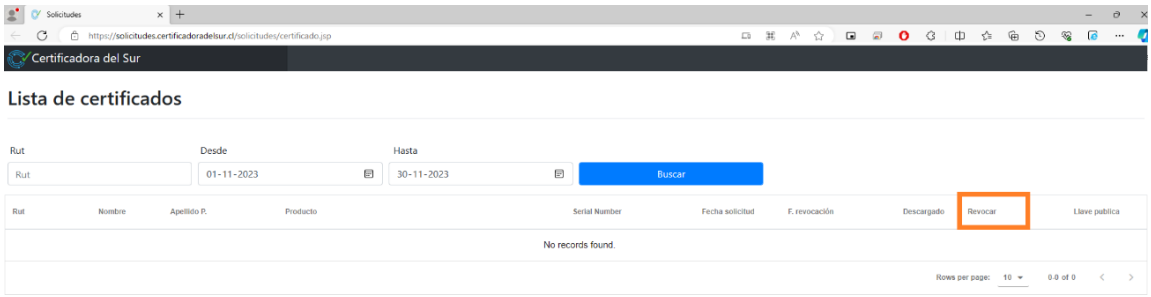
La Autoridad Certificadora no emitirá o reemitirá llaves para el titular luego de una revocación debido a que las llaves deben ser generadas por acción del Usuario o Titular.

5.4. SOLICITUD DE REVOCACIÓN

La solicitud de Revocación de un Certificado de firma electrónica podrá realizarse a través de alguna de las siguientes formas:

- A través de un correo electrónico enviado por el usuario o titular con la solicitud de revocación de Firma Electrónica Avanzada, firmada con su Firma Electrónica Avanzada, al correo revocacion@certificadoradelsur.cl.
- A través del portal de Certificadora del Sur en el siguiente link:

  https://solicitudes.certificadoradelsur.cl/solicitudes/certificado.jsp



- En forma presencial, el usuario o titular deberá hacer la solicitud de revocación en formato físico en las oficinas de Certificadora del Sur; donde se indicará el certificado que requiere revocar, deberá presentarse con su cedula de identidad vigente y deberá estampar su firma y huella en dicha solicitud, una vez acreditada su identidad y la vigencia de su cedula de identidad ante el Registro Civil, se le revocará el certificado en cuestión.

Además, los certificados de Firma Electrónica quedan revocados por:

a) Fallecimiento del titular o disolución de la persona jurídica que represente, en su caso.
b) Resolución judicial ejecutoriada.
c) 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.
d) Que el titular del certificado no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificador.
e) Que el titular del certificado no ha actualizado sus datos al cambiar éstos.
f) Las demás causas que convengan el prestador de servicios de certificación con el titular del certificado.

5.5. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADO

5.5.1. SOLICITUD DE CERTIFICADOS

La solicitud de certificado de firma electrónica avanzada se realizará a través del portal web de la Autoridad Certificadora: www.certificadoradelsur.cl o presencialmente en las oficinas administrativas de la empresa. Para esto, el Solicitante deberá proveer, y luego validar, la siguiente información: nombre completo, apellido paterno y apellido materno y la información del RUT (Rol Único Tributario).

En caso de haber errores en esta información, el Solicitante deberá realizar nuevamente su solicitud.

5.5.2. PROCEDIMIENTO DE REGISTRO DEL SOLICITANTE

Para que la Autoridad Certificadora autorice la emisión de un certificado digital a un solicitante, éste deberá entregar los siguientes antecedentes, para la comprobación fehaciente de su identidad:

1. Identificación del solicitante

   El solicitante deberá presentarse físicamente en las instalaciones de la empresa con su cedula nacional de identidad completando un formulario de solicitud de firma electrónica avanzada, dicha solicitud generará un numero de solicitud la que deberá ser firmada y se estampará la huella dactilar con tinta por el solicitante y se verificará la vigencia de la cedula de identidad ante el Registro Civil, verificando su nombre contra los datos capturados desde la cédula.

2. Ingreso de datos personales

   El segundo paso será el ingreso de los siguientes datos por parte del operador de registro:

   - ✓ RUT
   - ✓ Nombres
   - ✓ Apellido Paterno
   - ✓ Apellido Materno
   - ✓ Correo electrónico
   - ✓ Número de Serie de la cédula de identidad

3. Formulario de Solicitud

El solicitante deberá estampar su firma y huella dactilar con tinta en Formulario de Solicitud de Firma Electrónica Avanzada.

5.5.3. CERTIFICACIÓN DE INFORMACIÓN DE LA SOLICITUD DE CERTIFICADO DE FIRMA ELECTRÓNICA

Una vez que el Solicitante ha ingresado la solicitud de Certificado de Firma Electrónica Avanzada, el respectivo personal de Certificadora del Sur, certificará la siguiente información:

- Información ingresada en la solicitud
- Identidad del solicitante

El personal de Certificadora del Sur, al certificar estos datos firmará electrónicamente la solicitud incorporando la fecha y hora de su aprobación, en el sistema utilizado como Autoridad de Registro, con lo cual se gatillará la aprobación del certificado de firma electrónica avanzada.

5.6. EMISIÓN DE CERTIFICADOS

La Autoridad Certificadora Intermedia emitirá los certificados de firma electrónica una vez que cuente con:

- La aprobación de la AR de Certificadora del Sur
- La llave pública y la llave privada del usuario o titular (que solo es conocida por el usuario o titular).

La CA generara el certificado al Titular quien generara la clave de su certificado de firma electrónica avanzada, teniendo el control absoluto de dicho certificado. También, el Titular generará las credenciales para acceder al dispositivo criptográfico donde se almacenará el certificado.
El certificado se emitirá y almacenará en el dispositivo criptográfico de propiedad del Titular.

Lo anterior gatilla una notificación al usuario o titular para la habilitación de su certificado de firma electrónica avanzada.

5.7. ACEPTACIÓN DE CERTIFICADOS

El certificado se considerará aceptado cuando el solicitante una vez firmado y estampada su huella dactilar con tinta en el Contrato marco de servicios Certificadora del Sur SPA, firma y estampa su huella dactilar con tinta en Formulario Recepción de Certificado de Firma Electrónica Avanzada y recibe de la Autoridad Certificadora Token que contiene la llave pública y la llave privada que el Usuario o Titular dispuso para la creación del Certificado de Firma Electrónica Avanzada a través de su intervención como se menciona en el punto 5.6 Emisión de Certificados.
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 o cualquier tercero que de buena fe confíe en el contenido del Certificado.

