POLÍTICA DE CERTIFICADOS 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
VF_1.0		Diciembre 2021	Se revisa y modifica según Guía de Acreditación	Cristián Altamirano	Cristián Echeverría
VF_2.0		Abril 2022	Se incorporan observaciones Entidad Acreditadora	Flavio Tapia	Cristián Echeverría
VF_2.1		Agosto 2022	Se modifica el registro del titular, la autenticación y verificación de identidad del solicitante.	Flavio Tapia	Cristián Echeverría
VF_2.2		Agosto 2023	Se revisa y modifica según revisión de economía	Flavio Tapia	Cristián Echeverría
VF_2.3		Octubre 2023	Se revisa y modifica según revisión de economía	Flavio Tapia	Cristián Echeverría

CONTENIDO

1. INTRODUCCIÓN

El presente documento contiene la Política de Certificados (CP) referente a los certificados de Firma Electrónica Avanzada emitidos por Certificadora del Sur, la cual está regida por la ley 19.799 "SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA AVANZADA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA", su reglamento y normas técnicas asociadas.

1.1. VISIÓN GENERAL

La norma chilena Nch2805.Of2003 "Tecnología de la Información – Requisitos de las políticas de las autoridades certificadoras que emiten certificados de llaves públicas" define una Política de Certificados como "*conjunto designado de reglas que indica la aplicabilidad de un certificado a una comunidad particular y/o clase de aplicación con requisitos de seguridad comunes".*

Esta Política de Certificados (CP), en conjunto con la Declaración de Prácticas de Certificación (CPS), 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 Avanzada emitidos y los dispositivos seguros de creación de las llaves de Firma Electrónica Avanzada, tanto para la CA (HSM) y el titular (Token).

La estructura de esta Política de Certificados considera lo estipulado por la norma chilena Nch2805.Of2003 en la que se referencia la norma IETF RFC 2527 "Internet X.509 Pública Key Infraestructure Certificate Policy and Certification Practices Framework" y las 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 LA POLÍTICA

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 LA POLÍTICA

Nombre	POLÍTICA DE CERTIFICADOS – CERTIFICADORA DEL SUR
Versión Actual	2.3
Versión Anterior	2.2
Fecha Última Actualización	OCTUBRE 2023
OID (Object Identifier)	1.3.6.1.4.1.55784
URL de Publicación	https://www.certificadoradelsur.cl/website/descargas.jsp

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 esta misma política, 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 el solicitante.

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 para a tener la calidad de Suscriptor, 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 esta Política de Certificados, 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 POLÍTICA

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 POLÍTICA

1.5.1. DATOS DE CONTACTO DE LA ORGANIZACIÓN

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

1.5.2. PERSONA QUE DETERMINA LA IDONEIDAD DE LA CP

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 Certificadora Raíz deberá emitir un certificado raíz autofirmado para sí misma, en su calidad de Autoridad Certificadora Raíz.

La Autoridad Certificadora Raíz firmará los certificados electrónicos de las autoridades certificadoras intermedias, las cuales compartirán esta Política de Certificados, estableciendo de esta manera una cadena jerárquica de confianza entre la Autoridad Certificadora Raíz, y sus Autoridades Certificadoras Intermedias o Subordinadas.

2.1.2. OBLIGACIONES DE LA AUTORIDAD CERTIFICADORA

La Autoridad Certificadora deberá cumplir lo establecido en esta Política de Certificados, y en las Declaraciones de Prácticas de Certificación, que dependen de esta Política, para la emisión de certificados.

Las obligaciones de la Autoridad Certificadora contemplan el otorgamiento, suspensión y revocación de certificados de Firma Electrónica Avanzada a usuarios o titulares; la administración y operación de la PSC; la publicación y mantención de la lista de certificados emitidos vigentes, suspendidos, revocados, traspasados y homologados, a través de un registro de acceso público por medios electrónicos de manera continua y regular.

La información de los certificados emitidos y los datos proporcionados por el usuario o titular del certificado de Firma Electrónica Avanzada que sean necesarios para la emisión de dichos certificados, los cuales no podrán ser utilizados para otros fines, deberá ser almacenada durante a lo menos seis años, contados desde su emisión, así como también se deben aplicar las disposiciones de la Ley N° 19.628, sobre la Protección de la Vida Privada.

