microsystem
INFORMACIÓN INTELIGENTE | DESDE 1978

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN PO02

Microsystem S.A.

Actualizado por:	Revisado por:	Aprobado por:
Jaroslaw Marcin Iwanski Gerente I+D	Ricardo González Gerente Micro e-Doc	Nicolás Andalaft Gerente General

ÍNDICE

1. Introducción

1.1. Alcance y Objetivo

Microsystem S.A. en su rol de Proveedor de Servicios de Certificación (Autoridad Certificadora), posee dos documentos que le permiten gestionar el actuar de la Autoridad de Registro, estos son **ME-DG-PO01 Políticas de Certificación de Firma Electrónica Avanzada** (CP/PC) y **ME-DG-PO02 Declaración de Prácticas de Certificación** (CPS/DPC).

El documento de Políticas de Certificación antes mencionado, corresponde al conjunto de reglas establecidas por Microsystem S.A, con el objetivo de establecer la aplicabilidad del certificado de Firma Electrónica Avanzada y controlar su ciclo de vida.

Por otra parte, el presente documento, Declaración de Prácticas de Certificación, hace referencia al conjunto de prácticas que realiza la Autoridad Certificadora, para cumplir con las reglas establecidas en CP/PC en la prestación de los servicios de certificación de Firma Electrónica Avanzada (FEA) que serán brindados a una comunidad de usuarios, definiendo como Usuario, a los Titulares y las partes que confían.

Lo anterior, acorde a los requisitos del Ministerio de Economía, Fomento y Turismo, para los Prestadores de Servicio de Certificación (PSC).

La presente DPC es de carácter público y está dirigida a todas las personas naturales y jurídicas, ya sea en su rol de Solicitante, Titular o Partes que Confían, según se describe en el punto Partes Involucradas de PKI de FEA. Esta podrá ser consultada en la página web https://portal.ca.msys.cl/.

1.2. Administración del contenido

1.2.1. La revisión de este documento se realiza al menos una vez al año o según sea necesario para mantener en sintonía con los procesos del PSC.

1.2.2. El contenido de éste documento es administrado y mantenido por el personal designado por el Comité de Seguridad.

1.2.3. El PSC podrá modificar el contenido del presente documento, sin perjuicio de que se mantenga el nivel de calidad esencial de sus servicios de certificación, previa notificación y/o aprobación de los cambios por la Entidad Acreditadora, según la complejidad del proceso que afecte la modificación a realizar.

1.2.4. Cualquier cambio, previa aprobación interna y de la Entidad Acreditadora del Ministerio de Economía, será publicado en el sitio de **Portal de la Autoridad Certificadora de Microsystem S.A.** - https://portal.ca.msys.cl

1.3. Repositorio Documental

1.3.1. Todos los documentos aplicables al proceso de certificación de Firma Electrónica Avanzada, tales como Políticas de Certificación, Declaración de Prácticas de Certificación, Política de Protección de los Derechos de los Usuarios, Política de Privacidad, etc., son de carácter público y de libre acceso por medio del **Portal de la Autoridad Certificadora de Microsystem S.A.** - https://portal.ca.msys.cl

2. Glosario

PC - Políticas de Certificación (CP - Certification Policies)

DPC - Declaración de Prácticas de Certificación (CPS - Certification Practice Statement)

PKI - Public Key Infrastructure: Una infraestructura de clave pública (en inglés: Public Key Infrastructure) es una combinación de hardware, software, políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma electrónica (en el contexto de esta DPC entendida por Firma Electrónica Avanzada), el no repudio de transacciones electrónicas.

FEA - Firma Electrónica Avanzada: Es un par de llaves, en forma de un **Certificado de FEA** que contiene la llave pública, en conjunto con su llave privada correspondiente almacenada, bajo exclusivo control del Titular, en un dispositivo criptográfico certificado bajo norma FIPS 140-2 Level 3.

Permite al Titular establecer una relación de confianza con terceros, protegiendo la integridad de documentos, confirmando que no han sido alterados desde que fueron firmados por el Titular y validando la identidad del Titular y su autoría.

Certificado de FEA: Corresponde a un documento electrónico personal e intransferible, en formato X.509, emitido por un Prestador de Servicios de Certificación (PSC), vinculando al Titular con su par de llaves.

Dicho certificado debe contener: nombre, RUN, algoritmo y llave pública, fecha de expiración y organismo que lo emite. Con ello el PSC da fe de que la Firma Electrónica Avanzada corresponde a un usuario concreto que es el Titular.

Certificado Raíz: En criptografía y seguridad informática, un certificado raíz es un certificado de clave pública sin firma o autofirmado que identifica la autoridad certificadora raíz (CA). Un certificado raíz forma parte de un esquema de infraestructura de clave pública. La variedad comercial más común está basada en el estándar ITU-T X.509, el cual normalmente incluye una firma digital de una autoridad certificadora.

Los certificados raíces de las Autoridades Certificadoras acreditadas conforme a la legislación de Chile se pueden encontrar en la página de la Entidad Acreditadora del Ministerio de Economía de Chile: https://www.entidadacreditadora.gob.cl/certificados-raiz/

Certificado Autoridad Intermedia: Los certificados intermedios se usan en representación del certificado raíz para evitar la necesidad de utilizarlo directamente. Microsystem S.A., en su calidad de Autoridad Certificadora, utiliza certificados intermedios como un proxy porque es necesario mantener los certificados raíz detrás de varias capas de seguridad, para garantizar que sus llaves sean absolutamente inaccesibles.

El certificado raíz en conjunto con el o los certificado(s) intermedio(s) relacionados forman una cadena de confianza.

Suspensión o Revocación de un Certificado: Es la acción de anular la validez de un certificado antes de la fecha de vencimiento indicada en el mismo, especialmente cuando el Titular cree que sus claves privadas están bajo control de otros.

La suspensión es una **anulación temporal**. Se aplica cuando el Titular no tiene la certeza de la pérdida del control de la llave privada y estima que lo puede recuperar. Al recuperar el control de la llave privada, el Titular puede reactivar la vigencia restante del certificado. En caso de no lograr dicha recuperación, el Titular puede proceder a la revocación del certificado correspondiente.

La revocación es una **anulación definitiva e irreversible**. Aplica, por ejemplo, cuando el titular tiene la certeza de la pérdida del control de la llave privada y desea anular por completo la vigencia del certificado. Otros casos donde aplica revocación están descritos en Suspensión y Revocación de Certificados de FEA

CRL - Certificate Revocation List: La lista de revocación de certificados, conocida por sus sigla en inglés CRL (Certificate Revocation List) es un registro utilizado en la operación de algunos sistemas criptográficos, usualmente los de infraestructura de clave pública (PKI), para mantener un listado de aquellos certificados (más concretamente sus números de serie) que han sido revocados o suspendidos y, por tanto, no son válidos y no se debe confiar en ellos. La invalidez es definitiva para los certificados revocados y temporal para los suspendidos.

OCSP - Online Certificate Status Protocol: El Protocolo de estado de certificado en línea (OCSP - Online Certificate Status Protocol) es un protocolo de Internet utilizado para obtener el estado de revocación de un certificado digital X.509. Dicho certificado se describe en el documento de referencia individualizado en el punto 16.8 de esta DPC, RFC 6960, y se encuentra en la pista de estándares de Internet. Se creó como alternativa a las listas de revocación de certificados CRL.

No repudio: No repudio se refiere a un estado de negocios donde el supuesto autor de una declaración no es capaz de desafiar con éxito la validez de la declaración o contrato. El término es a menudo visto en un entorno legal donde la autenticidad de una firma está siendo desafiada. En tal caso, la autenticidad se está "repudiando". En caso de una Firma Electrónica Avanzada el hecho que un documento electrónico está firmado con un certificado de una persona es una prueba suficiente de la autenticidad de esta firma ante un juicio.

Repositorio: Un repositorio es un espacio centralizado donde se almacena, organiza, mantiene y difunde información digital, habitualmente archivos informáticos, que pueden contener documentación, conjuntos de datos o software.

Un par de llaves - llave privada y llave pública: **Llave privada** y **llave pública** son conceptos utilizados en la **criptografía asimétrica** (en inglés asymmetric key cryptography), también llamada **criptografía de clave pública** (en inglés public key cryptography). Una **llave privada** y una **llave pública,** que están relacionadas, forman un **par de llaves**.

La **llave privada** se aplica en operaciones de generación de un valor de una firma electrónica.

La **llave pública** se aplica en operaciones de verificación de un valor de una firma electrónica.

Dispositivo criptográfico: Es un dispositivo físico utilizado para proteger y acceder a un recurso restringido electrónicamente.

Este dispositivo se utiliza para resguardar la llave privada correspondiente a un certificado (en el contexto de esta DPC, un certificado de Firma Electrónica Avanzada).

PEN (Private Enterprise Number): Un número único asignado por la organización IANA a la solicitud de una empresa privada para identificar sus objetos a nivel de los certificados X.509, entre otros.

3. Partes Involucradas de PKI de FEA

3.1. Entidad Acreditadora

En conformidad con lo dispuesto en la ley 19.799, la Entidad Acreditadora en Chile es la Subsecretaría de Economía y Empresas de Menor Tamaño. Su responsabilidad es velar que un Prestador de Servicios de Certificación de Firma Electrónica Avanzada demuestre que cuenta tanto con los recursos necesarios para otorgar el servicio de manera adecuada, como los sistemas, programas informáticos, recursos físicos y humanos necesarios con el fin de otorgar el certificado de firma electrónica avanzada, permitiendo su inscripción en el registro de Prestadores de Servicios de Certificación acreditados.

3.2. Prestador de Servicios de Certificación (PSC) - Autoridad Certificadora (AC)

En conformidad a la ley 19.799 sobre documentos electrónicos, el Prestador de Servicios de Certificación, es la empresa encargada de brindar los servicios de certificado de firma electrónica avanzada y servicios de certificación de dicha firma, para lo que debe necesariamente estar acreditada por la Entidad Acreditadora. En el contexto de esta declaración de prácticas de certificación, Microsystem S.A. es el Prestador de Servicios de Certificación.

3.3. Autoridad de Registro (AR)

La autoridad de registro es una entidad encargada de recibir y tratar las solicitudes de Firma Electrónica Avanzada para ser evaluadas por la Autoridad Certificadora de Microsystem S.A. La autoridad de registro debe realizar la comprobación fehacientemente de la identidad de los solicitantes de certificados de Firma Electrónica Avanzada. Las actividades deberán ser desarrolladas dando pleno cumplimiento al contrato y a esta declaración de prácticas de certificación. Puede ser una de las siguientes:

- Interna - un funcionario de Microsystem S.A. con atribuciones de Operador de Registro
- Externa - ante notario público u oficial del registro civil

3.4. Solicitantes

Son personas naturales que solicitan a Microsystem S.A. la emisión de un certificado de Firma Electrónica Avanzada.

Las personas naturales que soliciten los servicios de certificación de Microsystem S.A., deben tener una Cédula de Identidad Chilena con mínimo 30 días de vigencia restante, la que será utilizada como credencial para emitir certificados.

Adicionalmente, debe entregar a la Autoridad de Registro, los antecedentes complementarios que se le soliciten, tal como se explica en el punto Solicitud de Certificado de FEA.

3.5. Titulares

Una vez aprobada con éxito la solicitud de emisión de un certificado de Firma Electrónica Avanzada el Solicitante se transforma en un Titular. Los Titulares reciben un certificado de Firma Electrónica Avanzada que los identifica y una clave privada para poder operar digitalmente con dicho certificado, siendo esta de exclusivo control del Titular; esta clave privada está asociada a la clave pública del certificado de FEA.

3.6. Portal de Usuario de Firma Electrónica Avanzada

Es un aplicativo web donde los Titulares pueden acceder a los servicios de la Autoridad Certificadora de Microsystem S.A. relacionados con la gestión de sus certificados emitidos por Microsystem S.A. Los servicios disponibles son: renovación, revocación, suspensión y solicitud de certificados. Microsystem S.A. en su rol del PSC, no ofrece los servicios de traspasos u homologación de certificados desde otras PSC.

El ingreso al aplicativo está disponible bajo apartado **Portal de Usuarios de Firma Electrónica Avanzada** en la pagina: https://portal.ca.msys.cl

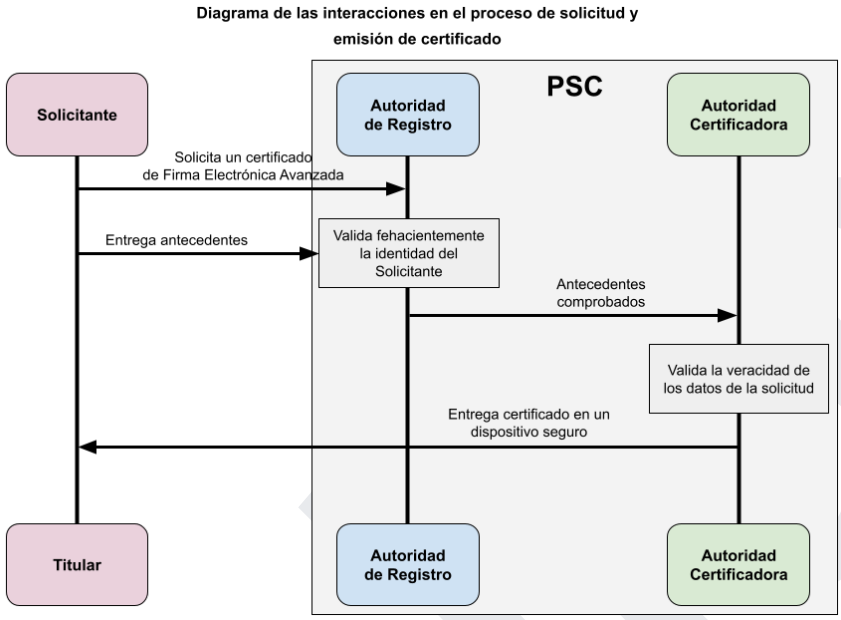
3.7. Partes que Confían

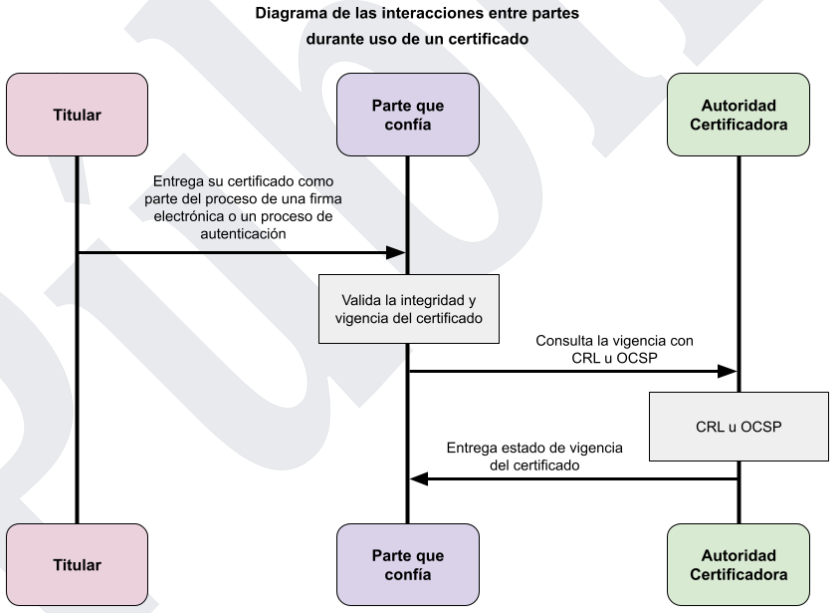
Las partes que confían son personas naturales o jurídicas que reciben un documento firmado electrónicamente o bien corroboran la identidad digital de un tercero, mediante el uso de una llave privada de una Firma Electrónica Avanzada emitida por Microsystem S.A., por su Titular, verificable a través de la llave pública que figura en el certificado de Firma Electrónica Avanzada del Titular.

Una parte que confía debe contar con los artefactos que le permitan 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 Microsystem S.A., 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 Microsystem S.A., tal como la lista de revocación de certificados CRL o el servicio de consulta de estado OCSP.

3.8. Diagrama de las interacciones entre partes





4. Consideraciones Generales

4.1. Obligaciones

4.1.1. Microsystem S.A. como PSC

4.1.1.1. Debe contar con políticas y prácticas de certificación que sean objetivas y no discriminatorias, en contra de las partes involucradas, siendo públicamente accesibles y escritas de forma sencilla y en idioma castellano.

4.1.1.2. Microsystem S.A. debe mantener un repositorio de acceso público de los certificados emitidos en su calidad de PSC, por medio del sitio web https://portal.ca.msys.cl/, dejando en evidencia el estado de los certificados emitidos: vigente, revocado, suspendido.

4.1.1.3. Microsystem S.A. debe proteger toda la información relevante de los Titulares y Solicitantes. La información será confidencial, por lo que no será utilizada con fines distintos a las actividades de Microsystem S.A. en su función de Autoridad Certificadora.

En casos particulares, se entregará información de los Titulares (siempre dentro del margen de la ley Nº19.799), para el Titular del certificado o para procedimientos judiciales por solicitud de tribunales.

4.1.1.4. Debe publicar en su sitio web https://portal.ca.msys.cl/ todas las resoluciones emitidas por la Entidad Acreditadora que le afecten.

4.1.1.5. Comprobar fehacientemente la identidad del Solicitante, por medio de una cita presencial para generar la solicitud del certificado de FEA, como se indica en el apartado Solicitud de Certificado de FEA de la presente DPC.

4.1.1.6. Contar con mecanismos adecuados para generar y entregar al Titular de forma segura la llave privada del certificado de FEA emitido por Microsystem S.A.

4.1.1.7. Revocar los certificados que no cumplan las políticas y prácticas de uso de certificados.

4.1.1.8. Notificar, en caso del término de sus funciones de PSC de FEA, a todos los Titulares vigentes y transferirlos, siempre cuando sea posible, a otro PSC de FEA. Cada Titular activo tendrá el derecho de negarse a esa transferencia, en aquel caso su certificado quedará revocado. En base a los plazos estipulados en el punto Término de actividades del PSC.

4.1.1.9. Solicitar la cancelación de la inscripción en el registro de PSC a la Entidad Acreditadora, en caso de cese de actividades, dentro de los plazos establecidos en el punto Término de actividades del PSC de la presente DPC.

4.1.1.10. Informar a la Entidad Acreditadora sobre cualquier circunstancia relevante que impida la continuación de la actividad de Microsystem S.A. como PSC. Debe comunicar de forma inmediata cuando se tenga conocimiento de ello, el inicio de un procedimiento concursal de liquidación o que se encuentre en cesación de pagos.