5.8. DEBERES Y PROCEDIMIENTOS DE LA PSC

Certificadora del Sur aplicara los siguientes procedimientos para los siguientes casos:

5.8.1. EXPIRACIÓN DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA

Certificadora del Sur establece que la Expiración de la vigencia del Certificado de Firma Electrónica Avanzada ocurre cuando se ha cumplido la fecha de expiración del Certificado de Firma Electrónica Avanzada contenida en el propio certificado.

5.8.2. RENOVACIÓN DE CERTIFICADO DE FIRMA ELECTRÓNICA AVANZADA

El Usuario o Titular podrá solicitar la renovación del certificado digital, siempre y cuando no hubiese expirado el Certificado de Firma Electrónica Avanzada, no se encuentre suspendido y no haya sido revocado.

Para renovar su certificado digital, el Usuario o Titular deberá presentar una nueva solicitud de certificado. Esto lo deberá hacer en forma presencial en las dependencias de Certificadora del Sur.

Para la renovación, Certificadora del Sur podrá solicitar información adicional para comprobar la identidad fehaciente del Usuario o Titular.

En ningún caso la renovación podrá implicar que el certificado digital tenga una duración superior a 3 años.

5.9. SUSPENSIÓN DE CERTIFICADOS

5.9.1. CIRCUNSTANCIAS PARA SUSPENSIÓN

Certificadora del Sur establece que la Suspensión de la vigencia del Certificado de Firma Electrónica Avanzada procede cuando se verifique alguna de las siguientes circunstancias:

a. Solicitud del titular del certificado.

b. Decisión de Certificadora del Sur en virtud de razones técnicas.

5.9.2. QUIEN PUEDE SOLICITAR UNA SUSPENSIÓN

La Suspensión puede ser solicitada por el Usuario o Titular.

5.9.3. PROCEDIMIENTO PARA SOLICITAR LA SUSPENSIÓN

El usuario o titular contará con dos formas de solicitar la suspensión de certificado de Firma Electrónica Avanzada:

1. A través de un correo electrónico el usuario o titular deberá enviar la solicitud de suspensión de Firma Electrónica Avanzada firmado con su Firma Electrónica Avanzada al correo revocacion@certificadoradelsur.cl.
2. En forma presencial, el usuario o titular deberá hacer la solicitud de suspensión en formato físico en las oficinas de Certificadora del Sur; donde se indicará el certificado que requiere suspender, deberá presentarse con su cedula de identidad vigente y deberá estampar su firma y huella en dicha solicitud, una vez acreditada su identidad y la vigencia de su cedula de identidad ante el Registro Civil, se le suspenderá el certificado en cuestión.

Certificadora del Sur declara que el estado suspensión será tratado como una revocación del Certificado de Firma Electrónica Avanzada, y que al momento de anular dicha suspensión se entregará un nuevo Certificado de Firma Electrónica Avanzada que cubra el tiempo restante del Certificado de Firma Electrónica Avanzada suspendido, sin ningún costo asociado para el Titular del Certificado de Firma Electrónica Avanzada.

5.9.4. TÉRMINO DEL PERIODO DE SUSPENSIÓN

Certificadora del Sur establece que la suspensión del Certificado de Firma Electrónica Avanzada terminará por cualquiera de las siguientes causas:

a. Por la decisión de Certificadora del Sur de revocar el certificado, en los casos previstos en la Ley.

b. Por la decisión de Certificadora del Sur de levantar la suspensión del certificado, una vez que cesen las causas técnicas que la originaron.

c. Por la decisión del titular del certificado, cuando la suspensión haya sido solicitada por éste.

Certificadora del Sur declara que el estado suspensión será tratado como una revocación del Certificado de Firma Electrónica Avanzada, y que al momento de anular dicha suspensión se entregará un nuevo Certificado de Firma Electrónica Avanzada que cubra el tiempo restante del Certificado de Firma Electrónica Avanzada suspendido, sin ningún costo asociado para el Titular del Certificado de Firma Electrónica Avanzada.

5.10. CRL

5.10.1. FRECUENCIA DE EMISIÓN DE LA CRL

Las listas de revocación (CRL) de Certificadora del Sur serán actualizadas cada 24 horas y serán publicadas en el repositorio público de certificados de la organización.

https://www.certificadoradelsur.cl/crl/c3.crl

5.10.2. REQUERIMIENTOS DE VERIFICACIÓN DE LA CRL

No Aplica

5.11. OCSP

5.11.1. DISPONIBILIDAD DEL SERVICIO DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA (OCSP)

La información en línea sobre el estado de un certificado, está disponible a través de la web, y el servicio OCSP.

Web:

https://solicitudes.certificadoradelsur.cl/solicitudes/certificado.jsp

OCSP:

https://www.certificadoradelsur.cl/website/documentos/ocsp.pdf

5.11.2. REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

Las terceras partes que confían deben verificar el estado de un certificado de firma electrónica en el cual van a confiar. Esta comprobación puede ser realizada mediante CRL, y en los casos que la CRL no esté disponible, mediante el protocolo OCSP, el cual tiene como único requisito que sebe ser consultado con un cliente compatible con RFC 6960.

5.12. OTRAS FORMAS DE AVISO DE REVOCACIÓN DISPONIBLES

No Aplica.

5.12.1. REQUERIMIENTOS DE OTRAS FORMAS DE VERIFICACIÓN DE REVOCACIÓN

No Aplica.

5.12.2. REQUERIMIENTOS ESPECIALES SOBRE COMPROMISO DE LA LLAVE

No Aplica.

5.13. CAMBIO DE LLAVES

La autoridad certificadora de firma electrónica avanzada no puede emitir un certificado nuevo, con la misma llave pública.

En el caso de compromiso de llaves, están deberán ser revocadas, eliminadas y emitidas nuevamente con sus respectivos nuevos certificados.

Los certificados firmados con las llaves comprometidas en el lapso de compromiso deberán ser revocados e informados a los Titulares de ellos para que se inicie un proceso de emisión de nuevos certificados firmados por la nueva CA.

5.14. COMPROMISO Y RECUPERACIÓN ANTE DESASTRES

La Autoridad Certificadora en caso de un desastre y/o compromiso de la llave privada, deberá reiniciar las operaciones a la mayor brevedad posible. Para esto deberá ejecutar el Plan de Recuperación de Desastres “PS03_Plan de Continuidad de Negocio y Recuperacion ante Desastres _ VF_3.1”, el cual se encuentra debidamente formalizado y versionado.

