# *POLÍTICAS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA AVANZADA*

## *PO01*

Microsystem S.A.

OID 1.3.6.1.4.1.54151.1.10

Público

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

# Índice

1. Introducción ..... 3
2. Glosario ..... 4
3. Partes Involucradas de PKI de Firma Electrónica Avanzada ..... 7
4. Ciclo de vida de un certificado de FEA ..... 10
5. Estructuras de Certificados de FEA, Registro de Acceso Público (CRL y OCSP) y Cadena de Confianza ..... 23
6. Usos del Certificado de Firma Electrónica Avanzada ..... 39
7. Obligaciones de las partes ..... 39
8. Limitaciones, Prohibiciones y uso no Autorizado ..... 44
9. Responsabilidades de Microsystem S.A ..... 44
10. Privacidad y Protección de los Datos ..... 46
11. Derechos de los titulares ..... 46
12. Declaración de las garantías y seguros ..... 47
13. Políticas de Seguridad ..... 47
14. Fiabilidad del Mecanismo Complementario de Verificación de Identidad para Emisión de Firma Electrónica Avanzada en Línea ..... 48
15. Datos de Contacto ..... 49
16. Documentos de referencia ..... 49
17. Control de Cambios ..... 50

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

# 1. Introducción

## 1.1. Presentación

Microsystem S.A. opera como Prestador de Servicios de Certificación (Autoridad Certificadora) para atender a una comunidad de usuarios, más adelante denominados titulares.

Este documento de Políticas de Certificación (PC) detalla las condiciones, procesos y normas[1] que se aplican en los procesos relacionados con la emisión y el uso de certificados de Firma Electrónica Avanzada de Microsystem S.A.

## 1.2. Identificación de este documento

El presente documento se denomina "Políticas de Certificación de Firma Electrónica Avanzada" de Microsystem S.A., las que internamente se citan como PC o PC-FEA y están registradas con el número único internacional (OID) 1.3.6.1.4.1.54151.1.10.

Microsystem S.A. tiene asignado el identificador (OID) 1.3.6.1.4.1.54151, el cual está registrado en la Internet Assigned Number Authority (IANA). Este número identifica únicamente a Microsystem S.A. en un contexto global.

## 1.3. Objetivo

Microsystem S.A. establece esta política, en conjunto con el documento **ME-DG-PO02 Declaración de Prácticas de Certificación**, como los instrumentos para definir las reglas aplicables para la solicitud, validación, aceptación, entrega, emisión, suspensión y revocación de los certificados, así como las restricciones y aplicaciones en las cuales se deben utilizar.

## 1.4. Alcance

Esta política explica las características de los servicios de certificación de Microsystem S.A. relacionados con los certificados de Firma Electrónica Avanzada emitidos por Microsystem S.A., cómo se otorgan los certificados, los mecanismos de verificación fehaciente de la identidad, los derechos y obligaciones de las partes, y detalla los servicios disponibles para la comunidad de usuarios de estos certificados.

El detalle de cómo el PSC, los titulares de los servicios de certificación y las partes que confían, deben cumplir con éstas **Políticas de Certificación** (CP - Certification Policies) está descrito en el documento **ME-DG-PO02 Declaración de Prácticas de Certificación** (CPS - Certification Practice Statement), que también aplica para todo lo demás no previsto expresamente por el documento presente.

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

[1] REGLAMENTO DE LA LEY 19.799 SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y LA CERTIFICACIÓN DE DICHA FIRMA



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

### 1.5. Roles y responsabilidades

El funcionamiento de los servicios de certificación del PSC Microsystem S.A. está plenamente respaldado por el Directorio de la empresa que mediante su Gerente General ha designado 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 y responsabilidades de acuerdo a lo establecido en en el punto **9. Controles de Personal del PSC** del documento **ME-DG-PO02 Declaración de Prácticas de Certificación**.

El Directorio se reúne periódicamente para revisar la operación de la Empresa.

### 1.6. Administración de la política

1.6.1. La revisión de este documento se realiza al menos una vez al año o según sea necesario para mantener en sintonía con otros documentos relacionados.

1.6.2. Las políticas de certificación contenidas en este documento son administradas y mantenidas por el personal designado por el Comité de Seguridad. 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.

1.6.3. 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

## 2. Glosario

**PC - Políticas de Certificación (CP - Certification Policies)**: Consiste en el conjunto de condiciones, procesos y normas que se aplican en los procesos de emisión y uso de certificados de Firma Electrónica Avanzada emitidos por Microsystem S.A.

**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 PC 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.



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

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, 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 certificados intermedios 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



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

**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 15.10 de esta política, RFC 6960, y se encuentra en el registro de los 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 una declaración o un 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 (Token criptográfico)**: Un dispositivo criptográfico es un dispositivo físico utilizado para proteger y acceder a un recurso restringido electrónicamente.

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



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

# 3. Partes Involucradas de PKI de Firma Electrónica Avanzada

## 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 Servicio de Certificación de Firma Electrónica Avanzada demuestre que cumple con los requisitos necesarios para desempeñar su rol. En particular, debe acreditar que el Prestador de Servicios de Certificación cuenta tanto con las instalaciones, sistemas, programas informáticos, y recursos físicos y humanos necesarios con el fin de otorgar el certificado de firma electrónica avanzada, permitiendo su inscripción en el registro de certificados acreditados.

## 3.2. Prestador de Servicio 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 política 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 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, estas **Políticas de Certificación (PC)** y la **Declaración de Prácticas de Certificación** (DPC) vigente. La recepción de la solicitud puede ser una de las siguientes:

- Interna Presencial - 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 confianza 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 se solicitarán antecedentes complementarios, tal como se explica en el proceso para la solicitud de un certificado (Solicitud de Certificado de FEA).



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

### 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; la clave privada está asociada a la clave pública de este certificado.

### 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 página del **Portal CA** de Microsystem: https://portal.ca.msys.cl

### 3.7. Partes que Confían - Modelo de Confianza

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 una Firma Electrónica Avanzada verificable con referencia a una clave pública que figura en el certificado del titular.

Las partes confiantes cumplen con obligaciones específicas como se describe en esta política.

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 previamente validar que el certificado fue emitido por Microsystem S.A. u otro PSC acreditado, utilizando como referencia la información publicada en el sitio de la Entidad Acreditadora (https://www.entidadacreditadora.gob.cl/) en la sección Certificados Raíces y la página con el listado de los PSC acreditados. Luego de confirmar el origen del certificado, se debe consultar información de revocación del certificado utilizando información de referencia contenida en el mismo certificado del firmante, tal como la lista de revocación de certificados CRL o un servicio de consulta de estado OCSP. Las validaciones de vigencia deben ser también aplicadas a todos los certificados intermedios entre el certificado raíz y el certificado de entidad final.