4.1.1.11. Cumplir con la Ley 19799 y el Decreto N° 181 Reglamento de dicha ley, acordes a la normativa vigente según lo indicado por la Entidad Acreditadora para cumplir el rol de una Autoridad Certificadora, y las leyes que rigen este tipo de actividades, tales como la ley del consumidor N° 19.496 y protección a la vida privada ley N° 19.628.

4.1.1.12. Cumplir con lo establecido en esta DPC y en la PC.

4.1.1.13. Microsystem S.A. debe cuidar y administrar de manera segura el sistema de llaves criptográficas del Certificado Raíz, ya que este último permite firmar certificados de las entidades de certificación intermedias. El Certificado Raíz de Microsystem S.A. es el fundamento del modelo de confianza de todos los certificados de entidades intermedias que ha emitido para proveer Servicios de Certificación.

4.1.1.14. Todos los documentos, registros públicos y servicios relacionados con las actividades y funciones del PSC, deben estar electrónicamente accesibles, para las partes involucradas, de manera continua y regular, según lo requieran.

4.1.2. Microsystem S.A. como Autoridad Certificadora (AC)

4.1.2.1. Emitir los certificados de FEA con la información del Titular exacta, según entregado en el procedimiento de registro, con estructura y contenido conforme a la normativa vigente, X.509 v3, identificándose en este en su rol de emisor, todo lo anterior en cumplimiento de lo estipulado en esta DPC y PC correspondiente.

4.1.2.2. Resguardar la confidencialidad de los datos de la creación de las FEAs.

4.1.2.3. Publicar en su sitio web https://portal.ca.msys.cl/ la PC y DPC.

4.1.2.4. Notificar al Titular y a la Entidad Acreditadora y publicar en su sitio web (https://portal.ca.msys.cl/), cualquier cambio que se realice en los documentos mencionados en el punto anterior y en los términos y condiciones básicas.

4.1.2.5. Mantener el acceso público a las Listas de Certificados Revocados (CRL), disponibles en el apartado de **Información de Confianza** del sitio web (https://portal.ca.msys.cl/), manteniendo las actualizadas de acuerdo a la vigencia de cada una y disponibilizar el servicio de consulta en línea de vigencia de certificados OCSP.

4.1.2.6. Proporcionar, administrar y utilizar una infraestructura segura y confiable para el procesamiento y difusión de todos los datos de la Autoridad Certificadora, que los proteja contra pérdida o falsificación, garantizando su integridad y disponibilidad.

4.1.2.7. Entregar los servicios con los protocolos y procedimientos de acuerdo a lo estipulado en la legislación.

4.1.2.8. Resguardar la información recopilada por un periodo de al menos 6 años desde la fecha de recepción / generación.

4.1.2.9. Disponer de recursos y capacidades adecuadas para la administración de activos criptográficos (llaves y dispositivos)

4.1.2.10. Poseer y aplicar los procedimientos de gestión de ciclo de vida de los activos criptográficos (llaves y dispositivos).

4.1.2.11. Asegurar que la llave privada del Titular se genere de acuerdo al algoritmo RSA con un largo al menos 2048 bits y quede almacenada, bajo su exclusivo control, en un dispositivo criptográfico certificado bajo norma FIPS 140-2 Level 3.

4.1.2.12. Realizar controles de seguridad física e informática de los diversos activos de la Autoridad Certificadora.

4.1.2.13. Respetar lo estipulado en los contratos firmados con los Titulares.

4.1.3. Microsystem S.A. como Autoridad de Registro

4.1.3.1. Comprobar fehacientemente la identidad del Solicitante previo a la emisión del certificado de FEA.

4.1.3.2. Recopilar y custodiar la información entregada por el Solicitante para la emisión del certificado de FEA.

4.1.3.3. Comunicar a la AC la información requerida para la emisión de los certificados de FEA.

4.1.3.4. Debe contar con la infraestructura y controles adecuados de seguridad física, red, personal y procedimientos para las actividades de registro mencionadas en el punto Solicitud de Certificado de FEA.

4.1.3.5. Informar a las partes involucradas las características generales de los procedimientos de creación y verificación de FEA, políticas y prácticas de certificación, y demás políticas que los Titulares se comprometen a seguir en la prestación del servicio, cuando se realiza la solicitud del certificado de FEA.

4.1.3.6. Gestionar los certificados de FEA en base a lo estipulado en las PC y DPC.

4.1.3.7. Formalizar el acuerdo contractual (Contrato de Suscripción de Firma Electrónica Avanzada) con el Titular previo a la emisión del certificado.

4.1.3.8. Realizar el cobro de las tarifas establecidas por los servicios de certificación solicitados por el Titular.

4.1.4. Partes que confían

4.1.4.1. Comprobar siempre, antes de confiar, la integridad de un certificado de Firma Electrónica Avanzada emitido por Microsystem S.A., comprobando su integridad mediante el certificado raíz y el certificado de la autoridad intermedia de FEA de Microsystem S.A. publicados en la página de la Entidad Acreditadora (https://www.entidadacreditadora.gob.cl/certificados-raiz/).

4.1.4.2. Comprobar siempre, antes de confiar, la vigencia de un certificado de Firma Electrónica Avanzada emitido por Microsystem S.A., comprobando su estado en el servicio de consulta disponible en la página web https://portal.ca.msys.cl/ y/o mediante CRL, OCSP correspondientes.

4.1.4.3. Aceptar los Certificados de FEA de Microsystem S.A. para todos los procesos y usos autorizados de acuerdo a lo estipulado en la Ley 19.799.

4.1.4.4. Conocer los usos adecuados, responsabilidades, términos y condiciones que afectan a los certificados en los que confía.

4.1.5. Solicitante

4.1.5.1. Conocer, aceptar y actuar conforme las políticas PC y prácticas de certificación DPC y los términos y condiciones aplicables del PSC (disponibles en el portal https://portal.ca.msys.cl/).

4.1.5.2. Proporcionar información completa, vigente y veraz al momento de la validación de los datos de su identidad personal u otras circunstancias objeto de la certificación, brindando declaraciones exactas y completas.

4.1.6. Titular

4.1.6.1. Conocer, aceptar y actuar conforme las políticas PC y prácticas de certificación DPC y los términos y condiciones aplicables del PSC (disponibles en el portal https://portal.ca.msys.cl/).

4.1.6.2. Utilizar de forma adecuada el certificado de FEA, ya sea para fines legales u otros autorizados en conformidad con la presente DPC (Uso del Certificado de FEA).

4.1.6.3. Notificar a Microsystem S.A. de cualquier cambio en la información presentada que pueda afectar materialmente la confiabilidad de su certificado.

4.1.6.4. Al detectar inexactitud o cambios en el contenido del certificado de FEA, mientras este se encuentra vigente, debe notificar a la Autoridad Certificadora en un tiempo razonable.

4.1.6.5. Cumplir con las obligaciones que la Ley chilena le impone.

4.1.6.6. Custodiar adecuadamente los mecanismos de seguridad (dispositivo criptográfico o token, llave privada y contraseñas de acceso a dicha llave) del funcionamiento del sistema de certificación que les proporcione el certificador. El Titular tiene prohibido transferir la propiedad de dichos mecanismos a terceros.

4.1.6.7. Dejar de usar la llave privada, cuando el certificado de Firma Electrónica Avanzada emitido por Microsystem S.A. termine su vigencia, ya sea de forma natural o anticipada por revocación.

4.1.6.8. Tomar medidas preventivas para evitar el compromiso, pérdida, divulgación, modificación o uso no autorizado de su clave privada.

4.1.6.9. Solicitar la revocación del certificado de FEA en caso de una ocurrencia que afecte materialmente la integridad de dicho certificado emitido por Microsystem S.A., ya sea por:

4.1.6.9.1. Pérdida, robo o extravío del token que almacena la llave privada.

4.1.6.9.2. Pérdida de control sobre dicha llave.

4.1.6.9.3. Compromiso de las contraseñas que permiten al Titular hacer uso de su certificado de FEA.

4.1.6.9.4. Inexactitudes o cambios en el contenido del certificado de FEA que conozca o pueda conocer

4.1.6.9.5. Incumplimiento de las obligaciones a las que se encuentra comprometido el Titular dentro de los requerimientos impuestos por la Subsecretaría de Economía y Empresas de Menor Tamaño.

4.1.6.10. Usar dispositivos y productos seguros que brinden la protección adecuada a sus claves.

4.1.6.11. Abstenerse de enviar a Microsystem S.A. o cualquier repositorio de información de Microsystem S.A. cualquier información ajena a los procesos de Firma Electrónica Avanzada.

4.1.6.12. Abstenerse de alterar un certificado de FEA emitido por Microsystem S.A.

4.1.6.13. Abstenerse de usar un certificado para fines no contemplados en la licencia de uso emitida por Microsystem S.A.

4.1.6.14. Sin limitar otras obligaciones establecidas en el documento de políticas **ME-DG-PO01 Políticas de Certificación de Firma Electrónica Avanzada**, los Titulares tienen el deber de abstenerse de cualquier manipulación en los certificados presentados para engañar o defraudar a terceros.

4.1.6.15. Abonar el valor tarificado por Microsystem S.A. por los servicios y productos contratados, según la información de tarificación entregada al momento de presentar la solicitud.

4.2. Prohibiciones

Queda expresamente prohibido a cualquiera de las partes involucradas, sea Solicitante, Titular, Partes que confían u otros, controlar, interferir, realizar ingeniería inversa, o cualquier otro acto que afecte la ejecución técnica de los sistemas, la propiedad intelectual de Microsystem S.A. y el código fuente de dicha propiedad.

4.3. Responsabilidades de Microsystem S.A

4.3.1. Mantener vigente seguro, que cubre eventual responsabilidad civil de los certificados de FEA emitidos por Microsystem S.A., que exige la ley N° 19.799 de firma electrónica avanzada y documentos electrónicos, por un monto igual al solicitado por la Entidad Acreditadora.

4.3.2. Atender y dar respuesta a las quejas y reclamos de los Titulares y partes relacionadas.

4.3.3. Responsabilizarse por los daños y perjuicios, que en el ejercicio de su actividad como PSC, originados por la emisión y certificación de los certificados de FEA. A excepción de los daños ocasionados por el uso fraudulento o indebido de un certificado de FEA por el Titular o un tercero.

4.3.4. La integridad y disponibilidad de la información publicada en el repositorio público es de exclusiva responsabilidad de Microsystem S.A., quien cuenta con los recursos y procedimientos necesarios para restringir el acceso a los repositorios con otros fines diferentes a la consulta de validación de certificados de FEA.

4.3.5. Entregar los certificados de la jerarquía de la Firma Electrónica Avanzada de Microsystem S.A. a la Entidad Acreditadora y publicarlos en la página web https://portal.ca.msys.cl/ durante todo el tiempo en que Microsystem S.A. se encuentre acreditado como PSC.

4.3.6. Limitación de Responsabilidad

4.3.6.1. La responsabilidad de Microsystem S.A. frente a las partes involucradas en relación al incumplimiento de sus obligaciones y responsabilidades y en cualquier otro asunto relacionado con los servicios prestados, no excederá en caso alguno al precio total del servicio de certificación contratado excluyendo valores correspondientes a los dispositivos criptográficos.

4.3.6.2. La responsabilidad de Microsystem S.A. está limitada frente a hechos fortuitos y fuerza mayor según descrito en el punto Casos de Fuerza Mayor y Caso Fortuito

4.3.7. Difusión de Información Pública Vigente

Dentro de las responsabilidades de Microsystem S.A., se incluye la publicación oportuna en su sitio web de archivos con información de acceso público correspondiente a las prácticas y políticas involucradas en su actividad como PSC, y el estado de los certificados emitidos. Dicha información se debe encontrar disponible de manera continua en el sitio web para el libre acceso de las partes interesadas.

4.3.7.1. Archivos sujetos a publicación frecuente o periódica

4.3.7.1.1. Glosa: Lista de Certificados Revocados de Titulares
Dirección: http://crl.ca.msys.cl/Microsystem_Firma_Electronica_Avanzada_-_P1.crl
Frecuencia actualización: Cada 24h

4.3.7.1.2. Glosa: Lista de Certificados Revocados de Autoridades Intermedias
Dirección: http://crl.ca.msys.cl/Microsystem_Root_CA_-_P1.crl
Frecuencia actualización: Cada 6 meses

4.3.7.1.3. Glosa: Consulta individual de estado de certificados emitidos
Dirección: https://portal.ca.msys.cl/ - apartado **Búsqueda de Certificados Emitidos**
Frecuencia actualización: Inmediata según cambio de un estado de cualquier certificado de Titulares

4.3.7.2. Archivos sujetos a publicación esporádica según sufran cambios

4.3.7.2.1. Certificado Raíz y certificado de la Autoridad Intermedia de FEA de Microsystem S.A.
Dirección: https://portal.ca.msys.cl/confianza/

4.3.7.2.2. Documentación de Políticas y Prácticas de Certificación, Privacidad, Protección de Derechos de Usuarios
Dirección: https://portal.ca.msys.cl/documentacion/

4.3.7.2.3. Resoluciones de la Entidad Acreditadora que conciernen PSC Microsystem S.A.
Dirección: https://portal.ca.msys.cl/resoluciones/

4.3.7.2.4. Utilitarios y drivers
Dirección: https://portal.ca.msys.cl/ - apartado **Descarga de Drivers y Aplicativos**

4.3.7.2.5. Información de Productos y Servicios con sus tarifas vigentes
Dirección: https://portal.ca.msys.cl/ - apartado **Productos y Servicios**

4.4. Auditorías u Otras Evaluaciones como herramientas de control de cumplimiento

Con el fin de velar por el correcto uso de los recursos y activos, tanto lógicos cómo físicos, y el correcto funcionamiento de los procesos y servicios del PSC, Microsystem S.A. integra las actividades en su rol de PSC con la Certificación ISO 27001:2013 de Microsystem S.A. como empresa integral.

Dado lo anterior, Microsystem S.A. se somete a tres tipos de auditorías para velar por el cumplimiento de la normativa ISO mencionada en el párrafo anterior y a las políticas y prácticas vigentes del PSC y la concordancia de estas con la normativa vigente, realizando los ajustes necesarios para rectificar las observaciones e irregularidades detectadas en todos los procesos de evaluación.

4.4.1. Auditorias ISO 27001

Con la finalidad de resguardar la seguridad física, técnica, y operacional de la información, y en particular de la PSC, Microsystem S.A. tiene vigente una certificación ISO 27001 desde 2015, y asume la responsabilidad de mantenerla vigente al menos durante el periodo en el que cumpla el rol de Entidad Certificadora. Para ello se realizan de forma anual una auditoría interna y una auditoría externa.

4.4.1.1. Auditoría Interna

Para dicha auditoría se contrata una empresa externa con personal calificado y sin ningún tipo de relación con Microsystem S.A., para auditar a la empresa. en la norma ISO 27001:2013.

4.4.1.2. Auditoría Externa

Microsystem S.A se somete a auditorías anuales realizadas por la empresa SGS, Proveedor de Servicios de Certificación ISO 27001, quien revisa y valida que se cumplan los requisitos de la norma ISO en cuestión y acreditan a Microsystem S.A. en dicha norma. Luego del periodo que dura la certificación, se realizará un proceso de re-certificación para validar la mantención de los estándares de seguridad declarados por Microsystem S.A.

4.4.2. Auditorías Internas PSC

Microsystem S.A. en su rol de PSC acreditado, realiza auditorías internas anuales para verificar que se cumplan los siguientes aspectos:

4.4.2.1. Disponibilidad de PC, DPC, Políticas de Privacidad, Derechos de los Usuarios, datos de contacto debidamente actualizados y registro de certificados emitidos en el sitio web https://portal.ca.msys.cl/

4.4.2.2. Cumplimiento de los procesos del ciclo de vida de los certificados de FEA.

4.4.2.3. Cumplimiento de la disponibilidad de los servicios CRL y OCSP.

4.4.2.4. Revisión de la vigencia de los procedimientos frente a contingencias y continuidad operacional.

4.4.2.5. Integridad de las llaves y los certificados de la Autoridad Certificadora.

4.4.2.6. Control de acceso a la información de los titulares.

4.4.2.7. Evaluación y cumplimiento de los niveles de seguridad física.

4.4.2.8. Evaluación y cumplimiento de los niveles de seguridad lógica y perimetral de los sistemas.

4.4.2.9. Revisión de los controles de acceso a la Base de Datos y otros repositorios de información.

Para la realización de estas auditorías, es el Comité de Seguridad quien designa a un auditor, ya sea interno o externo, con las competencias necesarias para realizar dicha evaluación. Sea cual sea la decisión del Comité, el auditor no podrá tener intereses compartidos con el proceso a auditar, velando por la objetividad del proceso de auditoría.

Posterior a la realización de la auditoría, el auditor en cuestión debe emitir un informe con las evidencias de lo auditado y los hallazgos encontrados. Este será entregado al Comité de Seguridad, quien lo elevará a la Alta Dirección para su conocimiento.

En caso de encontrar No Conformidades, Microsystem S.A. tomará todas las medidas necesarias para abordarlas y remediarlas en el corto plazo, en la medida de lo posible, asegurando el correcto funcionamiento del PSC.

4.4.3. Inspecciones Entidad Acreditadora

El Ministerio de Economía, Fomento y Turismo, por medio de la Entidad Acreditadora, en su rol de inspector, realiza inspecciones anuales y extraordinarias para corroborar el óptimo funcionamiento de Microsystem S.A. como PSC. Adicionalmente, podrá requerir de forma semestral información sobre el desarrollo de la actividad que realiza el PSC, conforme a lo dispuesto en el Art. 15° del Reglamento de la Ley N° 19.799.

4.5. Confidencialidad y Protección de Datos

4.5.1. Confidencialidad de la información de los Solicitantes y Titulares

Microsystem declara que los certificados, las listas de revocación, las respuestas del servicio OCSP, y la información contenida en ellos, no es considerada información confidencial como se establece en la ley 19.799.

El Solicitante, al momento de formalizar la solicitud de certificado digital, firmará un contrato con Microsystem, en el que consentirá explícitamente el uso de datos personales entregadas al PSC en el procedimiento registro (punto Solicitud de Certificado de FEA de este documento). Microsystem es responsable de utilizar dichos datos personales únicamente con el propósito de gestionar el ciclo de vida del certificado digital. En el anexo Contrato de Suscripción de Firma Electrónica Avanzada, se muestra un modelo de solicitud que firmará el solicitante.

4.5.2. Confidencialidad de las llaves privadas de la jerarquía de la AC de la Firma Electrónica Avanzada

Las llaves privadas correspondientes a los certificados de la jerarquía de la Autoridad Certificadora de la Firma Electrónica Avanzada, son generadas a través de un dispositivo HSM, el cual las genera, almacena y utiliza mediante mecanismos que cumplen con el estándar FIPS 140-2 nivel 3 y bajo exclusivo control del personal autorizado de Microsystem S.A. con múltiples niveles de control de acceso físico y lógico. Esto garantiza que las llaves privadas se traten en forma confidencial.