En las siguientes circunstancias la Autoridad Certificadora podrá dejar de funcionar, hasta haber superado el incidente y tener un análisis del nivel de compromiso de las llaves:

- Intromisión indebida al software de la Autoridad Certificadora
- Detección de intrusos en la red de la Autoridad Certificadora
- Detección de acceso indebido a espacios y/o recursos físicos de la Autoridad Certificadora
- Desastre natural u otro tipo de desastre (por ejemplo, incendio, inundación, etcétera).
- Sospechas fundadas de acceso indebido a las llaves de la autoridad certificadora

En caso de que se produzca un compromiso de la llave privada de la Autoridad Certificadora o una de sus Autoridades Certificados Intermedias, se informará a todos los Usuario o Titulares del evento, de ser necesario se podrá indicar que los certificados de firma electrónica emitidos en el lapso del compromiso de la llave privada ya no son válidos.

En paralelo se deberá generar un nuevo par de llaves y la eliminación de las llaves comprometidas.

5.14.1. RECURSOS COMPUTACIONALES, SOFTWARE O LOS DATOS ESTÁN CORRUPTOS

En caso de incidentes donde los datos o el software se corrompan, o existan fallas a nivel de hardware la Autoridad Certificadora, deberán preparar un informe del incidente, con alto nivel de detalle, donde deberá incluir cuando menos los métodos de respuesta al incidente de seguridad, y las medidas de mitigación que serán aplicadas para que este tipo de eventos no se vuelva a repetir.

5.14.2. REVOCACIÓN DE LA LLAVE PÚBLICA DE LA ENTIDAD

En el caso de un compromiso de la llave privada de la Autoridad Certificadora Raíz, la CA será revocada.

5.14.3. LA LLAVE DE LA ENTIDAD ESTÁ COMPROMETIDA

En el caso de un compromiso de la llave privada de la Autoridad Certificadora Raíz, o una de sus Autoridades Certificadoras Intermedias, la Autoridad Certificadora comprometida será revocada.

5.14.4. INSTALACIONES DE SEGURIDAD DESPUÉS DE UN DESASTRE NATURAL, O DE OTRO TIPO

En caso de desastre natural o provocado por el hombre, la Autoridad Certificadora y Autoridad de Registro deben implementar planes de recuperación de desastres. Para mayores detalles, revisar documento Plan de Recuperación de Desastres (DRP) “PS03_Plan de Continuidad de Negocio y Recuperacion ante Desastres _ VF_3.1”.

5.15. TÉRMINO DE LA AUTORIDAD CERTIFICADORA

Respecto al Termino de la Autoridad Certificadora, Certificadora del Sur acatara lo pertinente que está establecido en el Artículo 12 de la Ley 19.799.- “Son obligaciones del prestador de servicios de certificación de firma electrónica”:

c) 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;

g) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que dará a los datos de los certificados, especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;

h) En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere;

i) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento concursal de liquidación o que se encuentre en cesación de pagos, y

j) Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada.

Además, se considerará lo establecido en el Decreto N.181, en especial los siguientes artículos:

Artículo 8º. En caso que un prestador de servicios de certificación cese en la prestación del servicio, deberá comunicar tal situación a los titulares de los certificados por ella emitidos en la siguiente forma:

a) Si el cese es voluntario, con una antelación de a lo menos dos meses y señalando al titular que de no existir objeción a la transferencia de los certificados a otro prestador de servicios de certificación, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos. En este caso, si el prestador es acreditado, deberá traspasar los certificados, necesariamente, a un certificador acreditado.

b) Si el cese no es voluntario, la cancelación de la acreditación deberá comunicarse inmediatamente a los titulares. En caso que el prestador de servicios de certificación esté en situación de traspasar los certificados a otro prestador acreditado, deberá informar tal situación en la forma y plazo señalado en la letra a).

Si el titular del certificado se opone a la transferencia, el certificado quedará sin efecto sin más trámite, sin perjuicio de lo dispuesto en el artículo 11 de este Reglamento.

Artículo 9º. En caso que el cese en la prestación del servicio sea por voluntad del prestador acreditado de servicios de certificación, deberá solicitar a la Entidad Acreditadora, con al menos un mes de anticipación, la cancelación de su inscripción en el registro público a que hace referencia el artículo 16 de este Reglamento, comunicándole el destino que dará a los datos de los certificados, especificando, en su caso, los que va a transferir y a quién, cuando proceda.

Artículo 11. Los datos proporcionados por el titular del certificado deberán ser conservados por el prestador de servicios de certificación a lo menos durante seis años desde la emisión inicial de los certificados, cualquiera sea el estado en que se encuentre el certificado.

En caso que el prestador de servicios de certificación cese en su actividad, deberá transferir dichos datos a un prestador de servicios de certificación, que deberá estar acreditado si aquel lo fuera, o a una empresa especializada en la custodia de datos electrónicos, por el tiempo faltante para completar los 6 años desde la emisión de cada certificado. Esta situación deberá verse reflejada en el registro público que señala el artículo 16 de este Reglamento.

Certificadora del Sur, de buena fe, harán los esfuerzos comercialmente razonables para ponerse de acuerdo sobre un plan de terminación que minimice la interrupción de servicio a los Usuario o Titulares y terceros que confían.

- El plan de término puede cubrir temas tales como:
    - La notificación a las partes afectadas por la terminación, tales como Usuario o Titulares y Terceros que Confían
    - La preservación de los archivos de la CA y los registros para los plazos exigidos en la presente declaración
    - La continuación de los servicios de soporte a Usuario o Titulares y terceros que confían
    - La continuación de los servicios de revocación, tales como la emisión de la CRL o el mantenimiento de los servicios en línea de verificación de estado
    - La revocación de Certificados no vencidos sin revocar, de Usuario o Titulares y de CAs subordinadas, si es necesario
    - El reembolso (si es necesario) a los Usuario o Titulares cuyos certificados no expirados, ni revocados se revocan durante el plan de terminación o la disposición, para la emisión de los Certificados de reemplazo a través de CAs sucesoras
    - Disposición de la llave privada de la CA y el token de hardware que contiene dicha llave privada
    - Disposiciones necesarias para la transición de los servicios de la CA a una CA sucesora

6. POLÍTICA Y CONTROLES DE SEGURIDAD

Certificadora del Sur cuenta con una Política General de Seguridad de la Información, la que tiene por objeto proporcionar dirección y apoyo a la gestión de la seguridad de la información de la organización, entendida como la preservación de la confidencialidad, integridad y disponibilidad de la información.