Documentación, aplicativos y manuales relacionados con la confianza en la FEA están disponibles en las páginas del sitio: https://portal.ca.msys.cl

### 3.8. Diagramas de las interacciones entre partes



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

**Diagrama de las interacciones en el proceso de solicitud y emisión de certificado**

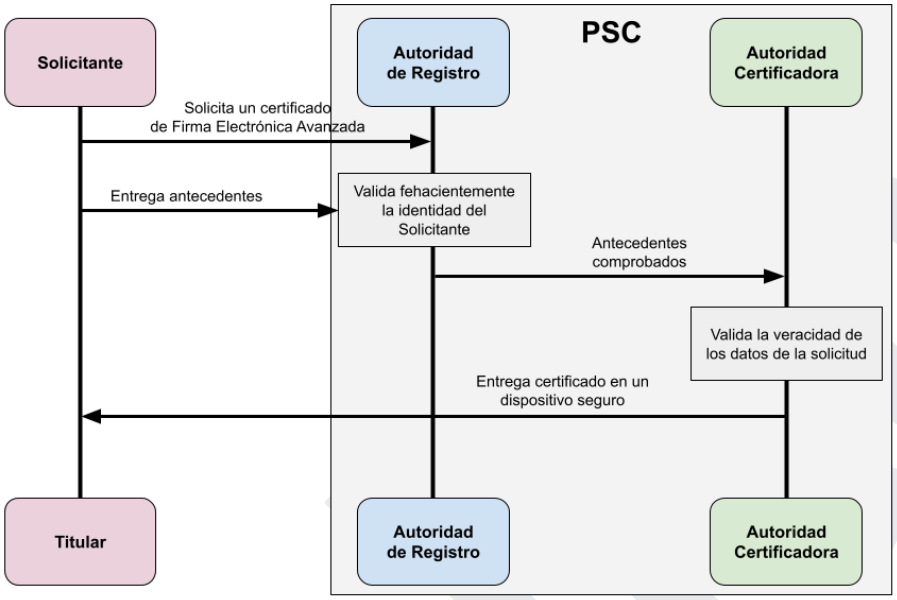
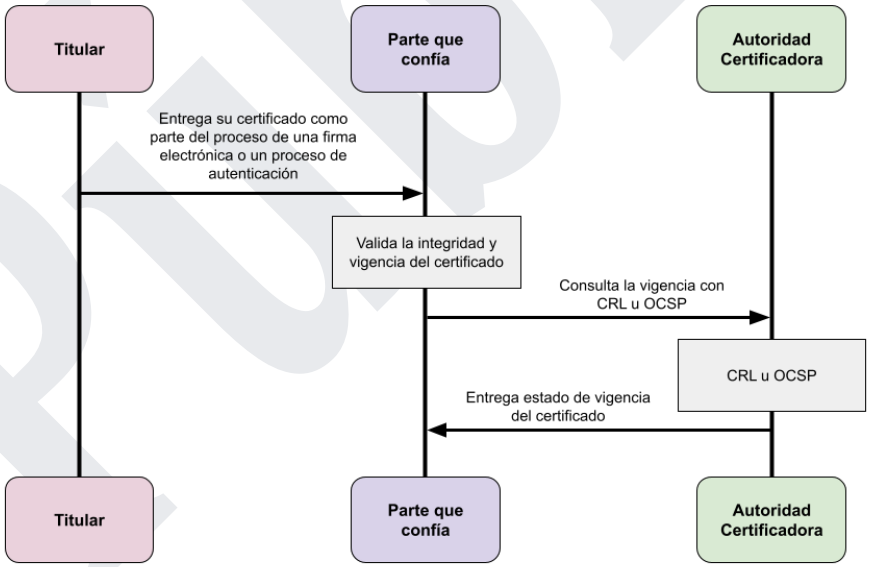



**Diagrama de las interacciones entre partes durante uso de un certificado**




Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

# 4. Ciclo de vida de un certificado de FEA

## 4.1. 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 deberá acudir a las oficinas del PSC a realizar el proceso de registro.

Presencial en terreno en domicilio del solicitante, donde el solicitante deberá realizar un agendamiento para que un Operador de Registro de la Autoridad de Registro realice el proceso de registro 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.

### 4.1.1. Registro Presencial en las Oficinas del PSC

4.1.1.1. El Solicitante inicia el proceso de registro realizando agendamiento de la visita a las oficinas del PSC a través del formulario habilitado por Microsystem y proporciona la siguiente información: Nombre, Apellido, Email, Teléfono, y detalles de la solicitud.

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

4.1.1.3. 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.

4.1.1.4. 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.

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

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

4.1.1.7. En el caso que el Solicitante cuente con un dispositivo criptográfico propio, este le facilita el dispositivo correspondiente al Operador de Registro, quien lo



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

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.

4.1.1.8. 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.

4.1.1.9. El Operador de Registro procede con la captura de la fotografía del Solicitante.

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

4.1.1.11. 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.

4.1.1.12. 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.

4.1.1.13. 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 4.1.1.11, y que se encuentran en control exclusivo del este mismo. Los factores que permiten la instalación de describen a continuación:

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

**4.1.1.13.2.** 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.

4.1.1.14. 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 del dispositivo para proteger su Firma Electrónica Avanzada y



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

tener el control exclusivo de esta. Se entiende, que si el dispositivo no es nuevo, el Solicitante tiene un control exclusivo de éste, según estipulado en el punto 7.6.6.

4.1.1.15. En presencia del Operador de Registro, mediante el Portal de Usuario de Firma Electrónica Avanzada, utilizando las claves del punto 4.1.1.13 y la clave del dispositivo criptográfico en control absoluto de éste, 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.

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

### 4.1.2. Registro Presencial en Terreno en Domicilio del Solicitante

4.1.2.1. El Solicitante inicia el proceso de registro realizando agendamiento de la visita en terreno a través del formulario habilitado por Microsystem https://www.microsystem.cl/firma-electronica-digital-avanzada/ y 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, copia 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.

4.1.2.2. La Autoridad de Registro requiere al Solicitante, mediante llamada telefónica, 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.

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

**4.1.2.3.1.** Valida la vigencia del documento en el SRCel y adjunta la evidencia a la solicitud.

**4.1.2.3.2.** Imprime el contrato de suscripción para ser firmado en terreno por el solicitante.

4.1.2.4. El Solicitante deberá recibir al personal de Microsystem, quien portará una credencial que lo identifica como Operador de Registro del PSC, en el Domicilio donde se solicitó el registro presencial, en la hora y día acordado.

4.1.2.5. 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, procede a capturar los datos de la cédula de identidad del



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

Solicitante, correspondiente al mismo RUN, y número de serie de la cédula de identidad proporcionados en la solicitud de agendamiento, mediante lectura digital (en caso de las cédulas electrónicas) o ingreso manual (para cédulas no electrónicas), y comprueba fehacientemente la identidad del solicitante verificando su nombre contra los datos capturados desde la cédula.

4.1.2.6. 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.

4.1.2.7. 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.

4.1.2.8. El Operador de Registro procede con la captura de la fotografía del Solicitante.

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

4.1.2.10. El Operador de Registro coordina con un Operador de Validación y solicita que revise fehacientemente la solicitud comprobando la veracidad de los datos. Siendo correcta la información entregada, se autoriza la emisión del certificado.

4.1.2.11. La Autoridad Certificadora le envía al solicitante 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:

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

**4.1.2.11.2.** 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.

4.1.2.12. 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 del dispositivo para proteger su Firma Electrónica Avanzada y



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

tener el control exclusivo de esta. Se entiende, que si el dispositivo no es nuevo, el Solicitante tiene un control exclusivo de éste, según estipulado en el punto 7.6.6.

4.1.2.13. En presencia del Operador de Registro, mediante el Portal de Usuario de Firma Electrónica Avanzada, utilizando las claves del punto 4.1.2.11. y la clave del dispositivo criptográfico en control absoluto de éste, 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.

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

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

4.1.3. **Registro en Línea a través del Sistema ClaveÚnica.**

4.1.3.1. 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**.