2.1.3. 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
- Enviar información fidedigna a la Autoridad Certificadora correspondiente
- Almacenar en forma segura, y durante a lo menos seis años que exige la ley, la documentación aportada en el proceso de emisión de un certificado.

2.1.4. 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.

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 presente

Política de Certificados, y la 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

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 de la ejecución defectuosa cuando su origen sea la omisión de las obligaciones que corresponden al solicitante, Usuario o 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 estas políticas y las correspondientes 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.

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. Mayores detalles del acceso al repositorio serán declarados en las Prácticas de Certificación de cada tipo de certificado de Firma Electrónica Avanzada.

2.4. RESPONSABILIDADES FINANCIERAS

2.4.1. COBERTURA DE SEGUROS

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

2.4.2. 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.

2.4.3. INDEMNIZACIÓN DE LAS PARTES QUE CONFÍAN

No aplica.

2.4.4. 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 Política de Certificados, 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. POLÍTICA 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 presente Política de Certificados
- Las Prácticas de Certificación de todos los certificados emitidos por la Autoridad Certificadora
- La información respecto al estado de vigencia y validez de los certificados emitidos, suspendidos, revocados, traspasados y homologados
- Los certificados de raíz e intermedios de todos los certificados bajo la Autoridad Certificado para el Estado
- La lista de los certificados revocados (CRL)
- La Declaración de Privacidad
- La consulta OCSP - Online certificate status protocol
- Las resoluciones de la Entidad Acreditadora que le afecten.

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 por la Autoridad Certificadora

- Todos los certificados revocados y suspendidos 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 auditoria 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.

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.

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.

Para mayores detalles de los registros y tipos de eventos que se deben registrar, revisar la Declaración de Prácticas de Certificación de cada Autoridad Certificadora, dependiendo del tipo de certificado.

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.

Certificadora del Sur declara tener un sistema de gestión de incidentes de seguridad, la operación de este está descrita en el documento interno PS07_Gestión de Incidentes de Seg de la Inf_VF_2.1. Adicionalmente, posee un plan de contingencia en forma del procedimiento interno PS03_Plan de Continuidad de Negocio y Recuperación ante Desastres _ VF_3.1

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 Política de Certificados.

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. La privacidad e integridad de la información mencionada, está garantizada por el procedimiento interno PS04 _Plan de Seguridad de Sistemas y Administracion _ VF_3.0 punto 28. ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN donde se detalla el almacenamiento de la información relevante de la Autoridad Certificadora. Se considera para el almacenamiento la información de las aplicaciones de la autoridad certificadora, registros, base de datos y configuraciones de los servicios.

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. 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.

4.1.4. 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.

4.1.5. INFORMACIÓN DIVULGADA POR LA ORGANIZACIÓN

4.1.5.1. 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 esta Política de Certificación y en las Prácticas de Certificación.

4.1.5.2. 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.

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

Revisar la Declaración de Prácticas de Certificación.

La Autoridad Certificadora publicara el estado de vigencia y revocación de los certificados de firma electrónica 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)

4.1.5.4. ENTREGA DE INFORMACIÓN POR SOLICITUD JUDICIAL

Revisar la Declaración de Prácticas de Certificación.

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.

4.1.5.5. ENTREGA DE INFORMACIÓN POR SOLICITUD DEL PROPIETARIO

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.

4.1.6. 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.	CN = Jose Cristian Echeverria Briones E = echeverria@certificadoradelsur.cl

	Initials se utilizará para incorporar el Rut del Titular.	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 sujeto, 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/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 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 con chip (por motivos de seguridad) completando un formulario de solicitud de firma electrónica avanzada, dicha solicitud generará un numero de solicitud la que deberá ser firmada y se obtendrá la huella dactilar con tinta y se verificará y reforzará la vigencia de la cedula a través del proceso de match on card. 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 enviará la clave pública, provista por el usuario a la CA, para que éste firme y se genere el certificado de firma avanzada, cuya llave privada será almacenada en un dispositivo criptográfico (token) que cumpla con la normativa técnica vigente a la fecha.

A continuación, se establecen las políticas generales para la validación de identidad de un solicitante.

5.1. REGISTRO INICIAL

5.1.1. TIPOS DE NOMBRES

Los certificados 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 Común). El valor autenticado del Nombre Común, es el nombre completo del solicitante de certificado.