4.5.3. Confidencialidad de las llaves privadas de Titulares de la Firma Electrónica Avanzada

La llave privada correspondiente al certificado personal de Firma Electrónica Avanzada de un Titular, es gestionada a través de un dispositivo criptográfico, el cual las genera, almacena y utiliza mediante mecanismos que cumplen con el estándar FIPS 140-2 nivel 3, garantizando exclusivo control de las llaves privadas por parte del Titular de la firma. Esto garantiza que las llaves privadas se traten en forma confidencial.

4.5.4. Reserva de la Información en la Prestación de Servicios de Certificación

Tanto la PSC como la AR mantendrán la más rigurosa reserva de toda información recibida por parte de los Solicitantes y Titulares de Certificados, siempre que la publicación o comunicación a terceros de dicha información sea necesaria para la correcta prestación de los servicios de certificación. El PSC entregará información de los Titulares (siempre dentro del margen de la ley Nº 19.799) al Titular del certificado o a solicitud de tribunales para procedimientos judiciales.

4.5.5. Protección de Datos

Microsystem S.A. deja constancia de la existencia de una base de datos con la información obtenida en los procesos de solicitud y registros de los solicitantes a los servicios de certificación, según se declara en las políticas de certificación. La responsabilidad de la base de datos recae directamente sobre Microsystem S.A. o cualquier entidad que la subrogue para llevar a cabo la gestión y prestación de servicios de certificación.

4.5.6. Información de utilidad pública

Microsystem declara que los certificados, las listas de revocación, las respuestas del servicio OCSP, y la información contenida en ellos no es considerada información confidencial, como se establece en la ley 19.799.

4.6. Derecho de Propiedad Intelectual

Microsystem S.A. es el Titular de los derechos de la propiedad intelectual de los servicios de certificación de Firma Electrónica Avanzada, incluyendo contenido de las páginas web (https://portal.ca.msys.cl/) y programas desarrollados por o para Microsystem S.A., los certificados, las marcas comerciales utilizadas en la prestación de los servicios de certificación y la presente DPC. Los certificados, las CRL y las respuestas OCSP son propiedad de Microsystem S.A., no obstante Microsystem S.A. autoriza la reproducción y distribución de los certificados, las respuestas OCSP y las CRL, de forma no exclusiva y libre de derechos, siempre que se reproduzcan y distribuyan en forma íntegra. Las llaves privadas y públicas son propiedad de los Titulares que las poseen legítimamente.

De lo anterior se excluyen aquellos archivos descargables (drivers, programas, etc.) publicados en la página web (https://portal.ca.msys.cl/) que no son propiedad de Microsystem S.A., por lo que son de exclusiva propiedad intelectual de sus creadores y se rigen por sus derechos intelectuales.

4.7. Uso del Certificado de FEA

Los certificados emitidos por Microsystem S.A. sólo pueden usarse para los fines que se enumeran a continuación, y cualquier otro uso queda estrictamente prohibido:

4.7.1. Garantía de integridad y evidencia de autoría

El certificado electrónico de Microsystem S.A. se puede utilizar para transacciones electrónicas específicas, que admiten la Firma Electrónica Avanzada, tales como formularios electrónicos, documentos electrónicos, correo electrónico, etc. Las principales funciones de una Firma Electrónica Avanzada son garantizar el no repudio y la integridad de las transacciones electrónicas firmadas. El certificado de firma sólo está garantizado para producir firmas electrónicas en el contexto de las aplicaciones que admiten certificados digitales. Los certificados

de Firma Electrónica Avanzada de Microsystem S.A. son apropiados para firmas electrónicas tomando en consideración a la Ley 19.799 Sobre Documentos Electronicos, Firma Electronica y Servicios de Certificación de dicha Firma.

4.7.2. Autenticación de usuarios

Los certificados electrónicos de FEA de Microsystem S.A. se pueden usar para operaciones de autenticación electrónica específicas de acceso a sitios web y otros servicios en línea, correo electrónico, etc. La función de autenticación de un certificado digital se puede determinar en cualquier contexto de transacción con el fin de verificar la identidad del usuario titular de un certificado digital.

4.7.3. Confidencialidad

Los certificados electrónicos de Microsystem S.A. se pueden utilizar para garantizar la confidencialidad de las comunicaciones electrónicas mediante algoritmos de encriptación compatibles. Todos los certificados de Microsystem S.A. son apropiados para la confidencialidad.

4.7.4. Usos prohibidos

Está prohibido cualquier otro uso de un certificado de Firma Electrónica Avanzada emitido por Microsystem S.A. que no sea compatible con la correspondiente política de certificación, **ME-DG-PO01 Políticas de Certificación de Firma Electrónica Avanzada**.

5. Identificación y Autenticación

5.1. Autenticación de la Identidad del Solicitante

5.1.1. El PSC, como Autoridad de Registro, verifica de forma fehaciente la identidad del Solicitante mediante una cita presencial, solicitud de visita en terreno o emisión en línea para la realización de la solicitud y posterior emisión del certificado de FEA, en base a lo establecido en la **ME-DG-PO01 Políticas de Certificación de Firma Electrónica Avanzada**.

5.1.2. El PSC, como Autoridad de Registro, verifica la validez y vigencia de los documentos, datos y atributos entregados por el Solicitante, en el punto anterior, para la emisión del certificado de FEA, dando su aprobación o rechazo a la continuidad del proceso, tal como se indica en el punto Solicitud de Certificado FEA.

5.1.3. Microsystem S.A. se reserva el derecho de no emitir el certificado de Firma Electrónica Avanzada a un Solicitante si considera que la evidencia presentada por este último no es suficiente para comprobar la autenticidad de lo solicitado en los párrafos anteriores.

5.2. Control de la Llave Privada

Ídem Confidencialidad de las llaves privadas de Titulares de la Firma Electrónica Avanzada.

5.3. Identificación y Autenticación para gestionar el ciclo de vida de certificado de FEA

5.3.1. Para re-emisión de llaves.
Microsystem S.A. no ofrece reemisión de llaves.

5.3.2. Para suspensión de Certificados de FEA
Ídem Suspensión y Revocación de Certificados de FEA

5.3.3. Para revocación de Certificados de FEA
Ídem Suspensión y Revocación de Certificados de FEA

5.3.4. Para renovación
Ídem Renovación y Renovación de un certificado revocado

6. Ciclo de Vida del Certificado de FEA

6.1. Solicitud de Certificado de FEA

Para realizar la solicitud de un certificado de FEA, el solicitante puede realizarlos a través de formulario habilitado por Microsystem S.A en su página web https://www.microsystem.cl/firma-electronica-digital-avanzada/. Las modalidades de registro son:

Presencial en las oficinas del PSC, donde el solicitante podrá acudir a las oficinas del PSC a realizar el proceso de registro.

Presencial en terreno en domicilio del solicitante, donde el solicitante podrá realizar un agendamiento para que el proceso de registro se realice en su domicilio, pudiendo ser este su domicilio particular (casa o departamento) o su domicilio laboral (oficina).

En línea donde el Solicitante realiza el proceso de registro, y verificación fehaciente de su identidad en línea a través del sistema ClaveÚnica y un mecanismo complementario.

6.1.1. Registro Presencial en las Oficinas del PSC

6.1.1.1. El Solicitante inicia el proceso de registro realizando agendamiento de la visita en oficina del PSC a través del formulario habilitado por Microsystem y proporciona la siguiente información: Nombre, Apellido, Email, Teléfono, Empresa, Cargo y detalle de la solicitud.

6.1.1.2. El Solicitante se deberá presentar en las oficinas del PSC el día y hora acordados.

6.1.1.3. El Operador de Registro inicia el proceso conectándose a la plataforma de la Autoridad de Registro a través de VPN securitizada con un token criptográfico personal del operador, a través de la red y notebook corporativo, y procede a capturar los datos de la cédula de identidad del Solicitante mediante lectura digital (en caso de las cédulas electrónicas) o ingreso manual (para cédulas no electrónicas), a continuación captura las imágenes de la cédula por ambos lados y comprueba fehacientemente la identidad del solicitante verificando su nombre contra los datos capturados desde la cédula.

6.1.1.4. El Solicitante concurre ante la Autoridad de Registro de Microsystem S.A., para solicitar la emisión de certificado de Firma Electrónica Avanzada, presentando su cédula de identidad vigente. En el proceso de registro participan un Operador de Registro y un Operador de Validación.

6.1.1.5. El Operador de Registro procede a capturar los datos de la cédula de identidad del Solicitante mediante lectura digital (en caso de las cédulas electrónicas) o ingreso manual (para cédulas no electrónicas), a continuación captura las imágenes de la cédula por ambos lados y comprueba fehacientemente la identidad del solicitante verificando su nombre contra los datos capturados desde la cédula.

6.1.1.6. El Operador de Registro le solicita al usuario sus datos del domicilio actual.

6.1.1.7. El Operador de Registro valida la vigencia del documento en el SRCeI y adjunta la evidencia a la solicitud.

6.1.1.8. En el caso que el Solicitante cuente con un dispositivo criptográfico propio, este le facilita el dispositivo correspondiente al Operador de Registro, quien lo conecta a su estación de trabajo y revisa con el utilitario del fabricante para asegurar que el dispositivo sea un modelo certificado **FIPS 140-2 Level 3** y que este no tenga datos preexistentes. La evidencia de lo realizado se guarda en el registro asociado con la solicitud. En el caso que el Solicitante no tenga un dispositivo, el Operador de Registro le asigna uno del stock disponible: 1 dispositivo nuevo y en conformidad a la normativa. El valor de un dispositivo nuevo se cobra adicionalmente al valor correspondiente al servicio de certificación.

6.1.1.9. Si los datos capturados y la cédula del solicitante son correctos, el Solicitante debe firmar un contrato de suscripción del certificado de Firma Electrónica Avanzada que incluye el consentimiento para el tratamiento de sus datos por parte de la Autoridad Certificadora. Realiza su firma de puño y letra y adicionalmente imprime su huella dactilar en el mismo documento.

6.1.1.10. El Operador de Registro procede con la captura de la fotografía (retrato) del Solicitante.

6.1.1.11. La información de la solicitud es validada verbalmente con el Solicitante.

6.1.1.12. El Operador de Registro requiere al Solicitante verificar que el correo electrónico y el teléfono móvil indicados en la solicitud, sean correctos, mediante el envío de códigos de validación por ambas vías, para asegurar futuras comunicaciones.

6.1.1.13. Un Operador de Validación revisa fehacientemente la solicitud comprobando la veracidad de los datos. Siendo correcta la información entregada, se autoriza la emisión del certificado.

6.1.1.14. La La Autoridad Certificadora le envía al solicitante, mientras este encuentra en las dependencias del PSC, 2 factores que permiten la instalación del certificado en su dispositivo de seguridad. Estos factores son enviados a los medios de contacto que el solicitante declaró durante el proceso de registro, validados según el punto 6.1.1.12, y que se encuentran en control exclusivo del este mismo. Los factores que permiten la instalación de describen a continuación:

6.1.1.14.1. Factor 1: Un mensaje SMS con clave de ingreso al Portal de Usuario Suscriptor de Firma Electrónica Avanzada.

6.1.1.14.2. Factor 2: Una notificación mediante correo electrónico, en este se notifica que el certificado de firma electrónica avanzada se encuentra disponible para instalación. Adicionalmente el correo electrónico contiene un adjunto cifrado que contiene la clave de instalación del certificado; para descifrar el adjunto el usuario debe utilizar la clave entregada en el Factor 1 mencionado en el punto anterior.

6.1.1.15. En presencia del Operador de Registro, si el dispositivo criptográfico elegido por el Solicitante es nuevo, el Solicitante realiza su inicialización y crea una clave secreta de acceso exclusivo del dispositivo para proteger su Firma Electrónica Avanzada y tener el control absoluto de esta. Se entiende, que si el dispositivo no es nuevo, el Solicitante ya tiene un control exclusivo de éste, según estipulado en el punto Obligaciones del Titular.

6.1.1.16. En presencia del Operador de Registro, mediante el Portal de Usuario de Firma Electrónica Avanzada, utilizando los Factores (Del Punto 6.1.1.14) y la clave personal del dispositivo criptográfico en poder exlusivo del titular, el Solicitante realiza la generación de su llave privada e instalación del certificado de la Firma Electrónica Avanzada en su dispositivo criptográfico. Mediante este acto el Solicitante se transforma en el Usuario Titular.

6.1.1.17. El Usuario Titular firma, de puño y letra, un comprobante de recepción de su dispositivo criptográfico con su certificado de Firma Electrónica Avanzada dentro.

6.1.2. Registro Presencial en Terreno en Domicilio del Solicitante

6.1.2.1. Agendamiento y Solicitud

6.1.2.1.1. El Solicitante inicia el proceso de registro agendando una visita en terreno a través del formulario habilitado por Microsystem S.A en su página web https://www.microsystem.cl/firma-electronica-digital-avanzada/.

6.1.2.1.2. Independiente del canal el Solicitante proporciona la siguiente información: RUN, número de serie de la cédula de identidad, nombre completo, domicilio donde se realizará el registro, correo electrónico, teléfono móvil, adjunta una

copia digital de su cédula de identidad por ambos lados, y selecciona los años de vigencia con los que solicitará el certificado y si adquiere un etoken o tendrá uno propio en el proceso de registro.

6.1.2.1.3. La Autoridad de Registro verifica la validez del correo electrónico y el número de teléfono móvil proporcionados por el Solicitante mediante el envío de códigos de validación por ambas vías. Esta verificación se realiza mediante llamada telefónica, y es necesaria para asegurar futuras comunicaciones.

6.1.2.2. Preparativos antes de la Visita en Terreno:

6.1.2.2.1. El Operador de Registro recibe la solicitud y realiza las siguientes comprobaciones antes de la visita en terreno:

6.1.2.2.1.1. Verifica la cédula de identidad:

6.1.2.2.1.1.1. Valida la vigencia del documento de identidad del Solicitante en el Sistema de Registro Civil e Identificación (SRCeI) y adjunta la evidencia a la solicitud.

6.1.2.2.1.1.2. Registra y valida los datos desde la cédula de identidad del solicitante en la solicitud.

6.1.2.2.1.1.3. Prepara el contrato de suscripción para que el Solicitante lo firme durante la visita en terreno.

6.1.2.3. Visita en Terreno:

6.1.2.3.1. El Solicitante debe recibir al personal de Microsystem, quien portará una Credencial de Presentación que lo identifica como Operador de Registro del PSC, en Domicilio del Solicitante, pudiendo ser su Domicilio Personal (Casa o Departamento) o su Domicilio Laboral (Oficina), en la hora y día acordado.

6.1.2.3.2. Durante el proceso de registro, el Operador de Registro inicia el proceso conectándose a la plataforma de la Autoridad de Registro a través de VPN securitizada con un token criptográfico personal del operador, a través de la conexión de su teléfono móvil y notebook corporativos, y luego procede a capturar los datos de la cédula de identidad del Solicitante, correspondiente al mismo RUN y número de serie proporcionados en la solicitud de agendamiento. Los datos se capturan mediante lectura digital en caso de cédulas electrónicas. En caso de cédulas no electrónicas valida con el solicitante los datos ingresados previamente durante la preparación de su visita.

6.1.2.3.3. En caso de que el Solicitante cuente con un dispositivo criptográfico propio, se procede a conectarlo a la estación de trabajo del Operador de Registro. Se verifica con el utilitario del fabricante que el dispositivo cumpla con el estándar

certificado FIPS 140-2 Level 3 y que no contenga datos preexistentes ajenos al Solicitante. Se guarda evidencia de esta revisión en el registro asociado con la solicitud. Si el Solicitante no posee un dispositivo criptográfico, se le asigna uno nuevo del stock disponible, en conformidad con la normativa. El costo de este dispositivo se cobra adicionalmente al servicio de certificación.

6.1.2.3.4. Si los datos capturados o ingresados de la cédula y la información del Solicitante son correctos, se procede a firmar el contrato de suscripción del certificado de Firma Electrónica Avanzada. En este documento, el Solicitante otorga su consentimiento para el tratamiento de sus datos por parte de la Autoridad Certificadora. Además, el Solicitante realiza su firma de puño y letra e imprime su huella dactilar en el mismo contrato.

6.1.2.3.5. El Operador de Registro procede con la captura de la fotografía (retrato) del Solicitante.

6.1.2.4. Validación de Datos y Autorización:

6.1.2.4.1. El Operador de Registro valida verbalmente con el Solicitante la información de la solicitud.

6.1.2.4.2. Luego, un Operador de Validación, operando remotamente, recibe la solicitud en la Plataforma de la Autoridad de Registro, revisa la solicitud, y comprueba la veracidad de los datos proporcionados, verificando fehacientemente la identidad del Solicitante. Si la información es correcta y no hay inconvenientes, se autoriza la emisión del certificado de Firma Electrónica Avanzada.

6.1.2.5. Envío de Instrucciones al Solicitante:

6.1.2.5.1. La Autoridad Certificadora envía al Solicitante, las instrucciones necesarias para completar el proceso: a) Un mensaje SMS con una clave de ingreso al Portal de Usuario Suscriptor de Firma Electrónica Avanzada. b) Una notificación de la disponibilidad de la emisión del certificado a través de un adjunto encriptado (con la clave correspondiente).

6.1.2.6. Inicialización y Generación de Claves:

6.1.2.6.1. En presencia del Operador de Registro, si el dispositivo criptográfico elegido por el Solicitante es nuevo, el Solicitante realiza su inicialización. Durante este proceso, se crea una clave secreta del dispositivo para proteger la Firma Electrónica Avanzada y asegurar el control exclusivo del titular. Si el dispositivo no es nuevo, se entiende que el Solicitante ya tiene control exclusivo de éste, según lo estipulado en el apartado Obligaciones del Titular.

6.1.2.7. Generación de Llave Privada e Instalación del Certificado:

6.1.2.7.1. En presencia del Operador de Registro, el usuario recibe 2 factores de instalación de certificado en su dispositivo de seguridad a los medios de contacto en control exclusivo del usuario Solicitante, validados al inicio del registro:

6.1.2.7.1.1. Factor 1: Un mensaje SMS con clave de ingreso al Portal de Usuario Suscriptor de Firma Electrónica Avanzada.

6.1.2.7.1.2. Factor 2: Una notificación mediante correo electrónico, en este se notifica que el certificado de firma electrónica avanzada se encuentra disponible para instalación. Adicionalmente el correo electrónico contiene un adjunto cifrado que contiene la clave de instalación del certificado; para descifrar el adjunto el usuario debe utilizar la clave entregada en el Factor 1 mencionado en el punto anterior.