A través de ese documento, la dirección superior de la organización establece una dirección política clara, en consonancia con sus objetivos comerciales y demuestra apoyo y compromiso con la seguridad de la información mediante la emisión y mantenimiento de esta política de seguridad de la información en toda la organización, así como define los responsables de la mantención y supervisión de la seguridad en la organización, y de reaccionar en caso de compromiso.

La gestión de la seguridad de la información tiene como requerimientos los definidos en el estándar ISO IEC 27001:2013 para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), además de los requisitos legales a cumplir en términos de la legislación vigente, normas y contractuales relativos a la seguridad de la información que sean aplicables a Certificadora del Sur.

Para asegurar el cumplimiento a los objetivos y requerimientos, la organización define Planes de Seguridad específicos para los aspectos fundamentales de Seguridad de la Información:

1. Seguridad del Personal

2. Seguridad de Sistemas de Información

3. Seguridad en las Comunicaciones (Plan de Seguridad Telecomunicaciones)

4. Administración de los Controles Ambientales (Plan de Seguridad Físico)

5. Administración de la Continuidad Operativa (Plan de Continuidad de Negocios y Recuperación ante desastres)

6. Administración del Riesgo (Matriz de Riesgos y Amenazas)

Por su parte, los controles de seguridad tienen por objeto preservar la confidencialidad, integridad y disponibilidad de la información.

La seguridad de las operaciones de la CA y de la Autoridad de Registro son la base de la confianza en los certificados digitales emitidos, siendo el objetivo reducir a la mínima expresión los riesgos que amenazan a los activos de información que gestiona la organización.

6.1. CONTROLES DE SEGURIDAD UTILIZADOS POR EL PSC

6.1.1. CONTROLES FÍSICOS DE SEGURIDAD

La Autoridad Certificadora, para la prestación de sus servicios, considera controles de seguridad físicos, tanto para los accesos a las oficinas administrativas, como para el acceso a data centers externos.

Los antecedentes específicos de seguridad son reservados, por motivos de seguridad, y se encuentran detallados en una Política de Seguridad Física de la organización, siendo auditados anualmente.

6.1.1.1. ÁREAS DE REGISTRO Y ENROLAMIENTO DE PERSONAS

La Autoridad Certificadora dispone de dependencias en las cuales los solicitantes de firma electrónica avanzada podrán comprobar presencialmente su identidad, la que se verificará fehacientemente utilizando su cédula nacional de identidad, el operador de registro verificará la vigencia de la cedula de identidad ante el Registro Civil. Esta área de registro y enrolamiento se encuentra en las oficinas administrativas de la empresa, la que dispone de elementos físicos y tecnológicos para que los solicitantes puedan validar su identidad y solicitar una firma electrónica avanzada.

6.1.1.2. ELIMINACIÓN DE RESIDUOS

La disposición final de los residuos se realiza en una empresa o lugar que cuente con las autorizaciones (permisos) sectoriales respectivos.

En el caso de medios físicos que contengan información, ésta es eliminada en forma previa a su disposición final, o inutilizados los medios físicos.

6.1.2. SEGURIDAD DEL DATA CENTER

El Data Center donde opera la Autoridad Certificadora sigue estándares internacionales establecidos por el UPTIME INSTITUTE que aseguran un adecuado funcionamiento de los equipos informativos albergados.

Las dependencias del data center contemplan:

- Sala de Servidores
- Sala de Comunicaciones
- Sala de Enlaces Externos
- Laboratorio de ensamble
- Cintoteca
- Sala de Operadores
- Sala Eléctrica y UPS
- Sala de Baterías
- Sala de tableros
- Subestación eléctrica
- Sala de grupos generadores
- Instalación de equipos exteriores: Unidades exteriores de clima (Chillers).

Algunas características con las que cuenta el Datacenter principal son las siguientes, respecto de la seguridad física:

- Sistema de control y registro de accesos
- Seguridad de acceso especial con guardia 7x24
- Sistemas de detección inteligente (Biometría)
- Ingreso de visitantes solo acompañados por personal de la empresa
- Puertas cortafuegos, F-60
- Sistema automático de audio evacuación
- Circuito cerrado de televisión con cámaras en todas las áreas de circulación

6.1.2.1. SISTEMA DE ENERGÍA ELÉCTRICA

El sistema de energía eléctrica se compone por

- 2 grupos generadores de 480 HP
- Capacidad de generación de 410 KVA, cada uno.
- Aplicación de uso continuo y respaldo
- Mantenimiento preventivo bimensual, pruebas de funcionamiento semanal

- Tiempo de toma de carga de 10 segundos.

El sistema es alimentado por un sistema de tanque de combustible diésel con capacidad para 18.00 litros, y autonomía de 5 días continuos para ambos generadores.

Adicionalmente se cuenta con un sistema de UPS, marca Emerson, las cuales cuentan con las siguientes características:

- Marca Emerson
- Modelo: NXr
- Capacidad: 120 KVA
- Banco de Batería: 40 baterias 12V/110Ah
- Autonomía: 40 minutos a plena carga

6.1.2.2. SISTEMA DE CLIMATIZACIÓN Y EXPOSICIÓN AL AGUA

El datacenter donde se realiza la emisión y gestión de los certificados de firma electrónica cuenta con sistema de climatización y de manejo de temperatura, exposición al agua y humedad inteligente.

El sistema contempla dos equipos condensadores HCR43 por unidad para enfriamiento ubicados en la azotea del edificio.

6.1.2.3. SISTEMA DE EXTINCIÓN Y CONTROL DE INCENDIOS

El datacenter cuenta con un sistema de detección inteligente de incendios, que permite una respuesta rápida y efectiva. Cuenta con un detector FirePrint que es capaz de diferenciar entre condiciones de falsa alarma y fuego genuino.

El sistema supresor utilizado es un FM200, el cual es un agente químico gaseoso, el cual es un sistema que no daña los equipos y es seguro para las personas al actuar rápidamente con una descarga en menos de 10 segundos.

6.1.2.4. SEGURIDAD LÓGICA DEL DATACENTER

La Instalación de la Autoridad Certificadora cuenta con sistemas de Firewall y detección de intrusos.

6.1.3. SEGURIDAD DEL DISPOSITIVO CRIPTOGRÁFICO HSM

El módulo criptográfico HSM, en el cual están almacenadas las llaves privadas, se encuentra custodiado en el datacenter de la PSC, la cual considera controles de seguridad físicos, lógicos y de telecomunicaciones. Los antecedentes específicos de seguridad son reservados, por motivos de seguridad, y se encuentran detallados en una Política de Seguridad Física de la organización, siendo auditados anualmente.