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 con chip (por motivos de seguridad) completando un formulario de solicitud de firma electrónica avanzada, dicha solicitud generará un numero de solicitud la que deberá ser firmada y se obtendrá la huella dactilar con tinta y se verificará y reforzará la vigencia de la cedula a través del proceso de match on card. 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 enviará la clave pública, provista por el usuario a la CA, para que éste firme y se genere el certificado de firma avanzada, cuya 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 re-emitirá 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 tendrá lugar cuando el prestador de servicios de certificación constate alguna de las siguientes circunstancias:

- Solicitud del titular del certificado.
- Fallecimiento del titular o disolución de la persona jurídica que represente, en su caso.
- Resolución judicial ejecutoriada.
- Que el titular del certificado al momento de solicitarlo no proporcionó los datos de la identidad personal u otras circunstancias objeto de certificación, en forma exacta y completa.
- Que el titular del certificado no ha custodiado adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que le proporcione el certificador.
- Que el titular del certificado no ha actualizado sus datos al cambiar éstos.
- Las demás causas que convengan el prestador de servicios de certificación con el titular del certificado.

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

5.4.1. QUIEN PUEDE SOLICITAR UNA REVOCACIÓN

La revocación de un certificado de firma electrónica avanzada podrá ser solicitada por:

- El titular del certificado de firma electrónica
- Por resolución judicial ejecutoriada

5.4.2. PROCEDIMIENTO PARA SOLICITAR UNA REVOCACIÓN

El usuario o titular podrá enviar la solicitud de revocación de Firma Electrónica Avanzada firmado con su Firma Electrónica Avanzada al correo revocacion@certificadoradelsur.cl para verificar su identidad, una vez recepcionada la solicitud se enviará un email de recepción de la solicitud al mismo correo que está asociado al certificado de firma electrónica avanzada y un segundo cuando esta ya está procesada. Una solicitud de revocación no debe ser procesada más allá de 24 horas desde la recepción de esta.

El suscriptor o titular podrá hacer la solicitud de revocación en formato físico a través de oficina, o alguna de las sucursales; deberá presentarse con su cedula de identidad vigente y se le notificará una vez que la revocación este efectuada a través de un correo electrónico, al mismo correo que está asociado al certificado de firma electrónica avanzada.

5.4.3. REVOCACIÓN Y PERIODO DE GRACIA

No aplica.

5.5. REQUERIMIENTOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS

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 la solicitud presencial, 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).

La solicitud de certificado de firma electrónica avanzada se realizará a través del portal web de la Autoridad Certificadora: www.certificadoradelsur.cl. En dicho portal el Solicitante deberá proveer, y luego validar, la siguiente información: La información del RUT (Rol Único Tributario), nombre completo, apellido paterno y apellido materno.

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 de identidad con chip (por motivos de seguridad), la que será verificada fehacientemente en forma presencial por el operador de registro, usando además el método “match on card” para reforzar la verificación fehaciente de identidad, verificando su nombre contra los datos capturados desde la cédula. El Operador de Registro valida la vigencia del documento en el Servicio Registro Civil.

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. SUSPENSIÓN DE CERTIFICADOS

5.8.1. 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.

5.8.2. QUIEN PUEDE SOLICITAR UNA SUSPENSIÓN

La Suspensión puede ser solicitada por el Usuario o Titular.

5.8.3. PROCEDIMIENTO PARA SOLICITAR LA SUSPENSIÓN

El usuario o titular podrá enviar la solicitud de suspensión de Firma Electrónica Avanzada firmado con su Firma Electrónica Avanzada al correo revocacion@certificadoradelsur.cl para verificar su identidad, una vez recepcionada la solicitud se enviará un email de recepción de la solicitud al mismo correo que está asociado al certificado de firma electrónica avanzada y un segundo cuando esta ya está procesada. Una solicitud de revocación no debe ser procesada más allá de 24 horas desde la recepción de esta.

En caso de que el usuario o titular haga la solicitud de suspensión en formato físico a través de oficina, o alguna de las sucursales, deberá presentarse con su cedula de identidad vigente y se le notificará una vez que la suspensión este efectuada a través de un correo electrónico, al mismo correo que está asociado al certificado de firma electrónica avanzada.

5.8.4. 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.