6.1.2.7.2. El Solicitante utilizando las claves proporcionadas en el punto 6.1.2.7.1 y la clave del dispositivo criptográfico en control absoluto del solicitante, realiza la generación de su llave privada e instala el certificado de la Firma Electrónica Avanzada en su dispositivo criptográfico.

6.1.2.7.3. Mediante este acto, el Solicitante se transforma en el Usuario Titular de la Firma Electrónica Avanzada.

6.1.2.8. Comprobante de Recepción:

6.1.2.8.1. El Usuario Titular firma, de puño y letra un comprobante de recepción de su dispositivo criptográfico con su certificado de Firma Electrónica Avanzada dentro.

6.1.3. Registro en Línea a través del Sistema ClaveÚnica.

6.1.3.1. El Solicitante deberá ingresar al sitio principal de Microsystem S.A. (https://www.microsystem.cl/firma-electronica-digital-avanzada/) donde podrá elegir la suscripción de la Firma Electrónica Avanzada mediante un Registro en Línea.

6.1.3.2. Al elegir la opción de suscripción de FEA mediante un Registro en Línea, el Solicitante será redirigido a la plataforma del Portal de Usuario de la Firma Electrónica Avanzada de Microsystem S. A.

6.1.3.3. Para realizar el Registro en Línea el Portal de Usuario utiliza 2 componentes, para ir registrando el estado de avance del Solicitante en éste proceso: Operador Virtual de Registro y Operador Virtual de Validación.

6.1.3.4. El proceso empieza con el Operador Virtual de Registro:

6.1.3.4.1. Al inicio se aplica un captcha para impedir el ingreso de robots.

6.1.3.4.2. Luego, para ejecutar un registro de datos iniciales del Solicitante y comprobar su identidad, el Solicitante es derivado a la página del sistema ClaveÚnica donde, la autenticación correcta al sistema ClaveÚnica, es reconocido como medio de comprobación fehaciente de la identidad del solicitante. Ésta operación le entrega al Operador Virtual de Registro el RUN y los nombres y apellidos completos del Solicitante.

6.1.3.4.3. Para completar los datos, el Operador Virtual de Registro le solicita al Solicitante los siguientes datos adicionales:

6.1.3.4.3.1. correo electrónico del Solicitante - para ser grabado en el certificado y para futuras notificaciones

6.1.3.4.3.2. número de teléfono móvil del Solicitante - para ser utilizado para la entrega del segundo factor de seguridad.

6.1.3.4.3.3. número de serie de una Cédula de Identidad - para validar que la cédula de identidad del solicitante está vigente.

6.1.3.4.3.4. Fecha de nacimiento.

6.1.3.4.3.5. código de convenio (Opcional) – para validar si tiene un código de convenio vigente que define la vigencia del certificado y define una tarifa rebajada para el precio del mismo.

6.1.3.4.4. El usuario selecciona la vigencia del certificado, en caso de que ésta no haya sido definida por con un Código de Convenio.

6.1.3.4.5. El Operador Virtual de Registro procede a verificar que el correo electrónico y el teléfono móvil indicados en la solicitud sean correctos, mediante el envío de códigos OTP al correo electrónico y SMS al teléfono móvil de contacto declarados por el solicitante, para asegurar futuras comunicaciones.

6.1.3.5. Siendo exitosa la primera parte del proceso, este continúa con el Operador Virtual de Validación, que realiza las siguientes validaciones:

6.1.3.5.1. A continuación el Solicitante deberá seleccionar el mecanismo complementario digital de comprobación de identidad:

6.1.3.5.1.1. Pago del importe del servicio, indicado en https://www.microsystem.cl/firma-electronica-digital-avanzada/ por la emisión de un certificado en línea, o tarifa rebajada si tuviese un código de convenio vigente con Microsystem S.A, mediante plataforma Khipu con una cuenta bancaria perteneciente al Solicitante.

6.1.3.5.1.1.1. El Solicitante deberá confirmar la vigencia del certificado en caso de no contar con un Convenio que la defina y mediante la plataforma Khipu realizar el pago indicado mediante una cuenta bancaria registrada a su nombre, quedando registrado si el pago fue correcto (Dando origen a una verificación correcta) o fue incorrecto (Interrumpiendo el proceso de emisión).

6.1.3.5.1.1.2. Si el Solicitante desiste en pasos posteriores la emisión del certificado en línea deberá contactar a soportepki@microsystem.cl para iniciar el proceso de reembolso del importe pagado, en caso de existir un pago, el cual será atendido en un plazo de 7 días hábiles.

6.1.3.5.2. El sistema valida la vigencia de la Cédula de Identidad utilizando el número de serie del documento proporcionado por el Solicitante.

6.1.3.5.3. Siendo correcta toda la información entregada por el Solicitante, se autoriza la emisión del certificado.

6.1.3.5.4. Al validar la identidad del Solicitante se le pide creación del PIN del Certificado de su Firma Electrónica Avanzada. Este PIN es personal e intransferible y no podrá ser olvidado por el Usuario.

6.1.3.5.5. Finalizado el proceso de registro y validación el Solicitante es derivado al Portal de Suscriptor de Firma Digital donde puede revisar sus suscripciones de Firma Electrónica Avanzada de Microsystem S.A. e instalar su certificado de FEA en línea en el Cloud Signer.

6.1.3.5.5.1. Si este será el primer ingreso del Solicitante al Portal de Suscriptor de Firma Digital, recibirá un mensaje SMS con la clave inicial.

6.1.3.5.5.2. El Solicitante puede proceder a instalar su FEA en el almacenamiento seguro en línea utilizando el servicio Cloud Signer de Microsystem S.A. Este servicio utiliza un módulo criptográfico certificado y operado bajo la norma FIPS 140-2 Level 3 para gestionar las llaves privadas de sus suscriptores. Todas las llaves privadas de Cloud Signer están protegidas mediante llaves de cifrado maestras, resguardadas por una partición dedicada. Cada llave privada de un suscriptor está protegida adicionalmente por el PIN del Certificado controlado por su titular.

6.1.3.5.5.3. Durante la instalación de la FEA se le solicita al Solicitante el PIN del Certificado y un segundo factor de seguridad enviado vía SMS al teléfono móvil del usuario.

6.1.3.5.5.3.1. El PIN del Certificado definido también será utilizado como el PIN de Firma del usuario. Cada acto de firma que el usuario realice utilizando su Certificado de Firma Electrónica Avanzada, almacenado en el servicio Cloud Signer de Microsystem S.A.,

requerirá el ingreso de dicho PIN de Firma, además de un segundo factor de seguridad consistente en una Clave OTP enviada vía SMS al número de teléfono móvil registrado por el usuario durante el proceso de registro y emisión del certificado.

6.1.3.5.6. Al realizar la instalación de la Firma Electrónica Avanzada en el dispositivo criptográfico, el Solicitante se transforma en el Usuario Titular.

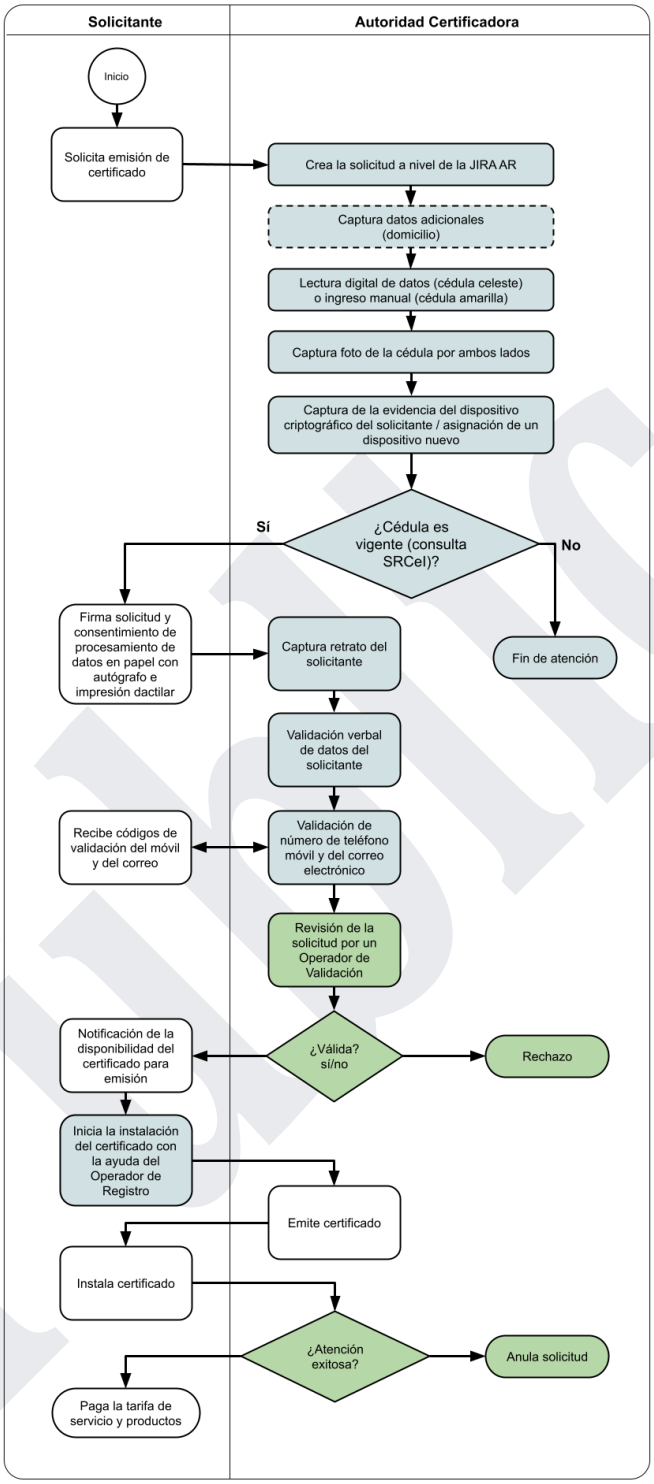


Diagrama Registro Presencial en las Oficinas del PSC y Registro Presencial en Terreno en Domicilio del Solicitante .

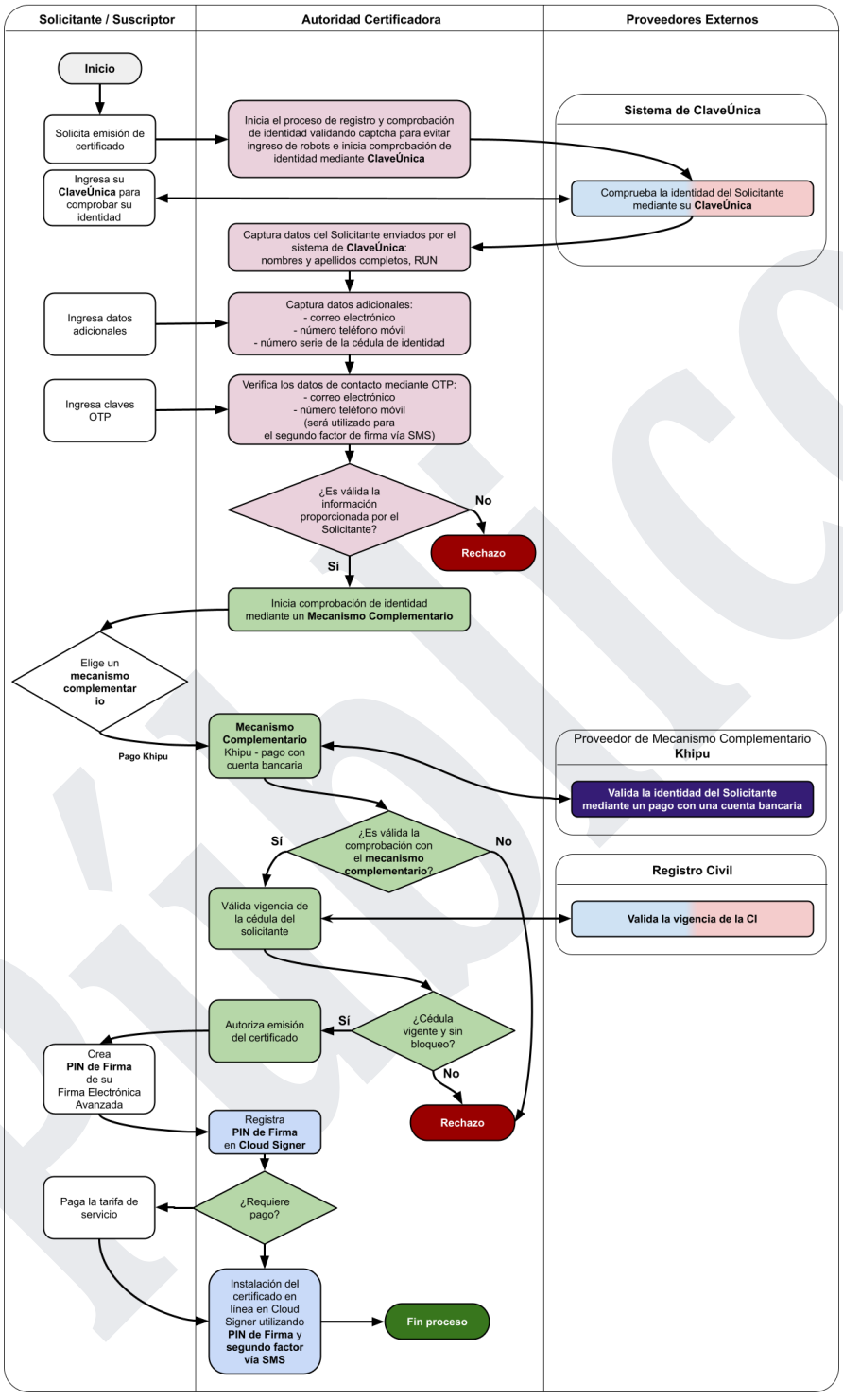


Diagrama Registro en Línea a través de Sistema ClaveÚnica.

6.2. Emisión de Certificado de FEA

Un certificado de Firma Electrónica Avanzada nace una vez queda aprobada una solicitud de suscripción de Firma Electrónica Avanzada, posterior a un procedimiento de registro que ejecuta una fehaciente validación de la identidad del Solicitante, descrito en el apartado Solicitud de Certificado de FEA, del presente documento. La emisión se realiza a través del Portal de Usuario de Firma Electrónica Avanzada. Para esto, se requieren: clave del portal (descrita para Registro Presencial en las Oficinas del PSC 6.1.1.14.1 y Registro Presencial en Terreno en Domicilio del Solicitante en el punto 6.1.2.7.1.1) y clave de instalación del certificado (descrita para Registro Presencial en las Oficinas del PSC 6.1.1.14.2 y Registro Presencial en Terreno en Domicilio del Solicitante en el punto 6.1.2.7.1.2).

6.3. Periodo de Vigencia

El periodo de vigencia está delimitado por las fechas de emisión y expiración, excluyendo los períodos de suspensión y revocación. Durante el periodo de vigencia, el certificado y su llave privada pueden ser utilizados para cualquier uso autorizado. Los certificados de Microsystem S.A. pueden tener una vigencia de 1, 2 o 3 años, según lo indicado por el solicitante en el momento de contratar el servicio, desde la fecha de emisión. Además, se conceden **15 días adicionales a la vigencia** para que el solicitante pueda gestionar la renovación del certificado.

6.4. Suspensión y Revocación de Certificados de FEA

6.4.1. **Suspensión** - si un Titular pierde temporalmente el control de su llave privada puede solicitar una suspensión temporal del certificado de Firma Electrónica Avanzada para evitar que se realicen actividades acreditadas por éste sin su consentimiento. Durante el periodo de la suspensión los servicios OCSP y CRL responderán que el certificado está suspendido. La suspensión puede ser solicitada exclusivamente por el Titular en base a lo siguiente:

6.4.1.1. Mediante cualquier medio de comunicación informado por la Autoridad Certificadora en su Portal de Usuario de Firma Electrónica Avanzada indicando un número de serie de una cédula personal vigente.

6.4.1.2. Mediante una acción de suspensión disponible en el **Portal de Usuario de Firma Electrónica Avanzada,** ingresando con sus credenciales de acceso y el envío de una clave OTP enviada a su correo electrónico. .

6.4.1.3. **La reactivación** se puede realizar exclusivamente mediante el **Portal de Usuario de Firma Electrónica Avanzada,** ingresando con sus credenciales de acceso.

6.4.2. **Revocación** - si un Titular pierde el control de su llave privada de manera irrecuperable debe informar a la Autoridad Certificadora del suceso para revocar el certificado correspondiente. Revocación puede ser solicitada por el Titular:

6.4.2.1. Mediante cualquier medio de comunicación autorizado por la Autoridad Certificadora indicando el código de revocación recibido al final del procedimiento de instalación del certificado.

6.4.2.2. Mediante una acción de revocación disponible en el **Portal de Usuario de Firma Electrónica Avanzada,** ingresando con sus credenciales de acceso y el envío de una clave OTP enviada a su correo electrónico. Para realizar el proceso de revocación, el usuario deberá seleccionar el certificado que desea revocar. Posteriormente, será necesario ingresar la clave de revocación, la cual fue enviada por correo electrónico tras completar el proceso de activación del certificado. Cabe destacar que el documento con la clave de revocación se puede abrir exclusivamente con el token y llave privada del mismo certificado. Es esencial que el documento sea abierto e impreso al recibirlo después de activar el certificado para resguardar la copia impresa en un lugar seguro para tenerla disponible cuando sea necesario revocar el certificado.

6.4.3. **Revocación por fallecimiento del Titular** - puede ser solicitada por cualquier persona que cuente con un certificado de defunción del Titular.

6.4.4. **Revocación por incumplimiento de las obligaciones** - puede ser realizada por la Autoridad Certificadora en base a los antecedentes que el Titular ha incumplido con las políticas del uso del certificado digital.

6.4.5. **Revocación por orden judicial o administrativa** - puede ser realizada por la Autoridad Certificadora desde la administración de registros.

6.4.6. **Revocación por cese de actividades de la Autoridad Certificadora de Microsystem S.A.**

6.5. Cambio de datos grabados en el certificado

Un Titular tiene derecho a realizar solo un proceso de cambio de datos por motivo de cambio de nombre y/o apellido legal, mientras dure la vigencia del certificado adquirido (siempre y cuando no sea un certificado gratuito), en aquel caso se revoca el certificado actual y se procede con el registro para emitir un nuevo certificado gratuito, con datos rectificados, con vigencia (1, 2 o 3 años) suficiente para cubrir el periodo restante de vigencia del certificado revocado.

Los certificados gratuitos están sujetos sólo a una revocación en caso de informar invalidez o cambio de los datos contenidos.

6.6. Renovación

Se procede con una solicitud y registro igual como para un certificado nuevo.

6.7. Renovación de un Certificado Revocado

Se procede con una solicitud y registro igual como para un certificado nuevo.

6.8. Expiración

Una vez cumplido el periodo de vigencia de un certificado éste de manera natural pierde validez para cualquier uso autorizado.