6.2. CONTROLES DE PROCEDIMIENTOS

Los procedimientos establecidos por la Autoridad Certificadora operan de forma segura y siguiendo instrucciones formalizadas a través de prácticas, procedimientos y manuales divulgados al personal que corresponda.

6.3. ROLES DE CONFIANZA

Certificadora del Sur cuenta con una matriz de segregación de funciones según las restricciones de seguridad definidas en la Política General de Seguridad y en la respectiva Política de Seguridad del Personal

6.3.1. CANTIDAD DE PERSONAS REQUERIDAS POR TAREA

El número mínimo de partes separadas necesarias para respaldar o recuperar el respaldo de una llave privada de la Autoridad Certificadora Raíz son 2.

El número mínimo de partes separadas necesarias para respaldar o recuperar el respaldo de una llave privada de la Autoridad Certificadora Intermedia son 2.

El número de partes distribuidas para llaves de recuperación de desastres puede ser menor que el número distribuido para llaves operacionales, mientras que el número de partes necesarias sigue siendo igual.

6.3.2. IDENTIFICACIÓN Y AUTENTICACIÓN DE CADA ROL

Certificadora del Sur cuenta con una matriz de segregación de funciones según las restricciones de seguridad definidas en la Política General de Seguridad.

6.4. CONTROLES DEL PERSONAL

La Autoridad Certificadora cuenta con personal que posee el conocimiento especializado para el funcionamiento apropiado de la Autoridad Certificadora, y soporten adecuadamente la confiabilidad de las operaciones.

6.4.1. REQUERIMIENTOS DE ANTECEDENTES Y CONOCIMIENTOS

El personal de confianza de la Autoridad Certificadora cuenta con conocimientos acorde a los servicios que se prestan, en especial los siguientes puntos:

- Conocimientos sobre Infraestructura de Llaves Publicas
- Título académico acorde a los servicios que presta la Autoridad Certificadora o experiencia demostrable en el ámbito de la emisión y uso de Certificados Digitales.
- Conocimientos de las políticas y procedimientos de la Autoridad Certificadora
- Competencias específicas para el desarrollo de su puesto
- Conocimientos relacionados a la Seguridad de la Información

6.4.2. PROCEDIMIENTO DE VERIFICACIÓN DE ANTECEDENTES

Los antecedentes del personal se validan en el momento de su contratación a través de entrevistas, certificados originales o copias notariales, y la experiencia previa demostrable.

6.4.3. REQUISITOS DE CAPACITACIÓN Y ENTRENAMIENTO

El personal de la Autoridad Certificadora cuenta con capacitaciones para la ejecución de sus funciones, en especial:

- Entrenamiento básico de infraestructura de llaves públicas (PKI)
- Entrenamiento en el uso de software y hardware criptográfico utilizado por la Autoridad Certificadora
- Introducción a la ejecución de sus tareas
- Capacitación y el entrenamiento en seguridad de la información

6.4.4. FRECUENCIA Y REQUERIMIENTOS DE REENTRENAMIENTO

La Autoridad Certificadora determinará, en función de cambios tecnológicos y de seguridad, la frecuencia en la que se impartirá el entrenamiento para los colaboradores, de tal forma que estos puedan llevar a cabo sus funciones de manera competente.

6.4.5. FRECUENCIA Y SECUENCIA DE LA ROTACIÓN DE LOS TRABAJOS

No Aplica.

6.4.6. SANCIONES POR ACCIONES NO AUTORIZADAS

Se determinará caso a caso según la gravedad de las acciones. Es deber de la jefatura directa, y del Gerente General de Certificadora del Sur, determinar las sanciones, que además podrán estar establecidas por contrato.

6.4.7. REQUERIMIENTOS DE PERSONAL CONTRATISTA

Certificadora del Sur puede contratar servicios de consultores independientes, o contratistas, habilitándolos para que realicen funciones para la Autoridad Certificadora o de Registro. Todos los contratistas y consultores independientes firmaran un Acuerdo de Confidencialidad y No Divulgación con Certificadora del Sur.

6.4.8. DOCUMENTACIÓN SUMINISTRADA POR EL PERSONAL

La documentación que deberá proporcionar el colaborador serán las que se especifiquen en la Política de Seguridad del Personal.

6.4.9. FINALIZACIÓN DEL CONTRATO

El departamento de Recursos Humanos deberá aplicar los procedimientos generales establecidos para la desvinculación de un trabajador de la Autoridad Certificadora, en especial procederá:

- Solicitar que se supriman los privilegios y accesos a componentes de software y hardware de la Autoridad Certificadora.
- Recuperar elementos que están en custodia del personal desvinculado, como:
  - Claves de acceso
  - Ped Keys
  - Equipos computacionales
  - Etcétera.
- Informar al resto de la organización de la desvinculación del personal, y a proveedores externos en caso de que aplique.
- En el caso de que el funcionario desvinculado compartiera una clave de acceso a elementos de la Autoridad Certificadora, por ejemplo, Ped Key, esta clave deberá ser cambiada según los procedimientos del caso.

6.5. CONTROLES TÉCNICOS DE SEGURIDAD

La Autoridad Certificadora contará con procedimientos y controles para garantizar la seguridad en la emisión de un certificado de firma electrónica, en especial los aspectos relacionados con la generación de llaves de sus certificados raíz e intermedias.

6.5.1. GENERACIÓN E INSTALACIÓN DEL PAR DE LLAVES

6.5.1.1. GENERACIÓN DEL PAR DE LLAVES

Todo par de llaves para los componentes de la Autoridad Certificadora (Certificados Raíz, Raíces Subordinadas, firma de CRL, entre otros) serán generadas en hardware criptográfico con certificación FIPS 140-2 Level 3, al menos.

La creación de llaves de la Autoridad Certificadora Raíz y de Firma Electrónica Avanzada deberán ser realizadas a través de una Ceremonia de Llaves que sigue un protocolo bien establecido y con presencia de testigos externos a la Autoridad Certificadora.

La creación de las llaves del Titular deberá ser generada con la intervención del mismo usuario tomando el control de acceso de ellas.

6.5.1.2. ENTREGA DE LLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

La llave pública del titular se entregará al emisor del certificado a través de la solicitud de certificado firmada con su propia llave privada.

Así también podrán entregar la llave pública del titular las aplicaciones registradas como de confianza ante la Autoridad Certificadora y que consuman de forma segura las interfaces de programación (API) expuestas para este propósito, en caso que existan.