5.9. CRL

5.9.1. FRECUENCIA DE EMISIÓN DE LA CRL

Las listas de revocación (CRL) de la Autoridad Certificadora serán actualizadas cada 24 horas y serán publicadas en el sitio web de la Autoridad Certificadora.

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

5.9.2. REQUERIMIENTOS DE VERIFICACIÓN DE LA CRL

Las partes que confían son personas naturales o jurídicas que reciben un documento firmado electrónicamente o bien corroboran la identidad digital de un tercero, a través de una Firma Electrónica Avanzada asociado a un certificado válidamente emitido por Certificadora del Sur, verificable a través de la llave pública que figura en el certificado de Firma Electrónica Avanzada del Titular.

Una parte que confía es responsable de verificar si se trata de un certificado original, si este certificado se encuentra con la vigencia en el momento que se produjo la firma del documento recibido y si el valor de la firma corresponde al documento y a la llave pública del certificado del firmante.

Para verificar el origen de un certificado digital se debe primero validar que el certificado de FEA fue emitido por Certificadora del Sur, utilizando como referencia la información publicada en el sitio de la Entidad Acreditadora (https://www.entidadacreditadora.gob.cl/) en la sección Certificados Raíces. Luego de confirmar el origen del certificado, se debe consultar información de revocación de Certificadora del Sur, tal como la lista de revocación de certificados CRL o el servicio de consulta de estado OCSP.

5.10. OCSP

5.10.1. 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

5.10.2. REQUERIMIENTOS DE VERIFICACIÓN DE REVOCACIÓN EN LÍNEA

Las terceras partes que confían deben verificar el estado de un certificado en el cual van a confiar. Esta comprobación puede ser realizada mediante CRL y/o mediante el protocolo OCSP, el cual tiene como único requisito que sebe ser consultado con un cliente compatible con RFC 6960.

5.11. OTRAS FORMAS DE AVISO DE REVOCACIÓN DISPONIBLES

No Aplica.

5.11.1. REQUERIMIENTOS DE OTRAS FORMAS DE VERIFICACIÓN DE REVOCACIÓN

No Aplica.

5.11.2. REQUERIMIENTOS ESPECIALES SOBRE COMPROMISO DE LA LLAVE

No Aplica.

5.12. 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.

5.13. 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 Recuperación ante Desastres _ VF_3.1”, el cual se encuentra debidamente formalizado y versionado.

5.13.1. 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 Certificado, o la Autoridad de Registro, según corresponda, 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.

5.13.2. 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.

5.13.3. 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 y los certificados de titulares emitidos firmados por esa CA, con fecha posterior a la del compromiso, serán revocados.

5.13.4. 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”.

5.14. 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 Titulares y terceros que confían.

El plan de término deberá incluir, a lo menos, lo siguiente:

- La notificación a las partes afectadas por la terminación, tales como 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 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 Titulares y de CAs subordinadas, si es necesario
- El reembolso (si es necesario) a los 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.

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.

La Autoridad Certificadora cuenta con la Política General de Seguridad, así como con políticas, planes y procedimientos específicos para gestionar la seguridad de sus operaciones.

6.1. CONTROLES DE SEGURIDAD FÍSICA, DE PROCEDIMIENTOS Y DEL PERSONAL

6.1.1. CONTROLES FÍSICOS DE SEGURIDAD

La Autoridad Certificadora, para la prestación de sus servicios, integrará a sus políticas y procedimientos los servicios de proveedores de Datacenter externos y/o internos de acuerdo a lo establecido en “SF01 Politica Acceso Fisico _ VF_2.0”.

6.1.2. UBICACIÓN Y CONSTRUCCIÓN DEL SITE PRINCIPAL

El datacenter principal se encuentra ubicado en Santiago, Región Metropolitana, Chile.

Las oficinas administrativas se ubican en la ciudad de Los Ángeles, Región del Biobío, Chile.

6.1.3. ACCESO FÍSICO

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.1. CONTROLES DE SEGURIDAD UTILIZADOS POR EL PSC.

6.1.4. ENERGÍA Y AIRE ACONDICIONADO

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.1.2.2. SISTEMA DE CLIMATIZACIÓN Y EXPOSICION AL AGUA.

6.1.5. EXPOSICIÓN DEL AGUA

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.1.2.2. SISTEMA DE CLIMATIZACIÓN Y EXPOSICION AL AGUA.