**4.1.3.2.** 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.

**4.1.3.3.** 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**.

**4.1.3.4.** El proceso empieza con el **Operador Virtual de Registro**:

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

**4.1.3.4.2.** 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.

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

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

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

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

**4.1.3.4.3.4.** Fecha de nacimiento.



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

**4.1.3.4.3.5.** código de convenio (Opcional) – para validar si tiene un código de convenio vigente que lo exime del pago por el importe del certificado.

**4.1.3.4.4.** 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.

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

**4.1.3.5.1.** A continuación el Solicitante deberá elegir un mecanismo complementario digital de comprobación de identidad, pudiendo ser este:

**4.1.3.5.1.1.** Responder en línea preguntas personales de seguridad, mediante un mecanismo de preguntas y alternativas de respuesta desplegados en pantalla. Servicio que es proporcionado por un proveedor externo.

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

**4.1.3.5.1.2.1.** Si la emisión del certificado está afecta a pago, el Solicitante deberá seleccionar la vigencia y certificado 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).

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

**4.1.3.5.1.2.1.1.** 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.

**4.1.3.5.1.2.2.** Si la emisión del certificado estuviese exenta de pago, el Solicitante deberá realizar un proceso de autenticación en una cuenta bancaria registrada a su nombre a través de la plataforma Khipu, quedando registrado si la autenticación fue correcta (Dando origen a una verificación correcta) o fue incorrecta (Interrumpiendo el proceso de emisión).

**4.1.3.5.2.** Valida la vigencia de la **Cédula de Identidad** utilizando el número de serie del documento proporcionado por el Solicitante.

**4.1.3.5.3.** Si el Solicitante hubiese realizado el procedimiento mediante el mecanismo complementario de responder en línea preguntas personales de seguridad, en esta etapa del proceso deberá realizar el pago del importe del servicio de emisión de certificado en línea, indicado en https://www.microsystem.cl/firma-electronica-digital-avanzada/, mediante plataforma de pago vigente. O quedará exento de pago si tuviese un código de convenio vigente con Microsystem S.A.

**4.1.3.5.3.1.** Si la emisión del certificado está afecta a pago, el Solicitante deberá seleccionar la vigencia y certificado y mediante la plataforma de pago vigente, quedando registrado si el pago fue correcto (Dando origen a una verificación correcta) o fue incorrecto (Interrumpiendo el proceso de emisión).

Publico



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

4.1.3.5.3.1.1. 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.

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

**4.1.3.5.5.** Una vez validada la identidad del Solicitante, este deberá ingresar un PIN personal e intransferible para la protección de su certificado de Firma Electrónica Avanzada (FEA), junto con una **clave OTP** enviada como segundo factor de autenticación al teléfono móvil registrado. En este mismo proceso, el certificado y su llave privada quedan activados y almacenados de forma segura en **Cloud Signer de Microsystem S.A.**, servicio que utiliza un módulo criptográfico certificado y operado bajo la norma FIPS 140-2 Level 3 para la gestión y protección de las llaves privadas de sus suscriptores. Las llaves privadas se encuentran protegidas mediante mecanismos criptográficos y, adicionalmente, cada llave privada está protegida por el PIN definido por su titular. Finalizado exitosamente este proceso, el Solicitante adquiere la calidad de **Usuario Titular** y queda habilitado para operar con su certificado de Firma Electrónica Avanzada a través de Cloud Signer.

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

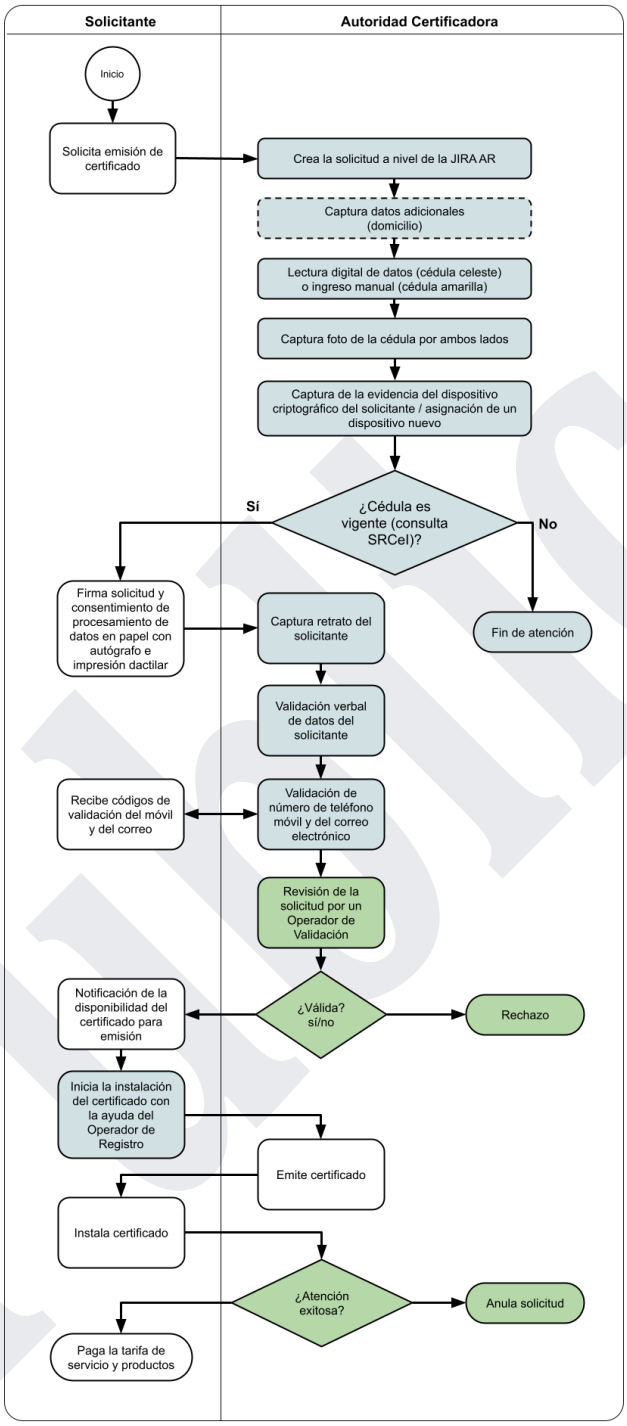



Diagrama Registro Presencial en las Oficinas del PSC y Registro Presencial en Terreno en Domicilio del Solicitante.