6.5.1.3. ENTREGA DE LLAVE PÚBLICA DE CA A USUARIOS

La llave pública de la Autoridad Certificadora se entregará al usuario a través de la cadena de certificados que contiene el certificado de firma electrónica del titular o podrá ser obtenida a través de la descarga de los certificados raíces publicados por la Autoridad Certificadora.

6.5.1.4. TAMAÑOS LLAVE

Todas las llaves serán iguales o superiores a 2048 bits, del tipo RSA (Sha256).

6.5.1.5. GENERACIÓN DE PARÁMETROS DE LLAVE PÚBLICA

Las llaves de la Autoridad Certificadora Raíz y Autoridad Certificadora de Firma Electrónica Avanzada se generan en HSM a través de un protocolo bien establecido y con testigos externos a la Autoridad Certificadora.

6.5.1.6. CONTROL DE CALIDAD DE PARÁMETROS

El identificador de algoritmo para firmar los certificados de firma electrónica será SHA256 with RSA (OID: 1.3.6.1.4.1.55784).

No se utilizarán llaves con RSA con SHA1, por considerarse un protocolo inseguro.

6.5.1.7. GENERACIÓN DE LLAVES DE HARDWARE / SOFTWARE

La Autoridad Certificadora generará sus llaves en HSM (Hardware Security Modules) que cumplen con la norma FIPS 140-2 Level 3, o superior.

Los titulares generarán sus llaves en el dispositivo de seguridad para el usuario, los cuales deberán cumplir la norma FIPS 140-2 Level 2 o superior, en el caso de los certificados de firma electrónica avanzada.

6.5.1.8. PROPÓSITOS DE USO DE LLAVES (SEGÚN EL CAMPO DE USO DE LLAVES X.509 V3)

Los certificados emitidos por la Autoridad Certificadora de Firma Electrónica tendrán la extensión KEY USAGE para definir el uso de las llaves, en especial para el uso de firma electrónica de documentos y el cifrado de ellos. Para esto en el certificado X509 se definirán los siguientes valores de la extensión anteriormente referenciada:

X509v3 Key Usage (1.3.6.1.4.1.55784)

Digital Signature, Non Repudiation, Key Encipherment

6.5.2. PROTECCIÓN DE LLAVE PRIVADA

6.5.2.1. ESTÁNDARES PARA EL MÓDULO CRIPTOGRÁFICO

Se utilizarán dispositivos denominados HSM (Hardware Security Module) que cumplen con la norma FIPS 140-2 Level 3 de la marca Utimaco, y el modelo CryptoServer.

6.5.2.2. CONTROL PRIVADO DE LLAVE PRIVADA (N FUERA DE M)

Las claves para la activación del dominio de clonación y acceso a las particiones de la Autoridad Certificadora Raíz y Autoridad Certificadora Intermedia, serán de control dual donde a lo menos se necesitarán dos personas para activar las claves privadas de la Autoridad Certificadora Raíz e Intermedia.

6.5.2.3. CUSTODIA DE LLAVE PRIVADA

Las claves para la activación del dominio de clonación y acceso a las particiones de la Autoridad Certificadora Raíz y Autoridad Certificadora Intermedia serán generadas en los HSMs, siguiendo un estricto protocolo efectuado con testigos externos, y funcionarios de confianza de Certificadora del Sur.

6.5.2.4. COPIA DE SEGURIDAD DE LLAVE PRIVADA DE LA CA

Certificadora del Sur debe mantener copias de seguridad de sus propias llaves privadas, la CA no mantiene copia de seguridad de los certificados de titulares, con el propósito de recuperarse en caso de desastres y daños en el equipamiento, las cuales deben ser almacenadas en instalaciones diferentes al DataCenter, pero con controles de seguridad físicos y lógicos similares a los del DataCenter.

Las copias de seguridad deben contar con medios de protección físicos y de cifrado, igual o superior, a la de los módulos criptográficos en el site principal.

6.5.2.5. ARCHIVO DE LLAVE PRIVADA

Después que se cumpla la vida útil de validez de un certificado de autoridad certificadora intermedia, el par de llaves asociado será almacenado y archivado de forma segura por periodo de al menos 6 años, utilizando módulos criptográficos que cumplan con la norma Fips 140-2 Level 3.

6.5.2.6. ALMACENAMIENTO DE LLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Se establecen mecanismos de seguridad, que aseguren que la transferencia de una llave privada a un módulo criptográfico no tendrá efectos de revelación no autorizada, modificación, robo, copia, perdida de dicha llave privada.

6.5.2.7. ALMACENAMIENTO DE INFORMACIÓN RELEVANTE

Certificadora del Sur almacenará la información relevante, esto es la obtenida dentro de los procesos de emisión, suspensión, revocación y renovación de los certificados digitales.

La información relevante obtenida como producto de los citados procesos será tratada como información confidencial y protegida con medios físicos y lógicos, y la comunicación interna de dicha información es realizada mediante conexiones seguras. Sólo tiene acceso a esta información personal autorizado de la organización. Los documentos que describen los controles de seguridad no técnicos (es decir, controles físicos, de procedimiento y de personal) utilizados por la organización para realizar de forma segura las funciones de archivo, protección y auditoría de la seguridad de la información se mantienen reservados, y su cumplimiento es auditado al menos de forma anual. No obstante lo señalado anteriormente, la información del solicitante contenida en el certificado digital será considerada pública.

6.5.2.8. MÉTODO DE ACTIVACIÓN DE LLAVE PRIVADA

Se deberán establecer mecanismos de seguridad, que aseguren que la activación de una llave privada en un módulo criptográfico no tendrá efectos de revelación no autorizada, modificación, robo, copia, perdida de dicha llave privada.

6.5.2.9. MÉTODO DE DESACTIVACIÓN DE LLAVE PRIVADA

La llave privada raíz de la Autoridad Certificadora, deberá mantenerse desactivada a nivel del HSM, ya que esta llave solo se utilizará para firmar certificados intermedios de la Autoridad Certificadora.

6.5.2.10. MÉTODO DE DESTRUCCIÓN DE LLAVE PRIVADA

Antes de destruir una llave privada, es necesario desactivarla. Para borrarla se utilizan las herramientas de gestión del módulo criptográfico donde esta almacenada, teniendo la precaución de que este procedimiento asegure que no hay restos de la llave privada que pudieran permitir la reconstrucción de la llave privada, y que este procedimiento no afecte la funcionalidad de otras llaves privadas que pudieran estar contenidas en este módulo criptográfico.