6.1.6. PREVENCIÓN Y PROTECCIÓN CONTRA INCENDIOS

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.1.2.3. SISTEMA DE EXTINCIÓN Y CONTROL DE INCENDIOS.

6.1.7. ALMACENAMIENTO DE MEDIOS

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.2.6. ALMACENAMIENTO DE LLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO.

6.1.8. ELIMINACIÓN DE RESIDUOS

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.1.1.2. ELIMINACIÓN DE RESIDUOS

6.1.9. COPIA DE SEGURIDAD EN EL SITE SECUNDARIO

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.2.4. COPIA DE SEGURIDAD DE LLAVE PRIVADA DE LA CA.

6.2. CONTROLES DE PROCEDIMIENTOS

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

6.3. ROLES DE CONFIANZA

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.3. ROLES DE CONFIANZA.

6.3.1. CANTIDAD DE PERSONAS REQUERIDAS POR TAREA

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.3.1. CANTIDAD DE PERSONAS REQUERIDAS POR TAREA

6.3.2. IDENTIFICACIÓN Y AUTENTICACIÓN DE CADA ROL

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.3.2. IDENTIFICACIÓN Y AUTENTICACIÓN DE CADA ROL.

6.4. CONTROLES DEL PERSONAL

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.4. CONTROLES DEL PERSONAL.

6.4.1. ANTECEDENTES, CALIFICACIONES Y EXPERIENCIA DEL PERSONAL

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.4.1. REQUERIMIENTOS DE ANTECEDENTES Y CONOCIMIENTOS.

6.4.2. PROCEDIMIENTO DE VERIFICACIÓN DE ANTECEDENTES

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.4.2. PROCEDIMIENTO DE VERIFICACIÓN DE ANTECEDENTES.

6.4.3. REQUISITOS DE CAPACITACIÓN Y ENTRENAMIENTO

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.4.3. REQUISITOS DE CAPACITACIÓN Y ENTRENAMIENTO.

6.4.4. FRECUENCIA Y REQUERIMIENTOS DE REENTRENAMIENTO

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.4.4. FRECUENCIA Y REQUERIMIENTOS DE REENTRENAMIENTO.

6.4.5. FRECUENCIA Y SECUENCIA DE LA ROTACIÓN DE LOS TRABAJOS

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.4.5. FRECUENCIA Y SECUENCIA DE LA ROTACIÓN DE LOS TRABAJOS.

6.4.6. SANCIONES POR ACCIONES NO AUTORIZADAS

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.4.6. SANCIONES POR ACCIONES NO AUTORIZADAS.

6.4.7. REQUERIMIENTOS DE PERSONAL CONTRATISTA

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.4.7. REQUERIMIENTOS DE PERSONAL CONTRATISTA.

6.4.8. DOCUMENTACIÓN SUMINISTRADA POR EL PERSONAL

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.4.8. DOCUMENTACIÓN SUMINISTRADA POR EL PERSONAL.

6.5. CONTROLES TÉCNICOS DE SEGURIDAD

La Autoridad Certificadora contará con procedimientos y controles para garantizar la seguridad en la emisión de un certificado, en especial los aspectos relacionados con la generación de llaves de sus certificados raíces, contenidos en el punto 6.5. CONTROLES TÉCNICOS DE SEGURIDAD de la Declaración de Prácticas de Certificación de la Autoridad Certificadora.

6.5.1. GENERACIÓN E INSTALACIÓN DEL PAR DE LLAVES

6.5.1.1. GENERACIÓN DEL PAR DE LLAVES

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.1.1. GENERACIÓN DEL PAR DE LLAVES.

6.5.1.2. ENTREGA DE LLAVE PRIVADA A LA ENTIDAD

No aplica.

6.5.1.3. ENTREGA DE LLAVE PÚBLICA AL EMISOR DEL CERTIFICADO

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.1.2. ENTREGA DE LLAVE PÚBLICA AL EMISOR DEL CERTIFICADO.

6.5.1.4. ENTREGA DE LLAVE PÚBLICA DE CA A USUARIOS O TITULARES

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.1.3. ENTREGA DE LLAVE PÚBLICA DE CA A USUARIOS.

6.5.1.5. TAMAÑOS DE LLAVE

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.1.4. TAMAÑOS LLAVE.