6.9. Homologación o Traspaso de Certificado de otro PSC

El PSC Microsystem S.A. no realiza traspasos u homologaciones de certificados provenientes de otros PSC. Sin perjuicio de lo anterior, cualquier persona que cumpla con los requisitos del PSC Microsystem S.A., podrá solicitar un nuevo certificado.

6.10. Limitaciones, Prohibiciones y uso no Autorizado

Los certificados del PSC Microsystem S.A., no han sido diseñados y destinados para ser utilizados como elementos de control de situaciones peligrosas o para usos donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Está expresamente prohibido cualquier otro uso de un certificado de Firma Electrónica Avanzada emitido por Microsystem S.A. que no sea compatible con esta Política, la Declaración de Prácticas de Certificación correspondiente, la normativa chilena y los convenios internacionales ratificados por Chile.

Queda expresamente prohibido a cualquiera de las partes involucradas, sea Solicitante, Titular, Partes que confían u otros, controlar, interferir, realizar ingeniería inversa, o cualquier otro acto que afecte la ejecución técnica de los sistemas, la propiedad intelectual de Microsystem S.A. y el código fuente de dicha propiedad.El PSC Microsystem S.A. no realiza traspasos u homologaciones de certificados provenientes.

7. Ciclo de vida del PSC

7.1. Inicio de actividades del PSC

Una vez obtenida la Acreditación de parte del Ministerio de Economía, Fomento y Turismo de Chile, se revocarán todos los certificados emitidos en pruebas previas a la fecha de inicio de actividades oficiales.

7.2. Procesos de auditoría de seguridad

Microsystem S.A. realiza procesos de auditoría anuales para velar por la seguridad de la información y de los sistemas que opera, bajo los parámetros de la ISO 27001, siguiendo los pasos indicados en el procedimiento interno **CG-FR-PAI Plan Auditoría Interna punto 8**.

Este procedimiento es aplicable para las inspecciones ordinarias y extraordinarias a realizar por parte de la Entidad Acreditadora a Microsystem como PSC, ya sea por medio de funcionarios o

peritos especialmente contratados y habilitados para cumplir con dicha función en los plazos establecidos en el Decreto 181 art 15.

7.3. Almacenamiento de Información Relevante

Microsystem S.A. establece que toda aquella información relacionada con la ejecución de los procesos del PSC, será almacenada por un periodo de al menos 6 años, desde la fecha de recepción o generación de dicha información.

La privacidad e integridad de la información mencionada, está garantizada por el procedimiento interno **ME-DG-PS5 Implementación del Plan de Seguridad de Sistemas** punto 15.5. que hace referencia al documento interno **OP-PR-RESP Procedimiento de Respaldo** punto 7.3 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, evidencia subidas a las APP, base de datos y configuraciones de los servicios.

7.4. Cambio de Datos de Creación de FEA

Siendo que el periodo máximo de vigencia de un certificado personal de FEA del PSC Microsystem S.A. es de 3 años y la vigencia de un certificado de Titular no puede superar a la vigencia de los certificados de la Autoridad Certificadora que los emite, la jerarquía vigente deja de emitir certificados personales a lo mínimo a 4 años antes de la fecha de expiración de la jerarquía, continuando la operación de los servicios de confianza CRL y OCSP, la jerarquía pasa al modo manutención. Para poder continuar con la emisión de los certificados personales el PSC realiza una nueva ceremonia de creación de llaves generando una nueva jerarquía vigente de certificados Raíz e Intermedio de FEA, en conformidad con la guía de acreditación y entrega los nuevos certificados de la Autoridad Certificadora a la Entidad Acreditadora. Los nuevos certificados de la Autoridad Certificadora Microsystem S.A. se publican en el sitio web https://portal.ca.msys.cl

7.5. Gestión de Incidentes y Superación de Situaciones Críticas

Microsystem S.A. declara tener un sistema de gestión de incidentes de seguridad, la operación de este está descrita en el documento interno **ME-DG-PS07 Gestión de incidentes de Seguridad de la Información**. Adicionalmente, posee un plan de contingencia en forma del procedimiento interno **ME-DG-PS03 Continuidad Operacional Orientada a la Autoridad Certificadora**.

7.6. Casos de Fuerza Mayor y Caso Fortuito

Siendo excluido del cumplimiento de las obligaciones y compromisos frente a las situaciones consideradas como casos de fuerza mayor y caso fortuito de acuerdo a lo estipulado en el art. 45°

del Código Civil de la República de Chile, Microsystem S.A. declara tener procedimientos para enfrentar tales situaciones dentro del marco del plan de contingencia (Gestión de Incidentes y Superación de Situaciones Críticas) y tomará todas las medidas necesarias para reducir la demora en la restauración de los servicios y el cumplimiento de los compromisos.

En caso de ocurrir tal situación Microsystem S.A. notificará a los Usuarios en un plazo de 5 días hábiles sobre la ocurrencia de este y sus efectos en la prestación de servicios.

7.7. Término de actividades del PSC

7.7.1. Causales

7.7.1.1. **Por decisión interna de Microsystem S.A. (cese voluntario)**

En caso de cese voluntario de término de actividades del PSC, Microsystem S.A. declara las siguientes medidas:

7.7.1.1.1. Comunicar a cada uno de los Titulares de certificados de FEA vigentes el cese de actividades del PSC, vía correo electrónico, con una antelación mínima de dos meses al cese efectivo de la actividad. Posterior al envío de la comunicación, el Titular tendrá 15 días corridos para presentar su oposición a la transferencia de los datos de su certificado a otro PSC, solicitando así la anulación de la vigencia del certificado antes mencionado. En caso de no existir oposición o nombramiento por parte del Titular terminado el plazo mencionado anteriormente, se transferirá de forma automática el certificado de FEA a otro PSC.

7.7.1.1.2. Solicitar la cancelación de la inscripción en el registro de prestadores acreditados a la Entidad Acreditadora, con antelación no inferior a un mes a la fecha de cese de actividades, y comunicar el destino de los datos de los certificados, especificando, si serán transferidos y a quién, o si los certificados quedarán sin efecto, según corresponda. Lo anterior, por medio de una carta dirigida a la Subsecretaría de Economía y Empresas de Menor Tamaño, a través de la Oficina de Partes.

7.7.1.1.3. Realizar anunció, por medio de publicación en diarios nacionales y en el portal del PSC (https://portal.ca.msys.cl/).

Lo anterior será notificado con un mínimo de 60 días previo al cese de las actividades.

7.7.1.2. **Por desacreditación (cese involuntario), en caso de incumplimiento de lo solicitado por la Entidad Acreditadora**, Microsystem S.A. declara las siguientes medidas:

7.7.1.2.1. Publicar en el portal del PSC (https://portal.ca.msys.cl/) la resolución de la Entidad Acreditadora que lo afecta.

7.7.1.2.2. Realizar anunció, por medio de publicación en diarios nacionales.

7.7.1.2.3. Comunicar de forma inmediata a cada uno de los Titulares de certificados de FEA vigentes el cese de actividades del PSC, vía correo electrónico. Posterior al envío de la comunicación, el Titular tendrá 15 días corridos para presentar

su oposición a la transferencia de los datos de su certificado a otro PSC, solicitando así la anulación de la vigencia del certificado antes mencionado. En caso de no existir oposición o nombramiento por parte del Titular terminado el plazo mencionado anteriormente, se transferirá de forma automática el certificado de FEA a otro PSC.

Lo anterior será notificado de forma inmediata al recibir la resolución de la Entidad Acreditadora.

7.7.1.3. **Otras Causales de Cese involuntario**

Microsystem S.A. informará a la Entidad Acreditadora sobre cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad como PSC. Comunicando especialmente, cuando tenga conocimiento de ello, el inicio de un procedimiento concursal de liquidación o que se encuentre en cesación de pagos.

7.7.2. Transferencia a otro PSC

En caso que los Titulares no expresen oposición a la transferencia de los datos de su certificado a otro PSC vigente, Microsystem S.A. podrá transferir las obligaciones y derechos a un PSC, existente en el registro de la Entidad Acreditadora, que tenga la disponibilidad y las condiciones para recibir la transferencia.

Si no es posible realizar lo anterior, la empresa revocará todos los certificados, 60 días posteriores al envío de la comunicación del término de las operaciones.

7.7.3. Indemnización

7.7.3.1. Los Titulares, cuyos certificados de FEA sean revocados por cese de actividades, tendrán derecho a recibir una indemnización.

7.7.3.2. En caso de indemnizaciones, por anulación de la vigencia del certificado de FEA, producto del cese de actividades del presente PSC, se indemnizará a los Titulares que presenten la información solicitada por el PSC en un plazo de 60 días corridos desde el término anticipado de la vigencia del certificado en cuestión.

7.7.3.3. Información necesaria para hacer efectivo el pago de la indemnización

7.7.3.3.1. Datos bancarios para transferencia o depósito de una cuenta perteneciente al Titular del certificado.

7.7.3.3.2. Número de serie de la Cédula de Identidad vigente del Titular.

7.7.3.4. El monto a indemnizar, será proporcional al costo del servicio, en base al total de días contra los días restantes desde el momento de la certificación, excluyendo de la indemnización el valor del dispositivo criptográfico y otros servicios complementarios tales como visita en terreno.

8. Controles de Procedimiento

Microsystem S.A. mantiene una certificación ISO 27001 vigente desde el año 2015, otorgada por la empresa de auditoría SGS Chile. Con la finalidad de resguardar la seguridad física, técnica, y

operacional de la PSC, Microsystem S.A. cuenta con una serie de procesos y definiciones gestionados bajo los principios de la norma ISO 27001.

Todos los procedimientos del PSC están diseñados para funcionar en base a múltiples roles con responsabilidad distribuida garantizando que ninguna ruta crítica de operación dependa de una sola persona.

9. Controles de Personal del PSC

El órgano más alto del PSC es el Directorio de la Empresa, que plenamente respalda toda la operación del PSC. El Directorio vela sobre los servicios del PSC delegando las responsabilidades al Gerente General que designa al Comité de Seguridad responsable de gestionar los recursos necesarios y un equipo de personas de alta confiabilidad, cada uno de los cuales tiene un rol de confianza con sus respectivas responsabilidades. El detalle de los procedimientos de la gestión del personal del PSC está estipulado en el documento **ME-DG-PS04 Plan Seguridad de Sistemas**.

9.1. Roles Existentes en los Procedimientos del PSC

9.1.1. Comité de Seguridad

9.1.1.1. El Comité de Seguridad, que opera en el marco de la certificación ISO 27001 de Microsystem, cumple también el rol de Comité de Seguridad de la AC.

9.1.1.2. El Comité de Seguridad de la Información de Microsystem S.A. asume la responsabilidad general en cuanto a la actualización e implantación de las políticas y procedimientos de seguridad que han sido aprobadas, lo que incluye:

9.1.1.2.1. Cautelar que los sitios donde se encuentran los sistemas de Microsystem S.A., cumplan con manejar adecuadamente los sistemas de protección perimetral y la correcta gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.

9.1.1.2.2. Asumir la responsabilidad de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, y otras tareas relacionadas.

9.1.1.2.3. Autorizar movimientos de material fuera de las instalaciones de la AC.

9.1.1.2.4. Efectuar la selección y determinar la contratación de terceros especialistas que puedan colaborar en la mejora de la seguridad de la AC de Microsystem S.A.

9.1.1.2.5. Delegar ciertas responsabilidades, a quienes cumplan con las condiciones necesarias para dichas funciones según procedimientos internos, disponibles en el gestor documental de Microsystem S.A., **OP-PR-OP Procedimiento de Continuidad Operacional** (apartado 9.3) y **CG-MA-PSI Política de Seguridad de la Información** (apartado 5).

9.1.1.3. Es el Comité encargado de seleccionar a los miembros que ocuparan los cargos dentro del PSC, en base a los procedimientos internos de reclutamiento y selección (**ME-DG-PS04 Plan Seguridad de Sistemas**.).

9.1.2. Oficial de Seguridad

Debe cumplir y hacer cumplir las políticas de seguridad de Microsystem S.A., y debe encargarse de cualquier aspecto relativo a la seguridad de la AC de Microsystem S.A., desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red. Asiste y supervisa las actividades del Administrador de la Autoridad Certificadora.

9.1.3. Administrador de la Autoridad Certificadora

Todas las operaciones realizadas por el Administrador de la Autoridad Certificadora son ejecutadas con supervisión del Oficial de Seguridad o su participación activa donde lo indica el procedimiento.

9.1.3.1. Activar los servicios de CRL y OCSP

9.1.3.2. La instalación y configuración de sistemas operativos, de productos de software y del mantenimiento y actualización de los productos y programas instalados.

9.1.3.3. Establecer y documentar los procedimientos de monitorización de los sistemas y de los servicios que prestan.

9.1.3.4. Gestionar la llaves privadas de la Autoridad Certificadora en conjunto con el Oficial de Seguridad y el Comité de Seguridad

9.1.4. Administrador de Sistemas

9.1.4.1. Supervisar procedimientos de monitoreo de disponibilidad de los servicios del PSC y revisar ejecución de los procedimientos autorizados de mantenimiento del PSC tales como respaldos de sistemas, datos y bitácoras.

9.1.4.2. Supervisar estado de sistema de seguridad perimetral.

9.1.4.3. Notificar cualquier irregularidad detectada al Administrador de la Autoridad Certificadora y al Oficial de Seguridad.

9.1.5. Operador de Registro

Responsable de realizar el registro presencial o en terreno ante la solicitud de un certificado de firma, preocupándose de la verificación fehaciente de la identidad del solicitante y la tramitación del cobro.

9.1.6. Operador de Validación

Tiene por función validar el correcto ingreso de una solicitud de certificado, revisando la información recopilada durante el proceso de registro. Adicionalmente se encarga de gestionar las suspensiones, revocaciones y renovaciones de certificados canalizadas mediante teléfono o correo electrónico.

10. Controles de Seguridad Física

10.1. Data Center

Microsystem S.A. cuenta con servidores y dispositivos criptográficos redundantes, colocados en dos proveedores de data center los cuales disponen de certificación ISO27001 y homologación TIER III (IIA) y certificación TIER III (NetGlobalis). Ambos cuentan con redundancia de suministro eléctrico (protegiendo apagón o desconexión de la energía eléctrica), redundantes sistemas de refrigeración y redundantes enlaces a Internet. Lo anterior garantiza alta disponibilidad de los servicios de certificación frente a interrupciones de servicio imprevistas y además permiten realizar mantenimiento o cambio de equipos en caso de pérdida o término de vida útil de hardware. Considerando lo anterior el PSC Microsystem S.A. está preparado para garantizar continuidad operacional según niveles exigidos por la normativa. Más información del data center en documento interno **OP-PR-MDS Descripción Medidas de Seguridad** punto 7.

10.1.1. Accesos

Solo pueden solicitar acceso a los servidores el Gerente de Operaciones TI, el Jefe de Soporte de Clientes, el Jefe de Soporte Interno y el Oficial de Seguridad. Solo estas personas pueden solicitar acceso.

Para realizar la visita a la zona de seguridad elevada (AC), esta debe ser realizada por personal técnico y el Oficial de Seguridad o su subrogante.

10.2. Oficinas de Microsystem S.A.

La atención al público para las solicitudes de atención presencial se realiza en las oficinas de Microsystem S.A. que cuentan con sistema de cámaras de seguridad con grabación continua 24x7, dando de esta forma al PSC la capacidad necesaria para supervisar accesos a sus dependencias en todo momento.

El acceso a las oficinas del Microsystem es solo para colaboradores registrados, ya que el acceso es por medios biométricos (huella dactilar) o tarjeta electrónica.

Las oficinas cuentan con un sistema de detección de acceso no autorizado y alarma supervisada por una empresa externa que controla y supervisa los horarios de activación y desactivación del bloqueo de ingresos.

11. Controles de Seguridad Técnica

11.1. Controles de Acceso Lógico del PSC

11.1.1. Todos los accesos administrativos a los sistemas del PSC requieren acceso mediante una conexión VPN o SSH autenticada con un dispositivo criptográfico personal, o presencia física en el terminal del servidor de acuerdo a las políticas de acceso al Data Center.

11.1.2. Todos los accesos operativos a los sistemas del PSC requieren acceso mediante una VPN autenticada con un dispositivo criptográfico personal del operador.

11.1.3. Todas las autorizaciones de emisión de certificados personales de Firma Electrónica Avanzada acreditada están respaldadas y protegidas por 2 firmas electrónicas avanzadas de emisión interna - Operador de Registro y Operador de Validación, registradas y emitidas por el Administrador de la Autoridad Certificadora en conjunto con el Oficial de Seguridad.

11.1.4. Todos los equipos computacionales portátiles cuentan con mecanismos de cifrado de información retenida perteneciente a los procesos del PSC.

11.2. Comunicaciones

Todas las comunicaciones que trafican la información confidencial entre los Usuarios y el PSC están protegidas por el cifrado de datos mediante el protocolo HTTPS con algoritmos que se consideran seguros a la fecha, para lo cual el PSC continuamente está revisando las recomendaciones de seguridad de la industria de las tecnologías de información.

11.3. Firewall

Todos los sistemas del PSC en ambos Data Center están protegidos por Firewall de capa 4 de OSI y además todos los servicios http y https de acceso público están protegidos por un sistema WAF - Web Application Firewall - capa 7 de OSI.

11.4. Procesos de auditoría automatizada

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

11.4.1. Ingresos exitosos y fallidos a las VPNs

11.4.2. Ingresos no autorizados a servicios protegidos por Firewall

11.4.3. Peticiones válidas e inválidas enviadas hacia servicios WEB

11.4.4. Comandos ejecutados en los terminales de los servidores

11.4.5. Actividades realizadas por los operadores a nivel de la Autoridad de Registro y automáticas que forman parte de los procesos de atención.

11.4.6. Actividades administrativas realizadas a nivel de la Autoridad de Registro

11.4.7. Actividades automáticas y manuales ejecutadas, fallidas y exitosas, realizadas a nivel de la Autoridad Certificadora

11.4.7.1. Asignación o desasignación de permisos de operadores

11.4.7.2. Cambios de configuración

11.4.7.3. Emisión de las listas CRL

11.4.7.4. Eventos de ciclo de vida de los certificados personales de Firma Electrónica Avanzada

11.4.7.5. Eventos de ciclo de vida de los certificados raíces e intermedios de la Autoridad Certificadora

11.4.7.6. Activación y desactivación de la conexión entre la Autoridad Certificadora y el dispositivo HSM que protege las llaves privadas de esta

11.4.8. Resultados de ejecución de tareas de respaldo

11.5. Medidas de seguridad para gestión del ciclo de vida de las llaves privadas

El detalle de los procedimientos relacionados está en el documento **ME-DG-PS06 Plan de Administración de Llaves**.