6.5.3. OTROS ASPECTOS DE LA GESTIÓN DE PARES DE LLAVES

6.5.3.1. ARCHIVO DE LLAVE PÚBLICA

Certificadora del Sur archivará sus propias llaves públicas, así como las de las CA subordinadas, según lo especificado en la sección 3.2.9 Archivo de Registros de esta Declaración de Practicas de Certificación.

6.5.3.2. PERÍODOS DE USO DE LAS LLAVES PÚBLICAS Y PRIVADAS.

Las llaves privadas y públicas no serán utilizadas para ningún propósito de firma después de la fecha en que expira el certificado de autoridad certificadora intermedia y CA Root al cual están asociadas.

6.5.3.3. GENERACIÓN E INSTALACIÓN DE DATOS DE ACTIVACIÓN

Los custodios de llaves de protección de las llaves privadas de la CA, previamente designados por la Autoridad Certificadora, tienen la obligación de no divulgar sus claves, exponerlas, compartirlas por ningún medio de transmisión física ni electrónica.

6.6. CONTROLES DE SEGURIDAD INFORMÁTICA

Requisitos técnicos específicos de seguridad informática

Certificadora del Sur cuenta con un Plan de Seguridad de la Información, el cual contempla controles de seguridad, recuperación de desastres y controles de acceso.

6.6.1. CONTROLES DE SEGURIDAD DE RED

Certificadora del Sur cuenta con un Plan de Seguridad de Red, el cual contempla controles de acceso exclusivo, otorgando acceso a la red a Servidores y personal autorizados y certificados por la empresa.

6.6.2. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

Certificadora del Sur cuenta con módulos criptográficos certificados bajo la norma FIPS 140-2 Level 3, o superior.

Para mayores detalles se debe revisar la certificación número 1694 del National Instute of Standards and Technology (NIST) de los Estados Unidos, en conjunto con Computer Security División and the Communications Security Establishment del Gobierno Canadiense.

7. PERFILES DE CERTIFICADO Y CRL

7.1. PERFIL DE CERTIFICADO

Un certificado de firma electrónica emitido por la Autoridad Certificadora contendrá como mínimo la siguiente información:

- Un código de identificación único del certificado

- Identificación de la Autoridad Certificadora
- El nombre completo del titular
- Rol Único Tributario del Titular
- Rol Único Tributario de la Autoridad Certificadora
- Email del Titular
- Identificación de la Política de Certificados
- Identificación de la CRL
- Uso de las llaves
- Vigencia del Certificado
- Llave Publica

Los certificados corresponden al estándar X.509 v3, a continuación, un ejemplo de la información que podrá tener un certificado de Firma Electrónica Avanzada:

certificadora del sur
Private RSA Key
Strength: 2048 bits

certificadora del sur
Identity: Jose Cristian Echeverria Briones
Verified by: Firma Electronica Avanzada Certificadora del Sur
Expires: 03/07/23
Subject Name
C (Country): CL
O (Organization): Certificadora del Sur
OU (Organizational Unit): IT
initials (Initials): 11960129-0
CN (Common Name): Jose Cristian Echeverria Briones
EMAIL (Email Address): cecheverria@byeconta.cl
Issuer Name
C (Country): CL
O (Organization): Certificadora del Sur
OU (Organizational Unit): Terminos de Uso en https://www.certificadoradelsur.cl
CN (Common Name): Firma Electronica Avanzada Certificadora del Sur
Issued Certificate
Version: 3
Serial Number: 19 E3 C1 72 21 E0 EF DF
Not Valid Before: 2020-07-03
Not Valid After: 2023-07-03
Certificate Fingerprints
SHA1: 89 EB 0C DA 89 F9 8F F1 72 4A BF FF B0 79 25 9C 85 11 1C 6C
MD5: 8E 50 18 A5 6C 41 CD 3A 89 FE 65 2B 79 6B 8C F0

Public Key Info
Key Algorithm: RSA
Key Parameters: 05 00
Key Size: 2048
Key SHA1 Fingerprint: B4 1E 96 96 5B AB EA D1 3B 71 D9 23 DB FD 79 D3 8D 16 DB CD
Public Key: 30 82 01 0A 02 82 01 01 00 83 F7 7F F2 28 06 86 FA 19 33 06 EF 38 01 BF E9 58 76 A7 9D 41 EA CB 8C A7 1E 02 CD 37 1E 04 FA 95 13 14 49 44 16 D1 30 B5 FA 75 75 E0 08 7C 63 4C 53 F3 C1 53 63 F0 A1 1D 2E 17 7A 08 94 53 BA E5 B3 29 63 DC 20 7C E6 2F 52 D0 69 F5 43 8B 98 E9 9E 66 3A 63 DA F8 DE 49 93 2C 94 82 CD 8C 09 2C 3B 67 62 3F 06 5D A0 BA BE 3A 69 01 E9 51 CA 2B 81 EF 5F 1C 31 D7 56 1C 38 0C B5 1F F1 99 7F DF 59 B3 C9 BD D0 F1 DB 88 BD 6E 8B 6F 34 6E 22 20 55 D7 78 6B C2 AC 77 FB 4C 70 39 98 21 6C B4 45 E5 9E D6 AD 85 9D C9 53 83 1A 8D 01 AB 10 1A D9 4F EF 9C B0 19 1A 01 1C FC 77 57 34 8E 8B 9B FA 0E 7D 1F 58 3A 93 EC 40 32 E7 10 C8 AD 27 97 10 BE D4 88 FB EE 0F 95 E1 25 8F 82 FF 10 71 0C 74 F2 12 A9 6E 51 D4 71 F9 FF 6C 86 87 41 98 4E 19 FA A0 C3 FB 30 BA 21 45 E6 3A 36 2C BF 28 A3 02 03 01 00 01
Extension
Identifier: 1.3.6.1.5.5.7.1.1
Value: 30 31 30 2F 06 08 2B 06 01 05 05 07 30 01 86 23 68 74 74 70 73 3A 2F 2F 6F 63 73 70 2E 63 65 72 74 69 66 69 63 61 64 6F 72 61 64 65 6C 73 75 72 2E 63 6C
Critical: No
Subject Key Identifier
Key Identifier: 62 A9 70 EF 0D 87 BB AF 5D 8B DE A0 78 63 22 95 D3 F2 49 06
Critical: No
Basic Constraints
Certificate Authority: No
Max Path Length: Unlimited
Critical: Yes
Extension
Identifier: 2.5.29.35
Value: 30 16 80 14 74 E6 1F DF BC 18 07 94 E6 26 CD 97 E8 DF FB 20 6A 77 97 5C
Critical: No
Extension
Identifier: 2.5.29.32
Value: 30 81 E3 30 81 80 06 0C 2B 06 01 04 01 83 99 71 01 04 01 03 30 70 30 6E 06 08 2B 06 01 05 05 07 02 02 30 62 1E 60 00 68 00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00 77 00 77 00 77 00 2E 00 63 00 65 00 72 00 74 00 69 00 66 00 69 00 63 00 61 00 64 00 6F 00 72 00 61 00 64 00 65 00 6C 00 73 00 75 00 72 00 2E 00 63 00 6C 00 2F 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 61 00 63 00 69 00 6F 00 6E 30 0E 06 0C 2B 06 01 04 01 83 99 71 01 04 01 02 30 4E 06 0C 2B 06 01 04 01 83 99 71 01 04 01 04 30 3E 30 3C 06 08 2B 06 01 05 05 07 02 01 16 30 68 74 74 70 73 3A 2F 2F 77 77 77 2E 63 65 72 74 69 66 69 63 61 64 6F 72 61