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

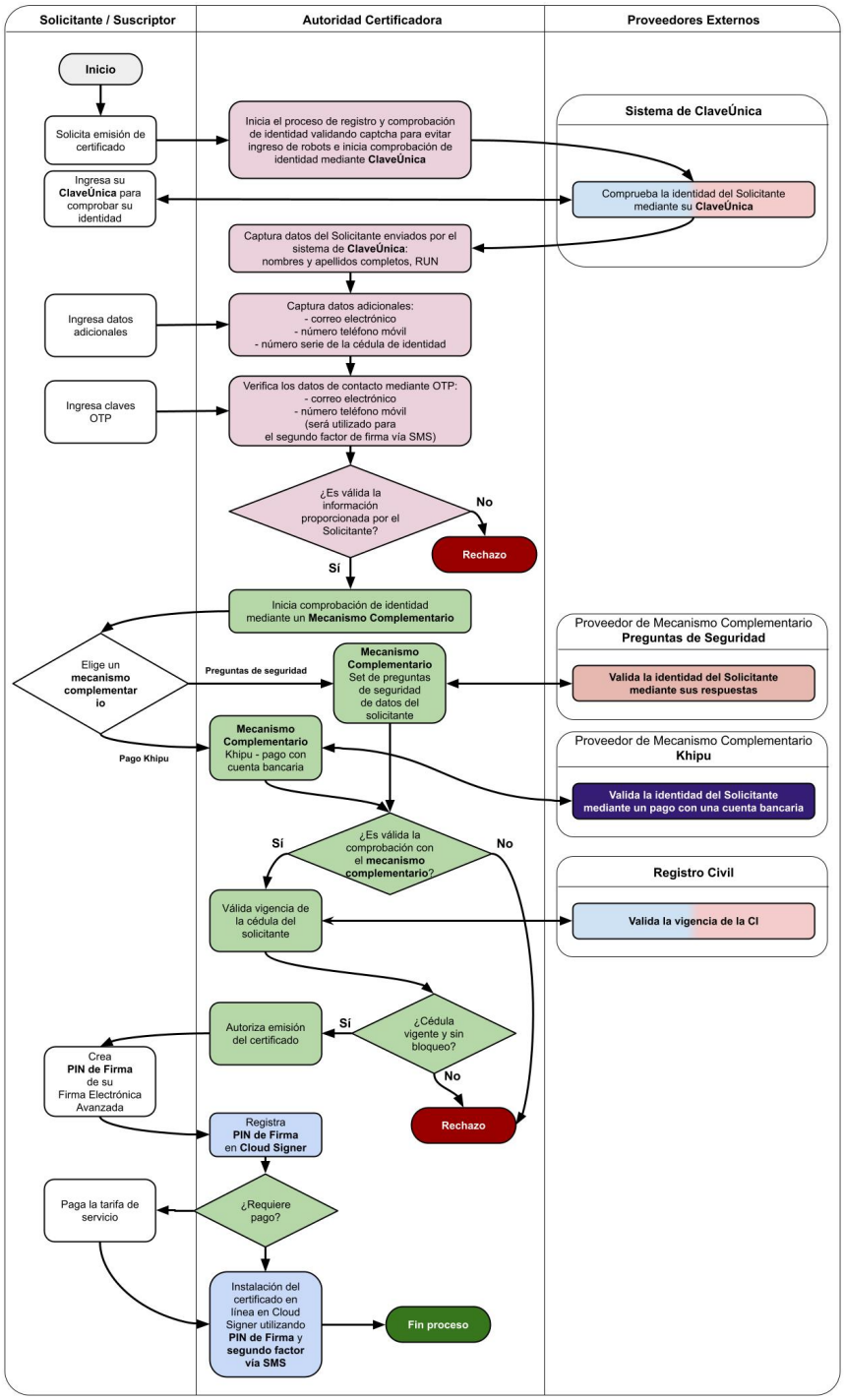



Diagrama Registro en Línea a través de Sistema ClaveÚnica.



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

## 4.2. 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 4.1.1.13.1 y Registro Presencial en Terreno en Domicilio del Solicitante en el punto 4.1.2.11.1) y clave de instalación del certificado (descrita para Registro Presencial en las Oficinas del PSC 4.1.1.13.2 y Registro Presencial en Terreno en Domicilio del Solicitante en el punto 4.1.2.11.2).

## 4.3. Periodo de Vigencia

El periodo de vigencia de un certificado está determinado por sus fechas de emisión y expiración, sin perjuicio de los periodos de suspensión o de su eventual revocación. Durante su vigencia, el certificado y su llave privada podrán ser utilizados para los usos autorizados.
Los certificados emitidos por Microsystem S.A. podrán tener una vigencia de 1, 2 o 3 años, de acuerdo con el periodo seleccionado por el solicitante al momento de contratar el servicio.
Asimismo, Microsystem S.A. podrá emitir certificados con una vigencia de 7 o 30 días, conforme a las condiciones y políticas comerciales establecidas por el PSC Microsystem para la prestación de sus servicios de Firma Electrónica Avanzada (FEA).
En todos los casos, el periodo de vigencia se contabilizará a partir de la fecha de emisión del certificado.

## 4.4. Suspensión y Revocación de Certificados de FEA

4.4.1. **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:

4.4.1.1. 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.

4.4.1.2. Mediante una acción de suspensión disponible en el **Portal de Usuario de Firma Electrónica Avanzada,** ingresando con sus credenciales de acceso.



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

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

4.4.2. **Revocación por Titular** - 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:

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

4.4.2.2. Mediante una acción de revocación disponible en el **Portal de Usuario de Firma Electrónica Avanzada,** ingresando con sus credenciales de acceso y haciendo uso del código de revocación.

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

4.4.4. **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.

4.4.5. **Revocación por orden judicial.**

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

## 4.5. 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.

## 4.6. Renovación

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

## 4.7. Renovación de un Certificado Revocado

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



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

### 4.8. Expiración

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

### 4.9. 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.

## 5. 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.

### 5.1. Formato del certificado de FEA

5.1.1. 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.

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

### 5.2. Extensiones de certificado de FEA

5.2.1. 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:

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

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

5.2.2. 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.

5.2.3. 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.



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

### 5.3. Extensiones críticas de certificado de FEA

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

5.3.1. Mostrar si un certificado está destinado a una CA o no.

5.3.2. Mostrar el uso previsto de la clave.

5.3.3. Prohibir cualquier uso del certificado inconsistente con las Políticas y Prácticas de Firma Electrónica Avanzada de Microsystem S.A.

### 5.4. 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** | 69:db:06:50:35:5f:32:5f:43:64:2c:8e:51:63:4e:76:51:b3:1d:24 |
| **ID Algoritmo de firma** | SHA256withRSA |
| **Validez** | |
| **No antes de** | Jan 5 17:03:52 2023 GMT |
| **No después de** | Jan 20 17:03:52 2024 GMT |
| **Emisor** | |
| **E-mail** | soportepki@microsystem.cl |
| **Nombre común** | Microsystem Firma Electronica Avanzada - P1 |
| **Unidad organizacional** | 94099000-9 |

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

| | |
|---|---|
| **Unidad organizacional** | Autoridad Certificadora |
| **Organización** | Microsystem S.A. |
| **Localidad** | Santiago |
| **Región** | Region Metropolitana |
| **País** | CL |
| **Sujeto titular** | |
| **E-mail** | rgonzalez@microsystem.cl |
| **Nombre común** | RICARDO ALEJANDRO GONZÁLEZ CORDERO |
| **Número de serie** | 16750106-0 |
| **Título** | PERSONA NATURAL |
| **País** | CL |
| **Llave pública** | |
| **Algoritmo** | RSA |
| **Largo** | 2048 |