11.5.1. Generación de las llaves de la Autoridad Certificadora

La generación de las llaves de la Autoridad Certificadora del PSC se realiza mediante un procedimiento **Ceremonia de Llaves** con participación de los siguientes roles del PSC: Comité de Seguridad, Oficial de Seguridad, Administrador de la Autoridad Certificadora, Operador de Registro y Operador de Validación. Adicionalmente asisten representantes de la Entidad Acreditadora como testigos del proceso. Las llaves de la Autoridad Certificadora nacen en un dispositivo criptográfico **HSM, Thales ProtectServer 2 PL25**, certificado bajo norma **FIPS 140-2 Level 3**. Después de ser creadas, las llaves son replicadas al segundo HSM para garantizar alta disponibilidad. El algoritmo de las llaves es **RSA**, la llave raíz tiene un tamaño de **4096 bits** y la llave intermedia de **2048 bits**. La generación de nuevas llaves para continuar con la operación del PSC frente a la expiración de las llaves vigentes, ocurre en una nueva **Ceremonia de Llaves** en un plazo entre 4 y 3 años antes de la expiración.

11.5.2. Almacenamiento, respaldo y recuperación de las llaves de la Autoridad Certificadora

11.5.2.1. Las llaves de la Autoridad Certificadora en su forma activa son almacenadas exclusivamente mediante un dispositivo criptográfico HSM donde han sido creadas, replicadas o restauradas mediante protocolos seguros.

11.5.2.2. El respaldo de las llaves privadas se realiza durante la **Ceremonia de Llaves,** mediante tarjetas inteligentes de respaldo con lector de tarjetas conectado al HSM de manera directa. Las tarjetas contienen la llave maestra de respaldos y son operadas por el Comité de Seguridad en modalidad 2 de 5. Las tarjetas de respaldo son almacenadas en un lugar seguro de donde pueden ser retiradas por 2 miembros del Comité de Seguridad. En el procedimiento de respaldo participan 5 integrantes del Comité de Seguridad, Oficial de Seguridad y Administrador de la Autoridad Certificadora.

11.5.2.3. La recuperación se realiza, en un ambiente físicamente seguro, con la participación de 2 miembros del Comité de Seguridad, Oficial de Seguridad y Administrador de la Autoridad Certificadora, utilizando un HSM igual o compatible con el HSM original, configurado para operar en modalidad FIPS 140-2 Level 3.

11.5.3. Distribución de las llaves públicas de la Autoridad Certificadora

11.5.3.1. Las llaves públicas de la Autoridad Certificadora son distribuidas en formato de certificados X.509, firmados en cadena de acuerdo a lo indicado en el apartado Cadena de Confianza de la Autoridad Certificadora Microsystem S.A. de esta DPC.

11.5.3.2. Las llaves públicas de la Autoridad Certificadora son publicadas en el sitio web de la **Entidad Acreditadora** en la sección **Certificados Raíz** https://www.entidadacreditadora.gob.cl/certificados-raiz/ y en la sección de **Información de Confianza** del sitio del PSC https://portal.ca.msys.cl/

11.5.3.3. Las huellas digitales de los certificados de la Autoridad Certificadora están notificadas en esta DPC, apartado Cadena de Confianza de la Autoridad Certificadora Microsystem S.A., y en el documento de **ME-DG-PO01 Políticas de Certificación de Firma Electrónica Avanzada** correspondiente, disponible en la sección **Documentación de las Políticas y Prácticas de Certificación** del sitio https://portal.ca.msys.cl/.

11.5.4. Usos de las llaves privadas de la Autoridad Certificadora

Las llaves privadas de la Autoridad Certificadora son utilizadas exclusivamente para los siguientes fines:

11.5.4.1. **Llave privada raíz**: Emisión de un certificado raíz y un certificado de la autoridad intermedia durante una **Ceremonia de Llaves**. Emisión de la lista de revocación de las autoridades intermedias, cada 6 meses, credenciales de activación manejadas por un Oficial de Seguridad y un Administrador de la Autoridad Certificadora. Al emitir la lista de revocación la llave queda desactivada. El algoritmo de hash utilizado para la emisión de CRL y certificados intermedios es SHA256.

11.5.4.2. **Llave privada de la autoridad intermedia**: Las credenciales de activación son manejadas por el Administrador de la Autoridad Certificadora bajo supervisión del Oficial de Seguridad. Se activa para operación automática de los servicios OCSP y

CRL y emisión de los certificados personales de Firma Electrónica Avanzada. La emisión de los certificados personales de Firma Electrónica Avanzada requiere la participación de 2 personas, Operador de Registro y Operador de Validación. El algoritmo de hash utilizado para la emisión de CRL, OCSP y certificados personales de FEA es SHA256.

11.5.5. Fin de vida útil de las llaves privadas de la Autoridad Certificadora

Al alcanzar el fin de vida útil de una llave privada de la Autoridad Certificadora se procede a eliminarla de los HSM del PSC y se eliminan todos los respaldos de esta.

11.5.6. Gestión del ciclo de vida de los HSM

11.5.6.1. El dispositivo HSM está configurado para operar de acuerdo a la norma FIPS 140-2 Level 3 y cuenta con un circuito de detección de acceso no autorizado que provoca un borrado de todas las llaves en caso de ser activado.

11.5.6.2. El dispositivo HSM está bajo monitoreo de su estado operacional durante todo el periodo de uso en los procesos del PSC para garantizar que esté operativo para cumplir con las funciones del PSC.

11.5.6.3. Todas las operaciones de manejo físico de los HSM se ejecutan por 2 funcionarios autorizados del PSC.

11.5.6.4. Al completar la vida útil del dispositivo, previo al retirar el dispositivo, se procede con la eliminación de todas las llaves almacenadas en su memoria.

11.5.7. Gestión de llaves privadas de Usuarios

Las llaves privadas de los Usuarios son generadas dentro de un dispositivo criptográfico certificado bajo norma FIPS 140-2 Level 3 mediante procedimientos que garantizan que el Usuario tiene un control exclusivo de sus llaves privadas.

11.5.8. Preparación de dispositivos criptograficos de Usuarios

11.5.8.1. Todos los dispositivos criptográficos de los usuarios, comercializados por el PSC, son comprados mediante canales oficiales de distribución del fabricante y previo a la entrega al Usuario son validados por un Operador de Registro.

11.5.8.2. Los dispositivos criptográficos proporcionados por el mismo Usuario son revisados por el Operador de Registro para validar que cumplen con los requisitos de FEA.

11.5.8.3. El stock de los dispositivos disponibles es almacenado en un lugar seguro de la oficina del PSC con acceso disponible al Operador de Registro.

11.5.8.4. El PIN del dispositivo criptográfico lo configura el Usuario antes de utilizar dicho dispositivo para generar las llaves privadas del Usuario.

11.6. Gestión de Activos

Para supervisar los ciclos de vida, políticas de seguridad, responsables y propiedad de todos los elementos de la plataforma de la Autoridad Certificadora, tales como, hardware, software y datos en sus diferentes expresiones, Microsystem S.A. implementa un **Sistema de Gestión de Activos** cuya operación está descrita con detalle en el documento interno **ME-DG-PS04 Plan Seguridad de Sistemas** (apartado **12. Gestión de Activos**).

12. Políticas de Respaldo y Retención

12.1. Información sujeta a retención

Con el fin de mantener un adecuado respaldo de la información involucrada en el proceso de certificación, así como para brindar seguridad y garantía a todas las partes involucradas, se almacenarán en un medio seguro una serie de archivos relevantes al proceso de certificación. Ellos son:

- Registros de auditoría técnica automatizada especificados en el punto Procesos de auditoría automatizada de esta DPC.
- Soportes de backup de los servidores que componen la infraestructura de la AC de Microsystem S.A.
- Documentación relativa al ciclo de vida de los certificados, entre la que se encuentra:
  - Solicitud de emisión de certificado.
  - Copia de la documentación de identificación aportada por el solicitante del certificado.
  - Identidad del operador de registro y validación que participaron en la emisión del certificado
  - Fecha de solicitud y verificación de identidad del Titular
- Contratos y acuerdos suscritos por Microsystem S.A. en su función de AC
- Autorizaciones de acceso a los Sistemas de Información

Más información en documento interno ME-DG-PS05 Implementación del Plan de Seguridad de Sistemas puto 15.5

12.2. Requerimientos para marca de tiempo de registros

Todos los registros de auditoría contienen la fecha y hora del servidor del PSC, para la ocurrencia del evento pertinente.

12.3. Sistema de colección de archivos

12.3.1. Los documentos electrónicos aludidos se mantienen en custodia electrónica cerrada para su conservación segura.

12.3.2. La consulta de los documentos electrónicos dejados en custodia electrónica en Microsystem S.A. la pueden realizar personas debidamente autorizadas, mediante el uso de doble factor, para garantizar la confidencialidad de la información y autorización requerida.

12.3.3. La verificación de la autenticidad de los documentos electrónicos más críticos está dada por la verificación de la Firma Electrónica Avanzada del emisor.

12.4. Procedimiento Interno ISO 27001

Toda la información retenida está sujeta a respaldos de acuerdo a las políticas y procedimientos establecidos bajo norma ISO 27001 en el procedimiento de respaldo, documento **OP-PR-RESP Procedimiento de Respaldo punto 7.3**.

13. Estructuras de Certificados de FEA, Registro de Acceso Público (CRL y OCSP) y Cadena de Confianza

En base a lo definido en detalle en el documento **ME-PR-TB01 Estructura e Información de un Certificado de Firma Electrónica Avanzada**, se resume lo siguiente.

13.1. Formato del certificado de FEA

13.1.1. Microsystem S.A emite certificados de FEA para personas naturales. Dichos certificados hacen uso de un dispositivo de creación de firma seguro, denominado Dispositivo Criptográfico, el cual debe estar certificado bajo norma FIPS 140-2 nivel 3, para proporcionar un alto nivel de aseguramiento.

13.1.2. El formato del certificado de FEA emitido por Microsystem S.A., está bajo los estándar X.509 v3.

13.2. Extensiones de certificado de FEA

13.2.1. Microsystem S.A., en los certificados que emite, incorpora extensiones definidas en la Ley 19.799 (Referencias 10.3). Las anteriormente mencionadas son las siguientes:

13.2.1.1. RUN del Titular del certificado - extensión con **OID 1.3.6.1.4.1.8321.1**

13.2.1.2. RUT del emisor del certificado - extensión con **OID 1.3.6.1.4.1.8321.2**

13.2.2. Adicionalmente los certificados emitidos por Microsystem S.A. pueden contener otras extensiones definidas por el estándar X.509 v3, así como cualquier otro formato, incluidos los utilizados por Microsoft.

13.2.3. El uso del certificado por parte del Titular está restringido mediante el uso de extensiones de certificado que describen los usos básicos de claves y los usos extendidos de claves.

13.3. Extensiones críticas de certificado de FEA

13.3.1. Microsystem S.A. usa ciertas extensiones críticas en los certificados que emite, con el fin de:

13.3.1.1. Mostrar si un certificado está destinado a una CA o no.
13.3.1.2. Mostrar el uso previsto de la clave.
13.3.1.3. Prohibir cualquier uso del certificado inconsistente con las Políticas y Prácticas de Firma Electrónica Avanzada de Microsystem S.A.

13.4. Estructura del certificado de FEA

A continuación, se incorpora una tabla con todos los campos de un certificado de usuario de Firma Electrónica Avanzada emitido por la Autoridad Certificadora Microsystem S.A.

Campo y Descripción	***Valor***
Versión del formato X.509	3 (0x02)
Número de serie	6d:73:10:57:65:7b:a4:f1:ea:00:b0:57:62:2f:d7:be:ab:4c:85:c2
ID Algoritmo de firma	SHA256withRSA
Validez	
No antes de	Aug 5 21:06:13 2022 GMT
No después de	Aug 20 21:06:13 2023 GMT
Emisor	
E-mail	soportepki@microsystem.cl
Nombre común	Microsystem Firma Electronica Avanzada - P1
Unidad organizacional	94099000-9
Unidad organizacional	Autoridad Certificadora
Organización	Microsystem S.A.

Localidad	Santiago
Región	Region Metropolitana
País	CL
Sujeto titular	
E-mail	jmarcini@gmail.com
Nombre común	JAROSLAW MARCIN IWANSKI
Número de serie	21149007-1
Título	PERSONA NATURAL
País	CL
Llave pública	
Algoritmo	RSA
Largo	2048

Módulo	00:c5:18:1b:7e:70:5d:9e:94:91:ab:9b:be:4a:95: bc:be:74:75:4e:8d:17:3e:5e:75:2e:fd:57:a0:e6: b9:e5:c4:61:84:db:43:48:00:38:09:2f:cc:e7:20: 28:e8:70:77:22:e5:5d:1a:23:76:69:28:05:d8:4a: 2d:99:ef:59:c3:d8:44:29:ef:57:93:c4:b6:7a:d3: 95:e3:34:bc:e6:8c:06:3f:74:69:8d:09:0e:0a:b1: 95:6e:fa:05:be:c8:cf:ed:f7:3d:a7:a1:db:6f:d6: ad:4c:db:73:9e:08:39:c5:4e:a7:6f:19:da:f3:8a: 03:ca:54:16:53:f4:4f:6c:e1:73:30:cb:c4:c8:29: fb:25:77:c1:51:d3:c5:78:af:df:08:f6:d4:9f:6a: 26:1c:28:1d:02:33:ba:67:08:1d:47:5a:eb:70:4c: 8a:16:c6:73:b8:31:7c:77:ed:c4:aa:4f:52:1b:16: 5e:c5:fc:09:a1:13:4b:a9:6c:e7:bc:0f:9b:d3:df: e4:ed:b4:62:1a:fa:b6:92:83:24:9b:b5:18:a0:ae: 9a:c6:ff:ac:05:8d:38:e1:ec:4c:1e:fb:8e:b4:66: c5:95:34:fb:91:6e:0f:7d:54:bc:06:bb:ea:43:5d: 2c:31:38:49:52:e4:6d:a9:a1:05:e1:79:c9:8b:32: 25:4b
Exponente	65537 (0x10001)
Firma del certificado	
Algorithm	SHA256withRSA
Valor de firma	95:c3:26:57:cc:71:bc:c4:9d:03:10:96:35:be:57:72:32:97: b3:3a:85:98:82:0d:d6:d8:7a:5c:71:6d:7a:29:6a:56:b4:30: ae:50:66:51:8b:33:cd:ac:4a:99:2b:b2:27:23:39:70:09:60: b9:93:f7:0c:77:9b:d4:64:00:e3:07:86:87:ba:91:24:00:ff: 7b:52:68:1e:4c:c3:73:27:91:86:e5:68:89:84:ec:73:de:d7: 9c:8d:26:04:52:ba:85:6b:aa:9c:9d:ef:1d:4e:60:ad:82:49: 6b:a9:65:e9:8c:10:9e:eb:51:02:c1:9b:5f:23:52:8d:8a:72: 4a:cf:95:61:dc:9e:e0:5f:94:63:fb:d4:93:ff:9d:9e:ed:cf: 66:56:d7:c0:2e:a1:00:f9:8b:ef:cb:54:8d:bf:ba:bd:02:72: c9:af:db:80:b2:b3:29:dc:da:c6:7b:5d:69:ca:ca:f5:b4:e3: 2e:62:5e:99:f8:57:62:26:58:93:84:57:8c:37:16:5e:db:f7: 24:e8:23:41:5e:3f:86:3e:c2:32:18:55:76:38:b2:f0:9e:23: 02:6e:62:b3:fa:d3:ca:4f:d7:6a:16:cc:08:07:7f:cc:d4:7a: 8d:24:db:ab:56:7e:bd:2c:05:1e:f5:7e:6f:cc:6b:cf:0a:e1: e6:1a:c8:41

Extensiones	
restricciones básicas	-
identificador de la llave de la autoridad	keyid:2F:7A:D6:E2:08:13:5E:52:7C:36:6D:42:60:44:32:56:5C:71:61:45
información de la autoridad, ubicación de la cadena emisora y del servicio OCSP	**cadena de confianza:** http://portal.ca.msys.cl/Microsystem_Firma_Electronica_Avanzada_-_P1.p7c **ocsp:** http://ocsp.ca.msys.cl/ocsp
información de las políticas *(Número de Empresa Privada "PEN" asignado a Microsystem SA es 54151)*	**OID de politicas:** 1.3.6.1.4.1.54151.1.10 **CPS:** https://www.microsystem.cl/cps **mensajes para usuarios:** **texto=**'Certificado para Firma Electronica Avanzada. Resolucion exenta XXX del XX de XXXX de XXXX, Subsecretaria de Economia, Fomento y Reconstruccion.' **texto=**'El uso de este certificado esta sujeto a las politicas y practicas de certificacion (CP y CPS) establecidas por Microsystem S.A., disponibles publicamente en https://www.microsystem.cl/cps'
información extendida de uso de llave	clientAuth, emailProtection
URL de distribución de CRL	http://crl.ca.msys.cl/Microsystem_Firma_Electronica_Avanzada_-_P1.crl
ID de la llave del titular	7b4cb6bc1352b75a3faa0a9d372a2393a22dcea8
usos de llave	digitalSignature,nonRepudiation,keyEncipherment,dataEncipherment,keyAgreement
nombre alternativo del emisor, RUT de la autoridad emisora	oid=1.3.6.1.4.1.8321.2 tipo=IA5_STRING texto='94099000-9'

según establecido en el DECRETO Nº 181	
nombre alternativo del titular, RUN del titular del certificado según establecido en el DECRETO Nº 181	id=1.3.6.1.4.1.8321.1 tipo=IA5_STRING texto='21149007-1'

13.5. Estructura completa de la lista de certificados revocados de Firma Electrónica Avanzada

A continuación se incorpora una tabla con todos los campos de una lista de certificados revocados de Firma Electrónica Avanzada emitidos por la Autoridad Certificadora Microsystem S.A.

Esta lista esta publicada en la URL:
http://crl.ca.msys.cl/Microsystem_Firma_Electronica_Avanzada_-_P1.crl

Esta lista se renueva automáticamente cada 24 horas.