6.5.1.6. GENERACIÓN DE PARÁMETROS DE LLAVE PÚBLICA

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.1.5. GENERACIÓN DE PARÁMETROS DE LLAVE PÚBLICA.

6.5.1.7. CONTROL DE CALIDAD DE PARÁMETROS

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.1.6. CONTROL DE CALIDAD DE PARÁMETROS.

6.5.1.8. GENERACIÓN DE LLAVES DE HARDWARE / SOFTWARE

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.1.7. GENERACIÓN DE LLAVES DE HARDWARE / SOFTWARE.

6.5.1.9. 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

El módulo criptográfico debe cumplir con la norma FIPS 140-2 Level 3.

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

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.2.2. CONTROL PRIVADO DE LLAVE PRIVADA (N FUERA DE M).

6.5.2.3. COPIA DE SEGURIDAD DE LLAVE PRIVADA

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.

6.5.2.4. ARCHIVO DE LLAVE PRIVADA

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.2.5. ARCHIVO DE LLAVE PRIVADA.

6.5.2.5. ALMACENAMIENTO DE LLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.2.6. ALMACENAMIENTO DE LLAVE PRIVADA EN EL MÓDULO CRIPTOGRÁFICO.

6.5.2.6. MÉTODO DE ACTIVACIÓN DE LLAVE PRIVADA

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.2.7. MÉTODO DE ACTIVACIÓN DE LLAVE PRIVADA.

6.5.2.7. MÉTODO DE DESACTIVACIÓN DE LLAVE PRIVADA

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.2.8. MÉTODO DE DESACTIVACIÓN DE LLAVE PRIVADA.

6.5.2.8. MÉTODO DE DESTRUCCIÓN DE LLAVE PRIVADA

Se aplicará lo indicado en las Declaración de Prácticas de Certificación de la Autoridad Certificadora, contenidas en el punto 6.5.2.9. MÉTODO DE DESTRUCCIÓN DE LLAVE PRIVADA.

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 Política de Certificados.

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

6.6.1. REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURIDAD INFORMÁTICA

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

6.6.2. CALIFICACIÓN DE SEGURIDAD INFORMÁTICA

Las áreas críticas y específicas de seguridad, y administración de la Infraestructura de Llave Pública, deberán cumplir con requisitos de seguridad definidos en la Política General de Seguridad de Certificadora del Sur.

6.6.3. CONTROLES TÉCNICOS DEL CICLO DE VIDA

Se aplicará lo indicado en las Prácticas de Certificación de la Autoridad Certificadora correspondiente al tipo de certificado.

6.6.4. CONTROLES DE DESARROLLO DE SISTEMAS

La Autoridad Certificadora establece Políticas de Desarrollo Seguro de Software, controlando que todos los desarrollos se realicen dentro de un entorno seguro, utilizando un proceso que asegure la calidad y seguridad en el proceso.

6.6.5. CONTROLES DE GESTIÓN DE SEGURIDAD

Se deben considerar todos los controles que se detallen en la Política General de Seguridad de Certificadora del Sur, y las demás políticas que componen el Sistema de Gestión de Seguridad de la Información:

- Política general de seguridad
- Política de seguridad física

- Política de seguridad sistemas de información
- Política de seguridad del personal
- Política de seguridad de las telecomunicaciones
- Política de gestión del riesgo – continuidad operativa
- Auditoría y cumplimiento

6.6.6. CLASIFICACIONES DE SEGURIDAD DEL CICLO DE VIDA

No Aplica.

6.7. CONTROLES DE SEGURIDAD DE RED

La Autoridad Certificadora contará con un Plan de Seguridad de Redes Computacionales, el cual deberá contemplar controles de seguridad, recuperación de desastres y controles de acceso.

6.8. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO

Se aplicará lo indicado en las Prácticas de Certificación de la Autoridad Certificadora correspondiente al tipo de certificado, contenidas en el punto 6.6.2. CONTROLES DE INGENIERÍA DEL MÓDULO CRIPTOGRÁFICO.

7. ADMINISTRACIÓN DE LA POLÍTICA DE CERTIFICADOS

7.1. PROCEDIMIENTOS DE GESTIÓN DEL CAMBIO

Las políticas 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.

7.2. 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 Política de Certificados en el sitio web https://www.certificadoradelsur.cl/website/descargas.jsp, y se mantendrá la versión anterior por un periodo de tiempo no inferior a 30 días.

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