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

| | |
|---|---|
| **Módulo** | 00:92:d4:ce:8b:1d:5f:c5:7a:7b:0e:ae:45:58:d9:<br>46:b3:15:99:10:2e:c2:b9:5a:d4:ed:3c:af:0f:8b:<br>7c:50:3b:87:88:0e:77:90:61:2a:ad:5e:d7:64:95:<br>2d:c3:c8:a5:03:57:3a:8f:c7:a8:55:04:52:84:4c:<br>2d:f5:91:32:c6:2d:9e:d2:e0:00:57:5b:71:80:6a:<br>ed:74:17:3d:93:e3:27:db:9a:21:c8:ae:f7:88:b9:<br>ae:c7:61:1d:31:cf:e5:16:2c:02:17:24:9c:73:c0:<br>73:2c:f8:d0:91:d9:f0:07:e4:6e:05:41:f6:8b:da:<br>b8:36:c6:86:58:12:f2:ae:f3:5c:08:0e:61:10:71:<br>13:fb:2d:5e:33:c0:b6:a9:79:97:dd:8c:d9:93:5d:<br>68:d4:1a:41:b3:03:c7:7c:f6:4c:38:9a:3d:53:ac:<br>61:dd:57:f1:7b:e6:4e:53:99:ff:64:d8:47:37:b4:<br>af:13:81:8f:50:ca:1d:2d:5f:46:7c:be:63:ef:55:<br>3f:6b:e4:d0:04:42:30:72:67:7d:71:73:a4:67:96:<br>cd:47:65:7d:87:3f:2d:4b:7f:27:ce:e4:b1:b8:c6:<br>e3:f3:b0:a2:72:39:3d:90:ff:9e:4f:37:b1:1b:28:<br>a2:77:8e:ac:a2:a1:74:58:53:4f:7b:2e:3e:d1:41:<br>f0:2f |
| **Exponente** | 65537 (0x10001) |
| **Firma del certificado** | |
| **Algorithm** | SHA256withRSA |
| **Valor de firma** | 7b:e7:88:55:b1:1e:62:f9:09:10:48:5c:a2:6b:59:33:bb:8e:<br>9a:28:17:c1:f5:65:d7:fc:24:0c:65:49:0d:16:8d:d5:e0:43:<br>c1:14:24:bb:29:18:13:5d:44:7d:b2:fb:72:56:41:03:11:2b:<br>1d:b1:08:d3:87:30:8f:32:c6:a3:54:9c:51:7f:c1:4f:3b:4e:<br>74:15:db:45:ce:bc:e8:0d:62:5b:e1:6d:8f:81:85:40:0e:1b:<br>3c:34:1b:fc:9d:5e:7c:4c:1c:e1:8f:ea:2d:53:07:80:ca:61:<br>c7:49:52:16:1d:6a:0d:d4:cb:99:26:68:f3:0d:85:c7:5e:8c:<br>b2:a2:89:b4:35:a5:b6:88:16:0c:fa:b3:11:8b:7f:cd:3e:9f:<br>9d:6b:11:be:55:3f:43:9b:ad:ec:f1:f6:89:3a:4b:fc:6e:db:<br>fa:09:fb:90:10:ca:71:df:50:97:58:75:1c:a4:12:8f:d6:22:<br>29:3f:e0:f6:b7:6d:89:e3:50:c8:d9:34:7d:48:d4:91:23:46:<br>2f:27:cb:eb:45:9e:06:22:bc:b6:d9:74:c1:3d:dd:ab:af:d5:<br>51:f8:48:78:0a:13:70:ad:a6:c8:8d:4f:10:a6:5c:03:cf:61:<br>68:53:e7:da:0c:f8:f6:dd:cc:f1:a5:9a:c9:50:81:96:ce:a1: |



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

| | |
|---|---|
| | 2e:02:c7:d0 |
| **Extensiones** | |
| **restricciones básicas** | - |
| **identificador de la llave de la autoridad** | keyid:64:25:20:5B:C5:C9:59:D7:C8:4F:4D:19:2D:4D:E0:91:22:EC:84:E9 |
| **información de la autoridad, ubicación de la cadena emisora y del servicio OCSP** | **cadena de confianza:**<br>http://portal.ca.msys.cl/Microsystem_Firma_Electronica_Avanzada_-_P1.p7c<br>**ocsp:**<br>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<br>**CPS:** https://www.microsystem.cl/cps<br>**mensajes para usuarios:**<br>**texto=**'Certificado para Firma Electronica Avanzada. Resolucion exenta XXX del XX de XXXX de XXXX, Subsecretaria de Economia, Fomento y Reconstruccion.'<br>**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** | 73:5A:29:B5:4C:8C:05:F7:16:1F:98:C2:BE:04:FA:BE:93:CA:89:9F |
| **usos de llave** | digitalSignature,nonRepudiation,keyEncipherment,dataEncipherment,keyAgreement |

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

| | |
|---|---|
| **nombre alternativo del emisor, RUT de la autoridad emisora según establecido en el DECRETO Nº 181** | oid=1.3.6.1.4.1.8321.2<br>tipo=IA5_STRING<br>texto='94099000-9' |
| **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<br>tipo=IA5_STRING<br>texto='16750106-0' |

### 5.5. 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** | **Last Update:** | Jan 20 06:13:20 2023 GMT |



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

| | | |
|---|---|---|
| **la lista** | | |
| **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:<br>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:<br>368D8AE9BA11D03D5A8BD4284F141274F870A6E5<br>Revocation Date: Aug 5 21:46:37 2022 GMT |
| **Un ejemplo de un certificado suspendido (Hold)** | | Serial Number:<br>0D30C5A926E368BFF819C57D00A008FFDBE51277<br>Revocation Date: Aug 5 21:38:13 2022 GMT<br>CRL entry extensions:<br>X509v3 CRL Reason Code:<br>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:<br>0b:94:39:54:39:08:c2:2e:35:d8:03:c2:ee:78:5b:ed:b5:39:<br>ef:17:c4:01:6e:02:23:3e:1b:18:17:7b:7d:b1:44:15:e4:5c:<br>82:79:a4:21:0e:a1:2e:80:ab:22:a6:b4:92:f2:ed:72:06:6b:<br>8a:00:b7:8a:61:40:3e:df:ae:1e:62:be:06:f7:3a:1d:be:1a:<br>e8:2a:b6:a6:90:60:2b:cc:7b:16:c7:30:1d:2e:d7:aa:d8:8a:<br>0a:44:9e:5b:a2:55:9c:26:d3:e2:4e:dd:87:44:7d:25:b1:5f:<br>2a:0e:53:94:81:53:f4:b9:dc:a2:85:3f:1c:c3:b3:43:49:6f:<br>e3:78:43:c0:1f:08:a9:cd:5a:34:a3:6e:99:3f:58:4c:dc:57:<br>46:80:02:2d:d7:cf:e4:bd:17:82:b7:24:a5:a0:9f:fe:9d:77:<br>34:32:f2:14:08:ef:1f:06:a7:15:ea:1a:ab:30:63:26:fb:6e:<br>ba:df:6b:6c:35:dd:99:f4:1c:4e:70:51:21:e5:a8:93:8a:a8:<br>68:ee:13:fe:ed:f3:49:1c:74:e9:f9:38:c9:41:b3:09:8f:b3:<br>e8:2c:a4:94:01:c9:5c:f2:e5:92:1c:d8:25:b5:5a:01:80:6a:<br>4a:80:c8:2c |