Descripción	***Campo***	***Valor***
La versión del formato de la estructura de la lista	**Certificate Revocation List Version:**	Version 2 (0x1)
El identificador del algoritmo de firma de los datos dentro de la lista	**Signature Algorithm:**	sha256WithRSAEncryption
El nombre del emisor de la lista	**Issuer:**	C = CL, ST = Region Metropolitana, L = Santiago, O = Microsystem S.A., OU = Autoridad Certificadora, OU = 94099000-9, CN = Microsystem Firma Electronica Avanzada - P1, emailAddress = soportepki@microsystem.cl

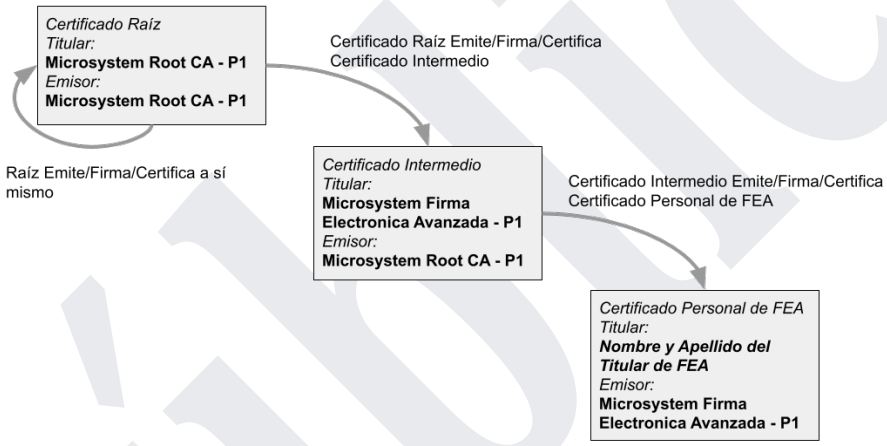
La fecha de emisión de la lista	**Last Update:**	Jan 20 06:13:20 2023 GMT
La fecha de la siguiente actualización de la lista	**Next Update:**	Jan 21 06:13:20 2023 GMT
Un atributo extendido de la lista que identifica la llave del firmante	**CRL extensions:**	X509v3 Authority Key Identifier: keyid:64:25:20:5B:C5:C9:59:D7:C8:4F:4D:19:2D:4D:E0:91:22:EC:84:E9
El folio de la lista	**X509v3 CRL Number:**	3
La lista los números de serie de los certificados revocados con sus fechas de revocación	**Revoked Certificates:**	Serial Number: 368D8AE9BA11D03D5A8BD4284F141274F870A6E5 Revocation Date: Aug 5 21:46:37 2022 GMT
Un ejemplo de un certificado suspendido (Hold)		Serial Number: 0D30C5A926E368BFF819C57D00A008FFDBE51277 Revocation Date: Aug 5 21:38:13 2022 GMT CRL entry extensions: X509v3 CRL Reason Code: Certificate Hold
El valor de la firma de los datos contenidos en la lista de acuerdo al algoritmo previamente especificado: sha256WithRSAEncryption	**Signature Value:**	a8:7b:7f:d3:77:63:87:67:1e:d1:73:84:22:e5:0d:55:0f:9b: 0b:94:39:54:39:08:c2:2e:35:d8:03:c2:ee:78:5b:ed:b5:39: ef:17:c4:01:6e:02:23:3e:1b:18:17:7b:7d:b1:44:15:e4:5c: 82:79:a4:21:0e:a1:2e:80:ab:22:a6:b4:92:f2:ed:72:06:6b: 8a:00:b7:8a:61:40:3e:df:ae:1e:62:be:06:f7:3a:1d:be:1a: e8:2a:b6:a6:90:60:2b:cc:7b:16:c7:30:1d:2e:d7:aa:d8:8a: 0a:44:9e:5b:a2:55:9c:26:d3:e2:4e:dd:87:44:7d:25:b1:5f: 2a:0e:53:94:81:53:f4:b9:dc:a2:85:3f:1c:c3:b3:43:49:6f: e3:78:43:c0:1f:08:a9:cd:5a:34:a3:6e:99:3f:58:4c:dc:57: 46:80:02:2d:d7:cf:e4:bd:17:82:b7:24:a5:a0:9f:fe:9d:77: 34:32:f2:14:08:ef:1f:06:a7:15:ea:1a:ab:30:63:26:fb:6e: ba:df:6b:6c:35:dd:99:f4:1c:4e:70:51:21:e5:a8:93:8a:a8: 68:ee:13:fe:ed:f3:49:1c:74:e9:f9:38:c9:41:b3:09:8f:b3: e8:2c:a4:94:01:c9:5c:f2:e5:92:1c:d8:25:b5:5a:01:80:6a: 4a:80:c8:2c

13.6. Estructuras de mensajes del servicio OCSP

De acuerdo con lo estipulado en la legislación vigente el servicio OCSP opera con mensajería que está conforme al estándar RFC 2560.

13.7. Cadena de Confianza de la Autoridad Certificadora Microsystem S.A.

Cada certificado personal de Firma Electrónica Avanzada de Microsystem S.A. está firmado por un certificado intermedio vigente de Microsystem S.A., aquel certificado intermedio está firmado a su vez por el certificado raíz vigente. Las dependencias de las firmas de certificación constituyen una cadena como se refleja en el diagrama, a continuación se encuentran detalles de los certificados raíz e intermedio vigentes de la Autoridad Certificadora Microsystem S.A.



13.7.1. Certificado raíz vigente **Microsystem Root CA - P1**
Emitido y firmado por sí mismo
Disponible en: https://portal.ca.msys.cl/confianza/MicrosystemRootCAP1.crt

Campo y Descripción	***Valor***
Versión del formato X.509	3 (0x02)
Número de serie	3d:43:d0:ad:2c:12:d1:ce:81:c2:b3:fe:de:5b:ca:09:32:34:61:86
ID Algoritmo de firma	SHA256withRSA

Validez	
No antes de	Jan 5 15:22:34 2023 GMT
No después de	Dec 31 15:22:34 2042 GMT
Emisor	
E-mail	soportepki@microsystem.cl
Nombre común	Microsystem Root CA - P1
Unidad organizacional	Autoridad Certificadora
Unidad organizacional	94099000-9
Organización	Microsystem S.A.
Localidad	Santiago
Región	Region Metropolitana
País	CL
Sujeto titular	
E-mail	soportepki@microsystem.cl
Nombre común	Microsystem Root CA - P1
Unidad organizacional	Autoridad Certificadora
Unidad organizacional	94099000-9
Organización	Microsystem S.A.

Localidad	Santiago
Región	Region Metropolitana
País	CL
Llave pública	
Algoritmo	RSA
Largo	4096
Módulo	00:cc:34:32:76:0f:62:2d:26:f6:a4:de:8a:a1:94: f9:05:5f:2f:08:3c:e9:9c:5b:43:69:8e:33:c8:4c: 28:0b:2c:0f:3b:1b:9b:fc:b8:1b:46:3f:c3:b5:83: c3:b3:1b:68:7e:d1:16:5e:5e:ca:7f:03:49:ed:66: bf:83:46:dc:dc:d2:03:e1:0a:91:6c:ce:c2:e2:80: 84:51:ad:3c:cd:79:46:38:4f:d0:2b:77:37:74:3d: b9:9b:16:95:72:ea:7a:8e:ff:e5:ad:e3:a3:24:35: 29:87:87:cd:6e:57:51:69:a8:5d:5c:a6:f3:31:cd: 01:a2:61:91:20:a0:6e:86:38:bc:69:fc:b9:37:c9: 69:31:3c:a3:a2:dc:89:5d:9b:0a:7c:7c:df:69:70: 37:b7:95:ac:36:4e:19:09:2c:a4:19:7f:69:13:b8: 04:7d:b3:60:4e:f7:25:c1:0a:5f:e1:91:d4:2d:e3: 89:dd:db:1b:49:c5:e9:5e:3b:e7:d0:6e:60:5a:fe: 5e:8f:22:c8:0d:bd:63:28:91:56:ef:96:b4:65:b1: dc:af:ce:3b:9e:ea:32:28:5f:2f:82:a0:c4:38:5b: d7:23:5b:5e:27:35:db:b3:1e:31:cb:32:34:ca:3d: aa:27:43:02:8d:75:05:4c:3a:71:2d:fc:81:91:e3: 70:92:df:d9:e0:1a:88:3b:18:64:b5:f3:a0:83:e2: 7f:6b:b8:aa:69:0b:b6:5e:47:13:ef:11:a5:f9:7d: 46:fa:39:2c:50:75:6b:b1:dd:1e:fd:d8:41:a4:1d: 8a:ef:2a:76:ca:8c:e4:01:e9:6e:11:80:f9:96:d6: d7:b9:a3:d4:38:29:c9:2d:a6:cd:a8:7b:75:64:7a: a9:6e:5d:05:8c:d8:4f:5f:23:bc:a6:f5:46:96:5f: e9:d2:78:b3:73:1d:c1:ef:91:56:2d:39:91:f4:0e: 0b:94:be:95:6a:ec:28:26:ab:83:af:b2:1c:74:e3: a6:4e:00:38:d1:a4:ee:ca:0e:96:1f:c7:36:ad:25: 4d:bb:2c:34:65:9a:9e:6b:89:e4:0d:61:d8:0d:e3: 23:74:ae:73:03:6f:6b:13:5a:37:bb:d5:97:c5:2e: 2a:c7:78:98:73:37:f1:95:80:4e:df:3e:be:40:37:

	b1:77:37:ca:e4:cb:c6:a6:02:47:fb:db:31:ac:c2: 3d:35:c2:5a:81:72:9c:93:31:67:1e:b3:ae:98:45: 8d:f0:53:ad:90:e8:68:3d:6e:77:97:88:35:d8:72: 73:a6:19:b7:bc:93:59:7e:1f:ea:5a:dc:7c:82:24: 28:43:3f:70:35:97:79:9b:ac:ed:79:b4:0b:41:fd: d8:4c:91
Exponente	65537 (0x10001)
Firma del certificado	
Algorithm	SHA256withRSA
Valor de firma	01:36:05:b0:49:ff:6b:82:6d:b0:16:1f:fe:29:a8:bf:d6:3b: 20:d2:a8:a4:f1:e7:23:53:5c:9c:63:e3:66:59:69:10:a6:6c: 48:3f:3b:4f:c8:9d:4a:d8:cd:51:8b:52:07:aa:34:4a:a2:4f: 64:17:23:3c:ed:2d:31:ae:4c:39:3d:36:f9:42:d7:97:52:b8: d1:2e:1c:d5:3e:4c:44:e9:a7:ce:4f:b1:a8:f1:e0:d9:e6:97: 69:60:8b:1d:f4:86:db:f1:ff:ef:27:97:3f:3a:b7:9e:3f:89: 46:ae:78:ad:c9:f0:3e:76:05:3f:62:17:01:4e:e8:4b:4c:17: 60:0f:56:cf:cd:66:98:16:78:63:12:b0:de:ea:ec:7c:f4:47: 3a:dd:e4:cc:11:46:3c:93:06:a6:a4:c2:1c:6d:7f:44:a9:66: 66:b5:4d:f6:e3:1a:ac:2a:b5:51:03:6a:6e:87:d5:5d:13:74: f5:48:62:e9:94:63:c8:b2:02:25:07:eb:75:ac:b2:14:41:b1: 3e:21:d8:a8:39:35:da:48:9d:50:69:8d:e9:56:1c:7f:ae:fa: 48:e6:ac:92:93:1f:04:3c:d7:6c:0e:e0:82:d8:f3:35:12:b9: 13:10:ff:5e:e6:17:fc:d5:a1:97:22:8c:74:10:15:41:cb:4a: 89:7a:89:74:93:c6:ac:c9:9e:a0:92:94:09:9e:7b:9e:1c:4c: 41:9a:0b:d1:6b:a4:07:24:e8:1e:01:cf:d4:ce:34:22:83:c7:

	18:f8:c2:7a:61:d9:fe:dd:44:2e:48:0e:f6:ce:ee:ab:bd:64: ab:e3:c1:44:c2:ef:52:f3:ae:a4:01:14:2d:e1:6c:ca:b4:a3: 0d:da:2a:5d:41:ad:f7:72:48:eb:5d:f2:5c:3c:97:4b:58:51: cf:08:70:09:85:94:22:49:8b:c6:d3:90:f1:87:58:78:c9:bc: 8b:40:bd:f6:ab:4e:73:0b:a4:bb:a5:ed:2d:67:7f:f7:3b:f4: be:82:10:6f:a7:23:f5:f5:3a:c0:a0:ba:57:b0:96:f6:9a:1f: f5:be:83:88:50:54:d8:d8:85:9a:b2:ac:4d:47:fc:95:73:10: 83:49:64:d3:65:9d:a0:7a:be:1e:c9:3d:58:ac:63:2c:f8:e8: 16:d8:a8:5c:a7:c8:0f:1b:9c:4b:71:bd:e8:66:a5:af:a3:3f: 9a:b3:e8:b8:54:95:51:d2:4f:56:ae:a3:43:f4:40:af:3f:1c: e5:8b:74:8f:15:a5:80:cf:13:b0:f0:e5:b7:35:e4:77:c8:54: 11:47:70:51:b8:9b:19:c0:49:f4:72:9b:b2:c8:82:08:b3:1b: 64:ec:f9:ba:89:46:b6:ca
Extensiones	
restricciones básicas	CA:TRUE
identificador de la llave de la autoridad	keyid:B5:B3:F8:DB:32:91:F2:F3:B5:E1:5F:65:1C:E1:83:4C:2A: B1:FA:F3
información de las políticas *(Número de Empresa Privada "PEN" asignado a Microsystem SA es 54151)*	**OID de políticas:** 1.3.6.1.4.1.54151.1.10 **CPS:** https://www.microsystem.cl/cps **mensajes para usuarios:** **texto=**'El uso de este certificado esta sujeto a las politicas y practicas de certificacion (CP y CPS) establecidas por Microsystem S.A., disponibles publicamente en https://www.microsystem.cl/cps'
información de uso de llave	Digital Signature, Certificate Sign, CRL Sign
ID de la llave del titular	B5:B3:F8:DB:32:91:F2:F3:B5:E1:5F:65:1C:E1:83:4C:2A:B1:FA: F3
huella digital SHA1	328a79d91057a38bd468e18a684c74f6c9be3155

13.7.2. Certificado de la autoridad intermedia **Microsystem Firma Electronica Avanzada - P1**

Emitido y firmado por el certificado raíz **Microsystem Root CA - P1**
Disponible en:
https://portal.ca.msys.cl/confianza/MicrosystemFirmaElectronicaAvanzadaP1.crt

Campo y Descripción	***Valor***
Versión del formato X.509	3 (0x02)
Número de serie	3c:dd:e3:52:1a:13:72:96:62:fc:18:1a:02:63:21:9e:10:f0:69:11
ID Algoritmo de firma	SHA256withRSA
Validez	
No antes de	Jan 5 15:31:25 2023 GMT
No después de	Dec 31 15:22:34 2042 GMT
Emisor	
E-mail	soportepki@microsystem.cl
Nombre común	Microsystem Root CA - P1
Unidad organizacional	94099000-9
Unidad organizacional	Autoridad Certificadora
Organización	Microsystem S.A.
Localidad	Santiago
Region	Region Metropolitana
País	CL

Sujeto titular	
E-mail	soportepki@microsystem.cl
Nombre común	Microsystem Firma Electronica Avanzada - P1
Unidad organizacional	Autoridad Certificadora
Unidad organizacional	94099000-9
Organización	Microsystem S.A.
Localidad	Santiago
Region	Region Metropolitana
País	CL
Llave pública	
Algoritmo	RSA
Largo	2048

Módulo	00:ba:ce:17:20:49:8a:06:65:3c:34:2a:80:1d:5e: 07:ab:b4:7d:32:e3:51:3b:86:c2:c3:b0:29:10:d7: d5:7b:e3:86:42:36:8d:cd:26:66:02:e3:61:1e:08: 43:94:4d:dd:4a:71:7a:05:8b:d1:62:4f:78:7a:d1: d3:7c:b7:62:80:b1:1e:b6:4c:84:31:0b:70:e8:bc: 94:fb:73:6c:a2:b2:15:d9:b7:c4:e4:ea:32:a8:24: 20:9b:18:5d:db:33:ab:de:f9:e9:8a:c4:a2:57:52: 0b:da:4f:1b:32:69:a3:11:58:4a:ee:cb:c1:e3:55: 4f:80:f0:31:70:d9:1e:68:ce:d8:38:2c:e2:f1:84: f4:fc:2d:6c:72:f3:bf:fa:aa:5b:bf:42:ce:86:50: 4c:85:b8:69:ab:f8:da:f0:a9:d5:0f:1b:4b:36:d4: f8:d6:e5:1a:c1:04:33:16:e2:80:88:d8:e6:15:6a: 5a:7d:31:1f:0d:b9:03:d2:dc:81:5a:1a:97:1f:7a: 98:6d:e6:99:dd:ee:21:ae:ec:4c:24:2a:92:ee:b3: 02:17:d2:bc:47:87:65:43:65:ef:25:85:1b:8c:2b: f3:de:5b:23:dc:82:5a:09:26:43:ca:bb:8e:e9:b3: 1d:ed:45:00:16:12:eb:eb:77:c5:bc:aa:c4:6a:6c: ef:b5
Exponente	65537 (0x10001)
Firma del certificado	
Algorithm	SHA256withRSA
Valor de firma	65:b7:9b:d8:30:35:a2:3e:fa:ed:55:17:85:1f:cc:59:74:f6: 94:38:79:4c:3f:59:65:7b:4d:58:04:70:93:20:c8:65:96:8c: 49:ab:2b:8b:3b:71:8c:a2:48:08:c6:15:35:b6:a9:2c:07:a0: e9:0d:dc:92:d9:9f:df:ea:72:ef:e1:6a:24:22:15:6a:74:46: 50:a5:0b:40:50:23:b0:f8:3d:fc:bb:69:0f:8c:31:bc:7e:a5: 93:ae:88:e6:9d:a6:7d:a1:65:39:a9:84:be:ef:9f:ac:32:7b: b0:36:44:c3:79:7c:21:33:1b:a1:02:0c:88:61:9e:b9:85:63: 97:51:ac:04:cb:52:38:82:a5:8a:2d:5e:65:9e:3d:d6:27:0e: 02:70:f4:b8:97:80:4e:c6:4e:72:4c:39:08:5e:0b:4f:bc:8f: b6:bb:43:6f:26:9e:72:d5:c6:dd:a9:0d:fe:9c:4c:f2:e2:c0: 73:20:2b:1b:dd:be:5d:44:a4:d6:3a:90:81:fd:4b:b8:8c:dd: 0e:c5:41:61:44:7e:f5:b0:3b:07:0f:d9:71:87:9b:75:7f:45: 00:4c:c8:0f:4a:1f:d0:25:7a:60:d5:9f:d5:db:e9:82:65:57: ae:82:47:95:a1:ac:d8:02:58:37:90:e8:b1:1c:5b:ed:96:86: 06:65:bd:f1:8d:c2:1d:1c:6d:b3:ff:9f:13:46:f6:fb:6d:e9:

	9c:fe:26:74:2f:85:2d:eb:e7:d7:18:f3:42:64:18:1a:1c:02: ae:49:15:22:a4:77:3d:26:86:9c:72:ab:74:80:6b:07:48:b6: 2a:45:36:c4:e6:22:25:c6:96:08:12:d0:d9:6a:14:80:32:0a: 55:2a:b0:da:9e:e8:b5:28:21:01:26:84:95:82:be:c6:f7:04: 46:09:82:77:e2:b3:4d:58:2d:08:f7:9b:3f:e5:d1:29:10:52: c2:e9:37:dd:da:34:b9:9b:1b:e3:42:f7:7a:ea:cf:d8:5a:f4: 9f:18:9e:e1:35:c8:2a:fa:d7:7d:ca:36:9b:23:88:46:ed:a6: e0:c5:55:05:84:6b:30:3a:9b:67:bb:39:bb:fd:e1:57:ce:17: e7:74:a6:61:12:38:d0:ac:a2:4e:2d:cf:c6:9e:02:5b:8b:d9: 1a:df:b9:4e:57:0d:aa:95:d8:39:e7:4b:f3:a5:43:23:f1:a9: ec:5d:eb:1d:f4:52:86:8d:e6:98:01:4b:bc:4f:c3:07:68:d2: ea:df:a5:01:81:8e:61:11:29:c9:a8:8a:fc:2e:07:0a:d8:4f: 85:1a:33:27:80:c3:c2:2c:4f:14:9a:f0:9f:90:ad:83:d0:d5: ca:f1:f3:f9:34:96:cf:c6
Extensiones	
restricciones básicas	CA:TRUE, pathlen:0
identificador de la llave de la autoridad	keyid:B5:B3:F8:DB:32:91:F2:F3:B5:E1:5F:65:1C:E1:83:4C:2A: B1:FA:F3
información de las políticas *(Número de Empresa Privada "PEN" asignado a Microsystem SA es 54151)*	**OID de políticas:** 1.3.6.1.4.1.54151.1.10 **CPS:** https://www.microsystem.cl/cps **mensajes para usuarios:** **texto=**'El uso de este certificado esta sujeto a las politicas y practicas de certificacion (CP y CPS) establecidas por Microsystem S.A., disponibles publicamente en https://www.microsystem.cl/cps'
URL de distribución de CRL	http://crl.ca.msys.cl/Microsystem_Root_CA_-_P1.crl
ID de la llave del titular	64:25:20:5B:C5:C9:59:D7:C8:4F:4D:19:2D:4D:E0:91:22:EC:84: E9
huella digital SHA1	853a0ae67ecace2cc3b44e9b8746d66f9bee00b9

14. Otros Aspectos Comerciales y Legales

14.1. Tarifas de Productos y Servicios

Las tarifas de los productos y servicios ofrecidos por Microsystem S.A. en su rol de PSC, se encuentran disponibles en el sitio web https://portal.ca.msys.cl/

El acceso a las Listas de Revocación de Certificados e información sobre el estado de los certificados emitidos por Microsystem es gratuito para todo usuario.