64 65 6C 73 75 72 2E 63 6C 2F 64 6F 63 75 6D 65 6E 74 61 63 69 6F 6E

Critical: No

Extension

Identifier: 2.5.29.31

Value: 30 30 30 2E A0 2C A0 2A 86 28 68 74 74 70 3A 2F 2F 77 77 77 2E 63 65 72 74 69 66 69 63 61 64 6F 72 61 64 65 6C 73 75 72 2E 63 6C 2F 63 32 2E 63 72 6C

Critical: No

Key Usage

Usages: Digital signature Key encipherment

Critical: Yes

Extended Key Usage

Allowed Purposes: Client Authentication Email Protection

Critical: No

Subject Alternative Names

Other Name: 1.3.6.1.4.1.8321.1=30 0c 0c 0a 31 33 38 34 35 32 38 30 2d 38

Critical: No

Signature

Signature Algorithm: 1.2.840.113549.1.1.11

Signature Parameters: 05 00

Signature: 4B E4 3F F1 E8 03 30 06 E1 60 88 C2 33 25 63 B0 B6 11 81 70 92 C0 6A E4 19 24 9C 13 99 FD AF 6E DB 73 D6 63 C1 D5 51 35 BE 1A CF 28 B3 13 B3 12 16 1D 89 B2 73 88 1C 94 5E 1F FB 03 C4 68 59 E3 EE 2B 89 00 67 D8 9E 6E 05 79 68 E7 26 E0 4F 4E 26 F0 4D 39 8A DE 5E 16 3A B6 15 0D 04 5B 55 74 F7 F1 88 2B 5F 5D 9E E3 0B F8 E5 BC 3F 0A 78 9B 25 8B 83 94 47 A7 EE 55 56 EF A9 4E 01 7C CE 8F 9E BF C9 30 DB F3 83 8E 8C 06 A0 19 D4 1B 97 1F 88 63 BE 47 75 2D 9D 84 2B B1 53 E4 90 02 0A 81 7A 0C 8D 8E 99 D1 00 F4 FD CD CB A7 CA 1B 03 F5 BB 61 A8 52 27 61 F6 C6 53 61 9F 58 D2 01 9F 7F 20 8A 07 CC BE F4 2E 4B E4 E5 FB B5 45 82 27 21 2B 56 AD F2 F4 9F DF 77 E3 BB 1C 8F 93 CA 53 CE 5F 31 36 47 36 1E 45 2B BD 25 18 79 67 BB 5D 2C 72 B9 E7 69 8E 0C AF 5E D6 86 DB C4 D2 CB 7C 17

7.1.1. NÚMERO (S) DE VERSIÓN

Los Certificados corresponden al estándar X.509 V3.

7.1.2. USO DE LA EXTENSIÓN DE POLÍTICA DE CERTIFICADO

Este campo se completa con el identificador de esta CPS, según lo que indica el estándar X.509 v3, y se establece en Falso.

7.2. PERFIL DE CRL

Las listas de revocación se actualizarán cada 24 horas y se encontraran disponibles en el sitio web www.certificadoradelsur.cl, cada certificado de firma electrónica avanzada tendrá la URL de acceso a su lista de revocación.

Versión	V2
Emisor	CN = FIRMA ELECTRONICA AVANZADA CERTIFICADORA DEL SUR OU = TERMINOS DE USO EN HTTPS://WWW.CERTIFICADORADELSUR.CL O = CERTIFICADORA DEL SUR C = CL
Fecha Efectiva	lunes, 20 de julio de 2020 17:41:25
Próxima Actualización	martes, 21 de julio de 2020 17:41:25
Algoritmo de Firma	sha256RSA
Algoritmo Hash de Firma	sha256
Identificador de Llave de Entidad Emisora	Id. de clave=74e61fdfbc180794e626cd97e8dffb206a77975c
Número CRL	Número CRL=02
Huella Digital	3c653ab5c110cb9db2476c415811940cb33924d0

7.2.1. NÚMERO (S) DE VERSIÓN

La CRL corresponde al estándar X.509 V2.

7.2.2. CRL Y EXTENSIONES DE ENTRADA DE CRL

No Aplica.

7.2.3. SERVICIO EN LÍNEA DE ESTADO DE CERTIFICADO (OCSP)

Certificadora del Sur contará con un servicio OCSP en la URL:

- Certificados de Firma Avanzada: https://ocsp.certificadoradelsur.cl

8. ADMINISTRACIÓN DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

8.1. PROCEDIMIENTOS DE GESTIÓN DEL CAMBIO

Las prácticas contenidas en este documento serán mantenidas por el personal de Certificadora del Sur, o un tercero delegado por la Autoridad Certificadora. Cualquier cambio sobre la versión base deberá ser aprobada por el Gerente General de Certificadora del Sur, considerando las observaciones que pudiera realizar el Oficial de Seguridad de la Información.

8.2. POLÍTICAS DE PUBLICACIÓN Y NOTIFICACIÓN

El presente documento contiene una sección de controles de versión, en esta sección solo se mencionan los cambios de línea base, así también se publicará la nueva Declaración de Prácticas de Certificación en el sitio web

https://www.certificadoradelsur.cl/website/acuerdoterceros.jsp y se mantendrá la versión anterior por un periodo de tiempo no inferior a 30 días, el que también puede ser accesado en el siguiente link.

Los comentarios, observaciones, solicitudes de cambio o reclamos relativos a este documento o a las Políticas de Certificados de Certificadora del Sur, deben ser enviadas al correo soporte@certificadoradelsur.cl.

***** FIN DEL DOCUMENTO *****