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

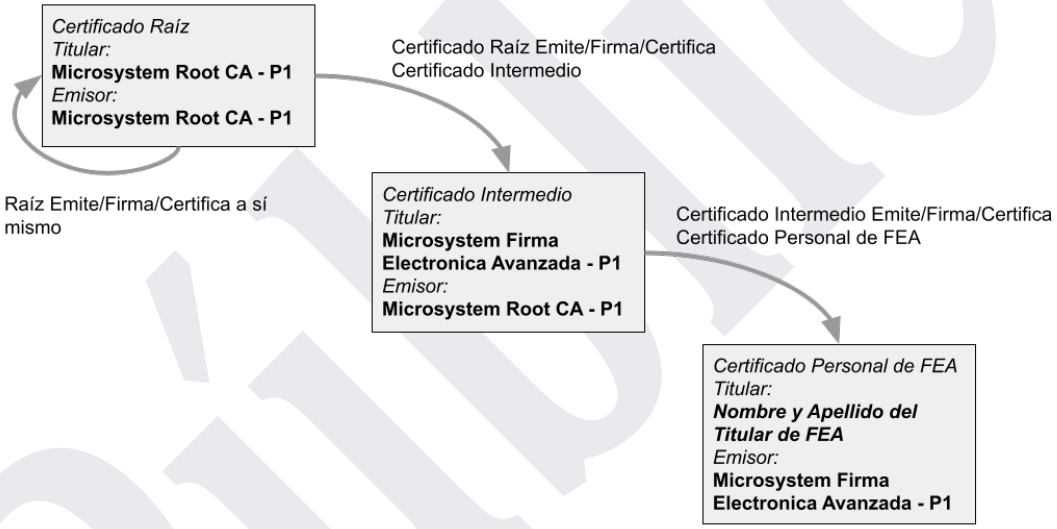
Público

## 5.6. 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.

## 5.7. 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.




5.7.1. 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 |



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

| | |
|---|---|
| **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 |

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

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

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

| | |
|---|---|
| | 4d:bb:2c:34:65:9a:9e:6b:89:e4:0d:61:d8:0d:e3:<br>23:74:ae:73:03:6f:6b:13:5a:37:bb:d5:97:c5:2e:<br>2a:c7:78:98:73:37:f1:95:80:4e:df:3e:be:40:37:<br>b1:77:37:ca:e4:cb:c6:a6:02:47:fb:db:31:ac:c2:<br>3d:35:c2:5a:81:72:9c:93:31:67:1e:b3:ae:98:45:<br>8d:f0:53:ad:90:e8:68:3d:6e:77:97:88:35:d8:72:<br>73:a6:19:b7:bc:93:59:7e:1f:ea:5a:dc:7c:82:24:<br>28:43:3f:70:35:97:79:9b:ac:ed:79:b4:0b:41:fd:<br>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:<br>20:d2:a8:a4:f1:e7:23:53:5c:9c:63:e3:66:59:69:10:a6:6c:<br>48:3f:3b:4f:c8:9d:4a:d8:cd:51:8b:52:07:aa:34:4a:a2:4f:<br>64:17:23:3c:ed:2d:31:ae:4c:39:3d:36:f9:42:d7:97:52:b8:<br>d1:2e:1c:d5:3e:4c:44:e9:a7:ce:4f:b1:a8:f1:e0:d9:e6:97:<br>69:60:8b:1d:f4:86:db:f1:ff:ef:27:97:3f:3a:b7:9e:3f:89:<br>46:ae:78:ad:c9:f0:3e:76:05:3f:62:17:01:4e:e8:4b:4c:17:<br>60:0f:56:cf:cd:66:98:16:78:63:12:b0:de:ea:ec:7c:f4:47:<br>3a:dd:e4:cc:11:46:3c:93:06:a6:a4:c2:1c:6d:7f:44:a9:66:<br>66:b5:4d:f6:e3:1a:ac:2a:b5:51:03:6a:6e:87:d5:5d:13:74:<br>f5:48:62:e9:94:63:c8:b2:02:25:07:eb:75:ac:b2:14:41:b1:<br>3e:21:d8:a8:39:35:da:48:9d:50:69:8d:e9:56:1c:7f:ae:fa:<br>48:e6:ac:92:93:1f:04:3c:d7:6c:0e:e0:82:d8:f3:35:12:b9:<br>13:10:ff:5e:e6:17:fc:d5:a1:97:22:8c:74:10:15:41:cb:4a:<br>89:7a:89:74:93:c6:ac:c9:9e:a0:92:94:09:9e:7b:9e:1c:4c: |

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

| | |
|---|---|
| | 41:9a:0b:d1:6b:a4:07:24:e8:1e:01:cf:d4:ce:34:22:83:c7:<br>18:f8:c2:7a:61:d9:fe:dd:44:2e:48:0e:f6:ce:ee:ab:bd:64:<br>ab:e3:c1:44:c2:ef:52:f3:ae:a4:01:14:2d:e1:6c:ca:b4:a3:<br>0d:da:2a:5d:41:ad:f7:72:48:eb:5d:f2:5c:3c:97:4b:58:51:<br>cf:08:70:09:85:94:22:49:8b:c6:d3:90:f1:87:58:78:c9:bc:<br>8b:40:bd:f6:ab:4e:73:0b:a4:bb:a5:ed:2d:67:7f:f7:3b:f4:<br>be:82:10:6f:a7:23:f5:f5:3a:c0:a0:ba:57:b0:96:f6:9a:1f:<br>f5:be:83:88:50:54:d8:d8:85:9a:b2:ac:4d:47:fc:95:73:10:<br>83:49:64:d3:65:9d:a0:7a:be:1e:c9:3d:58:ac:63:2c:f8:e8:<br>16:d8:a8:5c:a7:c8:0f:1b:9c:4b:71:bd:e8:66:a5:af:a3:3f:<br>9a:b3:e8:b8:54:95:51:d2:4f:56:ae:a3:43:f4:40:af:3f:1c:<br>e5:8b:74:8f:15:a5:80:cf:13:b0:f0:e5:b7:35:e4:77:c8:54:<br>11:47:70:51:b8:9b:19:c0:49:f4:72:9b:b2:c8:82:08:b3:1b:<br>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:<br>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<br>**CPS:** https://www.microsystem.cl/cps<br>**mensajes para usuarios:**<br>**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:<br>F3 |
| **huella digital SHA1** | 328a79d91057a38bd468e18a684c74f6c9be3155 |



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

5.7.2. 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 |

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

| | |
|---|---|
| **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 |

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

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



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

| | |
|---|---|
| | 06:65:bd:f1:8d:c2:1d:1c:6d:b3:ff:9f:13:46:f6:fb:6d:e9:<br>9c:fe:26:74:2f:85:2d:eb:e7:d7:18:f3:42:64:18:1a:1c:02:<br>ae:49:15:22:a4:77:3d:26:86:9c:72:ab:74:80:6b:07:48:b6:<br>2a:45:36:c4:e6:22:25:c6:96:08:12:d0:d9:6a:14:80:32:0a:<br>55:2a:b0:da:9e:e8:b5:28:21:01:26:84:95:82:be:c6:f7:04:<br>46:09:82:77:e2:b3:4d:58:2d:08:f7:9b:3f:e5:d1:29:10:52:<br>c2:e9:37:dd:da:34:b9:9b:1b:e3:42:f7:7a:ea:cf:d8:5a:f4:<br>9f:18:9e:e1:35:c8:2a:fa:d7:7d:ca:36:9b:23:88:46:ed:a6:<br>e0:c5:55:05:84:6b:30:3a:9b:67:bb:39:bb:fd:e1:57:ce:17:<br>e7:74:a6:61:12:38:d0:ac:a2:4e:2d:cf:c6:9e:02:5b:8b:d9:<br>1a:df:b9:4e:57:0d:aa:95:d8:39:e7:4b:f3:a5:43:23:f1:a9:<br>ec:5d:eb:1d:f4:52:86:8d:e6:98:01:4b:bc:4f:c3:07:68:d2:<br>ea:df:a5:01:81:8e:61:11:29:c9:a8:8a:fc:2e:07:0a:d8:4f:<br>85:1a:33:27:80:c3:c2:2c:4f:14:9a:f0:9f:90:ad:83:d0:d5:<br>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:<br>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<br>**CPS:** https://www.microsystem.cl/cps<br>**mensajes para usuarios:**<br>**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:<br>E9 |



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

| | |
|---|---|
| **huella digital SHA1** | 853a0ae67ecace2cc3b44e9b8746d66f9bee00b9 |

# 6. Usos del Certificado de Firma Electrónica Avanzada

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:

## 6.1. 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.

## 6.2. 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.

## 6.3. 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.

# 7. Obligaciones de las partes

## 7.1. Microsystem S.A. como PSC

7.1.1. 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.