14.2. Declaración de las garantías y seguros

14.2.1. Microsystem S.A. gestionará todos los procesos relacionados con la operación en función de la Autoridad Certificadora de acuerdo a los estándares ISO 9001.

14.2.2. Microsystem S.A. gestionará todos los aspectos de la seguridad de la información y de los procesos relacionados con la operación en función de la Autoridad Certificadora de acuerdo a los estándares ISO 27001.

14.2.3. Microsystem S.A. mantendrá vigente el Seguro de Responsabilidad Civil que exige el reglamento de la Ley de Firma Electrónica Avanzada y Documentos Electrónicos (Ley N° 19.799). Por lo tanto, en base al art. 12° del Decreto 181, dicho seguro deberá contener al menos las siguientes estipulaciones:

14.2.3.1. Una suma asegurada de al menos el equivalente de cinco mil unidades de fomento.

14.2.3.2. La ausencia de deducibles o franquicias, en la parte de la indemnización que no exceda el equivalente de cinco mil unidades de fomento.

14.2.3.3. La responsabilidad civil asegurada, que comprenderá la originada en hechos acontecidos durante la vigencia de la póliza, no obstante sea reclamada con posterioridad a ella.

14.3. Derechos del Usuario

14.3.1. Todo Usuario tendrá derecho a retractarse de la suscripción de los servicios de certificación, en un plazo de 10 días corridos contados desde la fecha de suscripción del certificado de FEA, siempre y cuando no haya utilizado este certificado, en base a los puntos especificados en el apartado Uso del Certificado de FEA

14.3.2. Microsystem S.A. establece que el Usuario tendrá derecho a un reembolso económico equivalente al valor monetario cancelado por el servicio de certificación, excluyendo el valor de los servicios auxiliares no reembolsables.

14.3.3. Microsystem S.A. establece la Política de Protección de los Derechos de los Usuarios, en base a lo que estipula la Ley 19.496. Dicha política se encuentra disponible en el sitio web https://portal.ca.msys.cl/documentacion/

14.4. Comunicación

14.4.1. Para comunicarse de forma individual con cada Titular, Microsystem S.A. utilizará el correo electrónico o el número móvil indicado al momento de la solicitud del certificado de FEA. Mientras que aquellas comunicaciones generales, serán publicadas en la página web.

14.4.2. Los medios de comunicación con el PSC son los indicados en el apartado Datos de Contacto.

15. Datos de Contacto

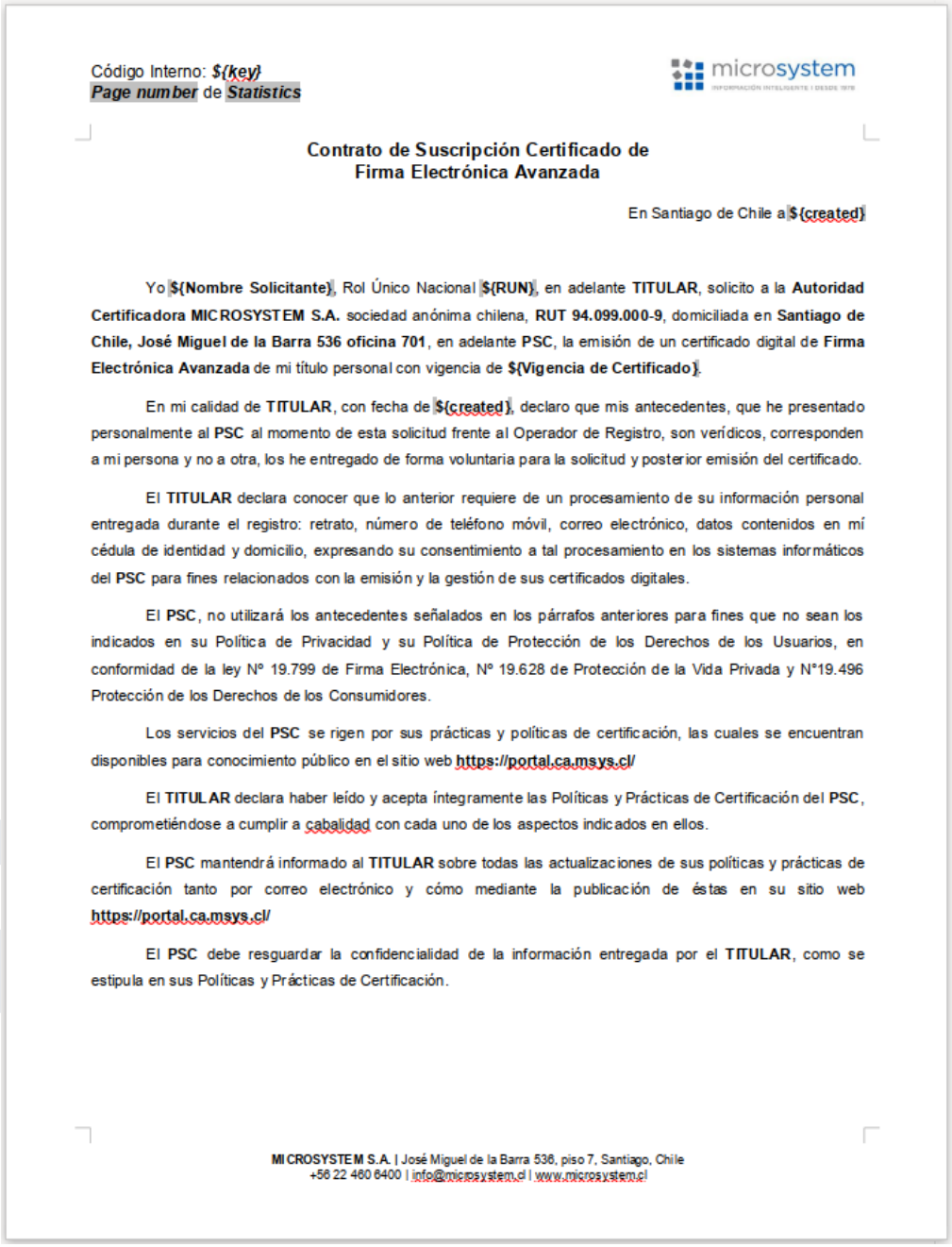
15.1. Dirección: José Miguel de la Barra 536 Piso 7, Santiago, Chile
15.2. Fono: +56224606400
15.3. E-mail: soportepki@microsystem.cl
15.4. Página web: https://www.microsystem.cl/firma-electronica-digital-avanzada/
15.5. Portal de la Autoridad Certificadora de Microsystem S.A. - https://portal.ca.msys.cl

16. Documentos de referencia

16.1. ME-DG-PO01 Políticas de Certificación de Firma Electrónica Avanzada
16.2. LEY SOBRE DOCUMENTOS ELECTRONICOS, FIRMA ELECTRONICA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA
16.3. REGLAMENTO DE LA LEY 19.799 SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y LA CERTIFICACIÓN DE DICHA FIRMA
16.4. MINECON - Entidad Acreditadora - Acreditación de Autoridades Certificadoras - Marco Legal
16.5. MINECON - Entidad Acreditadora - Acreditación de Autoridades Certificadoras - Guías de Acreditación
16.6. RFC 2510 - Internet X.509 Public Key Infrastructure Certificate Management Protocols
16.7. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
16.8. RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
16.9. ISO 9001
16.10. ISO/IEC 27001
16.11. ME-MA-MS Manual de Usuario del Portal de Firma Electrónica Avanzada
16.12. https://en.wikipedia.org/wiki/Private_Enterprise_Number
16.13. Registro de Números de Empresas Privadas https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

17. Anexos

17.1. Contrato de Suscripción de Firma Electrónica Avanzada



Código Interno: *${key}*
Page number de *Statistics*

microsystem

Contrato de Suscripción Certificado de Firma Electrónica Avanzada

En Santiago de Chile a **${created}**

Yo **${Nombre Solicitante}**, Rol Único Nacional **${RUN}**, en adelante **TITULAR**, solicito a la **Autoridad Certificadora MICROSYSTEM S.A.** sociedad anónima chilena, **RUT 94.099.000-9**, domiciliada en **Santiago de Chile, José Miguel de la Barra 536 oficina 701**, en adelante **PSC**, la emisión de un certificado digital de **Firma Electrónica Avanzada** de mi título personal con vigencia de **${Vigencia de Certificado}**.

En mi calidad de **TITULAR**, con fecha de **${created}**, declaro que mis antecedentes, que he presentado personalmente al **PSC** al momento de esta solicitud frente al Operador de Registro, son verídicos, corresponden a mi persona y no a otra, los he entregado de forma voluntaria para la solicitud y posterior emisión del certificado.

El **TITULAR** declara conocer que lo anterior requiere de un procesamiento de su información personal entregada durante el registro: retrato, número de teléfono móvil, correo electrónico, datos contenidos en mí cédula de identidad y domicilio, expresando su consentimiento a tal procesamiento en los sistemas informáticos del **PSC** para fines relacionados con la emisión y la gestión de sus certificados digitales.

El **PSC**, no utilizará los antecedentes señalados en los párrafos anteriores para fines que no sean los indicados en su Política de Privacidad y su Política de Protección de los Derechos de los Usuarios, en conformidad de la ley N° 19.799 de Firma Electrónica, N° 19.628 de Protección de la Vida Privada y N°19.496 Protección de los Derechos de los Consumidores.

Los servicios del **PSC** se rigen por sus prácticas y políticas de certificación, las cuales se encuentran disponibles para conocimiento público en el sitio web **https://portal.ca.msys.cl/**

El **TITULAR** declara haber leído y acepta íntegramente las Políticas y Prácticas de Certificación del **PSC**, comprometiéndose a cumplir a cabalidad con cada uno de los aspectos indicados en ellos.

El **PSC** mantendrá informado al **TITULAR** sobre todas las actualizaciones de sus políticas y prácticas de certificación tanto por correo electrónico y cómo mediante la publicación de éstas en su sitio web **https://portal.ca.msys.cl/**

El **PSC** debe resguardar la confidencialidad de la información entregada por el **TITULAR**, como se estipula en sus Políticas y Prácticas de Certificación.

MICROSYSTEM S.A. | José Miguel de la Barra 536, piso 7, Santiago, Chile
+56 22 460 6400 | info@microsystem.cl | www.microsystem.cl

Código Interno: ***${key}***
Page number de ***Statistics***

microsystem

PSC se obliga a emitir el certificado solicitado en base a la información proporcionada por el **TITULAR**, cualquier cambio en dicha información, posterior a la emisión del certificado, requerirá la adquisición de un nuevo certificado por parte del **TITULAR** y la revocación del certificado anterior.

${Nombre Solicitante} **FIRMA DEL TITULAR**	**IMPRESIÓN DACTILAR DEL TITULAR**

${Nombre Operador}
FIRMA DEL OPERADOR DE REGISTRO

Comprobante de Recepción de Certificado de Firma Electrónica Avanzada

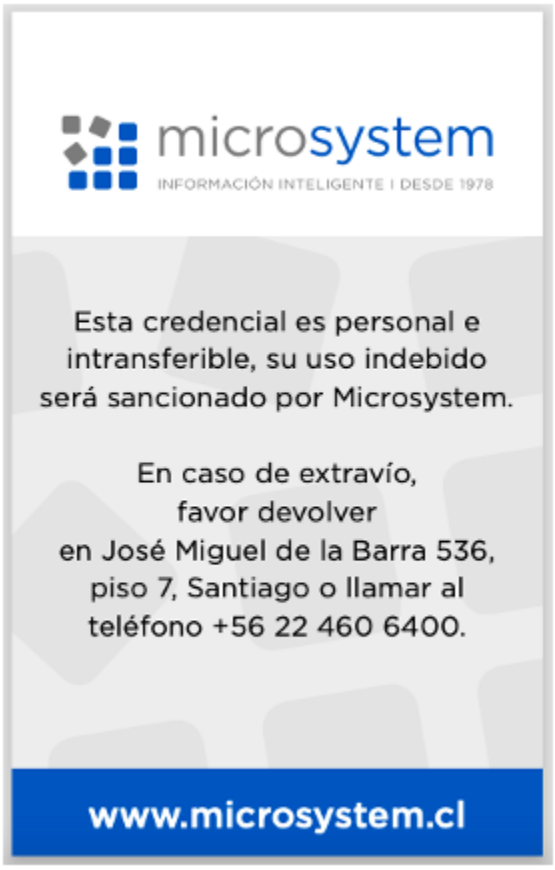
En Santiago de Chile a **${created}**

Yo **${Nombre Solicitante}**, Rol Único Nacional **${RUN}**, confirmo haber recibido a mí entera conformidad el certificado **Firma Electrónica Avanzada**, emitido por la **Autoridad Certificadora MICROSYSTEM S.A, RUT 94.099.000-9**.

${Nombre Solicitante}
FIRMA DEL TITULAR

MICROSYSTEM S.A. | José Miguel de la Barra 536, piso 7, Santiago, Chile
+56 22 460 6400 | info@microsystem.cl | www.microsystem.cl

17.2. Credencial de Presentación



18. Control de Cambios

Versión	Fecha	Responsable	Modificaciones
001	22/06/2021	Jefe de Proyecto - CA	Primera versión del documento
002	05/01/2022	Jefe de Proyecto - CA	Actualización apartado 15.2
003	10/01/2022	Jefe de Proyecto - CA	Se agrega el punto 7.5 (Renovación de un certificado revocado). Se reemplaza "Portal de Usuario" por "Portal de Suscriptor de Firma Digital".

004	14/03/2022	Jefe de Proyecto - CA	Se incorpora el PEN de Microsystem.
005	12/08/2022	Jefe de Proyecto - CA	Se actualiza anexo Solicitud de Firma Electrónica. Se incorpora punto Homologación o Traspaso de Certificado de otro PSC.
006	22/08/2022	Jefe de Proyecto - CA	Se modifica punto: 1. Introducción, objetivo y alcance, incorporando puntos: 1.1 Objetivo y Alcance 1.2 Administración del contenido. 10.2 Roles de confianza, glosa inicial. 10.2.5 Comité de Seguridad. 10.3 Auditorías
007	07/10/2022	Gerente I+D	Se reestructura el documento para alinearse con el art. 6° del Reglamento.
008	27/10/2022	Gerente I+D	Se actualiza el documento en base a las correcciones de la Entidad Acreditadora.
009	20/01/2023	Gerente I+D	Ajuste de contenido para acomodar la jerarquía productiva P1
010	03/08/2023	Gerente MicroeDoc	Incorporación de procedimiento de Registro Presencial en Terreno en Domicilio del Solicitante.
011	13/11/2023	Gerente MicroeDoc	Corrección de observaciones indicadas por Entidad Acreditadora asociadas al procedimiento de Registro Presencial en Terreno en Domicilio del Solicitante.
012	06/03/2024	Gerente MicroeDoc	Corrección de observaciones indicadas por Entidad Acreditadora asociadas al procedimiento de Registro Presencial en Terreno en Domicilio del Solicitante.
013	29/04/2024	Gerente MicroeDoc	Corrección de observaciones indicadas por Entidad Acreditadora asociadas al procedimiento de Registro Presencial en Terreno en Domicilio del Solicitante.
014	24/01/2025	Gerente MicroeDoc	Se incorpora captura de retrato del solicitante en los registros:

			Presencial en oficina PSC: 6.1.1.10. El Operador de Registro procede con la captura de la fotografía (retrato) del Solicitante. Presencial en domicilio del solicitante: 6.1.2.3.5. El Operador de Registro procede con la captura de la fotografía (retrato) del Solicitante. Se actualiza punto 6.3. Periodo de Vigencia Se actualiza punto 6.4.1.2 incoporando el envío de una clave OTP al correo electrónico del usuario. Se actualiza punto 6.4.2.2.incoporando el envío de una clave OTP al correo electrónico del usuario. Y actualizando proceso de revocación. Se incluye punto 6.4.5 y 6.4.6
015	05/03/2025	Gerente MicroeDoc	Se incorpora procedimiento de Registro en Línea a través de Sistema ClaveÚnica conforme al Decreto 24/2019 del Ministerio De Economía, Fomento Y Turismo; Subsecretaría De Economía Y Empresas De Menor Tamaño.