7.1.2. Microsystem S.A. debe mantener un repositorio de acceso público de los certificados emitidos en su calidad de PSC, por medio del sitio web



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

https://portal.ca.msys.cl/, dejando en evidencia el estado de los certificados emitidos: vigente, revocado, suspendido.

7.1.3. Microsystem S.A. debe proteger toda la privacidad de la información relevante de los Titulares y Solicitantes. El detalle de esta obligación se describe en el apartado Privacidad y Protección de los Datos.

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

7.1.5. 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 Registro Presencial de la presente PC.

7.1.6. 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.

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

7.1.8. 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** del documento **ME-DG-PO02 Declaración de Prácticas de Certificación**.

7.1.9. 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** del documento **ME-DG-PO02 Declaración de Prácticas de Certificación**.

7.1.10. 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.

7.1.11. 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.

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

7.1.13. 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.



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

7.1.14. 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.

## 7.2. Microsystem S.A. como Autoridad Certificadora (AC)

7.2.1. 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 PC y DPC correspondiente.

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

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

7.2.4. 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.

7.2.5. 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 la información actualizada de acuerdo a su vigencia y disponibilizar el servicio de consulta en línea de vigencia de certificados OCSP.

7.2.6. 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.

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

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

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

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

7.2.11. 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.

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

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



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

## 7.3. Microsystem S.A. como Autoridad de Registro

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

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

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

7.3.4. 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 FEA.

7.3.5. 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.

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

7.3.7. Formalizar el acuerdo contractual (punto **Contrato de Suscripción de Firma Electrónica Avanzada** del documento **ME-DG-PO02 Declaración de Prácticas de Certificación**) con el Titular previo a la emisión del certificado.

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

## 7.4. Partes que confían

7.4.1. 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/).

7.4.2. 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.

7.4.3. 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.

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

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

## 7.5. Solicitante

7.5.1. 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/).

7.5.2. 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.

## 7.6. Titular

7.6.1. 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/).

7.6.2. Utilizar de forma adecuada el certificado de FEA, ya sea para fines legales u otros autorizados en conformidad con la presente PC (Usos del Certificado de Firma Electrónica Avanzada).

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

7.6.4. 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.

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

7.6.6. Custodiar adecuadamente los mecanismos de seguridad (dispositivo criptográfico, 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.

7.6.7. 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.

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

7.6.9. 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:

7.6.9.1. Pérdida, robo o extravío del dispositivo que almacena la llave privada.

7.6.9.2. Pérdida de control sobre dicha llave.

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

Público



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

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

7.6.9.5. 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.

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

7.6.11. 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.

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

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

7.6.14. Sin limitar otras obligaciones establecidas en la presente PC, los Titulares tienen el deber de abstenerse de cualquier manipulación en los certificados presentados para engañar o defraudar a terceros.

7.6.15. 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.

# 8. 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.

# 9. Responsabilidades de Microsystem S.A

## 9.1. Responsabilidades

9.1.1. 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



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

avanzada y documentos electrónicos, por un monto igual al solicitado por la Entidad Acreditadora.

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

9.1.3. 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.

9.1.4. 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.

9.1.5. 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.

## 9.2. Limitación de Responsabilidad

9.2.1. 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.

9.2.2. 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** del documento **ME-DG-PO02 Declaración de Prácticas de Certificación**.

## 9.3. 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.

9.3.1. Archivos sujetos a publicación frecuente o periódica

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



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

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

9.3.1.3. 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

9.3.2. Archivos sujetos a publicación esporádica según sufran cambios

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

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

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

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

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

# 10. Privacidad y Protección de los Datos

Microsystem S.A. protege 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 PSC.

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.

Los documentos que amparan la privacidad y derechos de los usuarios son: **ME-DG-PPAC Política de Privacidad** y **ME-DG-PPDU Política de Protección de los Derechos de los Usuarios**, respectivamente. Dichos documentos se encuentran disponibles en la página web https://portal.ca.msys.cl/, en la sección **Documentación de las Políticas y Prácticas de Certificación**.

# 11. Derechos de los titulares

**11.1.** El titular tiene derecho a ser informado, al menos con dos meses de anticipación, por el PSC, del cese de su actividad, con el fin de hacer valer su oposición al traspaso de los



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 4° del artículo 16 de la ley 19.799, o bien, para que tomen conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador.

**11.2.** El titular tiene derecho a ser informado inmediatamente de la cancelación de la inscripción en el registro de prestadores acreditados, con el fin de hacer valer su oposición al traspaso de los datos de sus certificados a otro certificador, en cuyo caso dichos certificados se extinguirán de conformidad con el numeral 3º del artículo 16 de la ley 19.799, o bien, para tomar conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador.

**11.3.** El titular tiene derecho a traspasar sus datos a otro prestador de servicios de certificación.

**11.4.** El titular tiene derecho a ser indemnizado y hacer valer los seguros comprometidos, en conformidad con el artículo 14 de la ley 19.799.

**11.5.** El titular tiene derecho a ser informado, antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago, en su caso; de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso (Limitaciones, Prohibiciones y uso no Autorizado), y de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o que se conviniere.

# 12. Declaración de las garantías y seguros

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

**12.2.** Microsystem S.A. gestionará todos los aspectos de la seguridad de la información, seguridad lógica y seguridad física, relacionados con la operación en función de la Autoridad Certificadora de acuerdo a lo requerido por la normativa vigente, según estipulado en **ME-DG-PO02 Declaración de Prácticas de Certificación**.

**12.3.** Microsystem S.A. mantendrá vigente el seguro de responsabilidad civil que exige la Ley de Firma Electrónica Avanzada y Documentos Electrónicos, Ley N° 19.799.

**12.4.** Microsystem respeta todos los derechos del usuario, sin perjuicio de aquellos que deriven de la ley Nº 19.628, sobre Protección de la Vida Privada y de la ley Nº 19.496, sobre Protección a los Derechos de los Consumidores y podrán, con la salvedad de lo señalado en el número 10° del artículo 23° de la Ley 19.799, ejercerlos conforme al procedimiento establecido en esta última normativa.

# 13. Políticas de Seguridad

Para proporcionar los servicios de certificación de manera segura y confiable el PSC Microsystem S.A. implementa la gestión de los siguientes aspectos de seguridad pertenecientes al Microsystem S.A. en su función como el PSC:



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

**13.1.** Activos Físicos y Lógicos
**13.2.** Recursos Humanos
**13.3.** Seguridad Física y del Entorno
**13.4.** Comunicaciones y Operaciones
**13.5.** Control del Acceso
**13.6.** Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
**13.7.** Incidentes de la Seguridad de la Información
**13.8.** Continuidad del Negocio

La gestión de lo anterior se realiza de acuerdo a los estándares ISO 27001, en concordancia con la normativa vigente, según estipulado con detalle en los siguientes puntos del documento **ME-DG-PO02 Declaración de Prácticas de Certificación**: **7.5 Gestión de Incidentes y Superación de Situaciones Críticas**, **8. Controles de Procedimiento**, **9. Controles de Personal del PSC**, **10. Controles de Seguridad Física** y **11. Controles de Seguridad Técnica.**

Para garantizar el correcto funcionamiento de las políticas descritas en el presente documento Microsystem S.A. realiza periódicamente auditorías internas y externas de acuerdo a lo establecido en el punto **4.4. Auditorías u Otras Evaluaciones como herramientas de control de cumplimiento** del documento **ME-DG-PO02 Declaración de Prácticas de Certificación**.

# 14. Fiabilidad del Mecanismo Complementario de Verificación de Identidad para Emisión de Firma Electrónica Avanzada en Línea

De acuerdo con el **Informe de Sistemas de Pago – Agosto 2025** del Banco Central de Chile, las Transferencias Electrónicas de Fondos (TEF) en Chile operan sobre infraestructuras reguladas, supervisadas y diseñadas bajo estándares internacionales de seguridad, resiliencia operativa y trazabilidad. Estas transferencias se cursan en una **red cerrada del sistema financiero**, donde la identificación del ordenante se encuentra asociada de manera directa y contractual a la cuenta bancaria de origen.

En particular, el campo **"RUT Emisor"** que acompaña a una transferencia bancaria corresponde a un **dato maestro provisto por la institución financiera de origen**, cuya validez es **del 100% respecto del vínculo contractual entre el banco y su cliente**, no siendo un dato autodeclarado ni editable por el usuario final. Esta característica otorga a la transferencia bancaria un alto nivel de certeza respecto de la identidad del titular de la cuenta emisora.

Adicionalmente, según la información publicada por la Comisión para el Mercado Financiero en la **Publicación Semestral de Fraudes Asociados a Transacciones Electrónicas** (Ley



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

N°21.234, NCG N°487), la **tasa de fraude por suplantación de identidad en la apertura de cuentas bancarias (identidad sintética)** se mantiene en niveles **inferiores al 0,05%**, lo que implica que más del **99,9% de las cuentas activas corresponden a identidades válidamente verificadas por las instituciones financieras**.

Considerando conjuntamente:

- la veracidad contractual del identificador del ordenante (RUT Emisor),
- la baja incidencia de fraude de identidad en el sistema bancario chileno,
- y la operación de las TEF sobre infraestructuras críticas supervisadas por el Banco Central,

es posible **inferir razonablemente una fiabilidad superior al 99,9% en la correspondencia entre el emisor de una transferencia bancaria y su identidad real**.

En este contexto, la transferencia bancaria constituye un **mecanismo complementario altamente robusto para la verificación fehaciente de identidad del solicitante de firma electrónica avanzada en modalidad remota**, aportando un nivel de certeza significativamente superior al de otros mecanismos no presenciales basados exclusivamente en autodeclaración, credenciales digitales simples o validaciones de una sola capa.

# 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-PO02 - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - MICROSYSTEM S.A.
**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



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

**16.5.** MINECON - Entidad Acreditadora - Acreditación de Autoridades Certificadoras - Guías de Acreditación
**16.6.** MINECON - Entidad Acreditadora - Entidades
**16.7.** MINECON - Entidad Acreditadora - Certificados Raíz
**16.8.** RFC 2510 - Internet X.509 Public Key Infrastructure Certificate Management Protocols
**16.9.** RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
**16.10.** RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
**16.11.** ISO 9001
**16.12.** ISO/IEC 27001
**16.13.** https://en.wikipedia.org/wiki/Private_Enterprise_Number
**16.14.** Registro de Números de Empresas Privadas https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers
**16.15.** Fuente de Fiabilidad Mecanismo Complementario 1: https://www.cmfchile.cl/portal/estadisticas/617/w3-propertyvalue-48099.html
**16.16.** Fuente de Fiabilidad Mecanismo Complementario 2: https://www.bcentral.cl/documents/33528/7510377/Informe+de+Sistemas+de+Pago+agosto+2025.pdf/43522521-1ab0-fdc7-00e7-6ba4589eaba2?t=1754400620514

# 17. Control de Cambios

| Versión | Fecha | Responsable | Modificaciones |
|---|---|---|---|
| 001 | 22/06/2021 | Jefe de Proyecto - CA | Primera versión del documento |
| 002 | 10/12/2021 | Gerente I+D | Actualización del documento en base a los requisitos de la AC |
| 003 | 10/01/2022 | Gerente I+D | Se reemplaza “Portal de Usuario” por "Portal de Suscriptor de Firma Digital". |
| 004 | 14/03/2022 | Gerente I+D | Se elimina la mención a la Clave única.<br>Se incorpora el Private Enterprise Number de Microsystem asignado por IANA. |
| 005 | 13/06/2022 | Gerente I+D | Corrección al contenido del punto 3.7 en cuanto al modelo de confianza. |



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

| | | | |
|---|---|---|---|
| 006 | 08/07/2022 | Gerente I+D | Se incorporan los derechos del suscriptor.<br>Se incorporan deberes del PSC en materia de publicidad y entrega de la información de contacto adecuada.<br>Se incorpora la información sobre identificador OID de este documento.<br>Se incorpora la información de contacto. |
| 007 | 22/08/2022 | Gerente I+D | Se incorporan puntos 1.3 Objetivo, 1.4 Alcance, 1.5 Roles y responsabilidades, 1.6 Administración de la política, 11. Política de Seguridad.<br>Se modifica el punto 10.3, en relación a la declaración de garantías y seguros, haciendo mención al documento ME-DG-PO02. |
| 008 | 11/10/2022 | Gerente I+D | Se actualiza el documento en base a las correcciones de la Entidad Acreditadora. |
| 009 | 27/10/2022 | Gerente I+D | Se actualiza el documento en base a las correcciones de la Entidad Acreditadora. |
| 010 | 20/01/2023 | Gerente I+D | Ajuste de contenido para acomodar la jerarquía productiva P1. |
| 011 | 03/08/2023 | Gerente MicroeDoc | Se incorpora procedimiento de Registro Presencial en Terreno en Domicilio del Solicitante. |
| 012 | 13/11/2023 | Gerente MicroeDoc | Corrección de observaciones indicadas por Entidad Acreditadora asociadas al procedimiento de Registro Presencial en Terreno en Domicilio del Solicitante. |
| 013 | 06/03/2024 | Gerente MicroeDoc | Corrección de observaciones indicadas por Entidad Acreditadora asociadas al procedimiento de Registro Presencial en Terreno en Domicilio del Solicitante. |
| 014 | 29/04/2024 | Gerente MicroeDoc | Corrección de observaciones indicadas por Entidad Acreditadora asociadas al procedimiento de Registro Presencial en Terreno en Domicilio del Solicitante. |



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.

Público

| | | | |
|---|---|---|---|
| 015 | 21/08/2024 | Gerente MicroeDoc | Se incorpora procedimiento de Registro en Línea a través de Sistema ClaveÚnica conforme al Decreto 24 del Ministerio De Economía, Fomento Y Turismo; Subsecretaría De Economía Y Empresas De Menor Tamaño. |
| 016 | 13/11/2024 | Gerente MicroeDoc | Se realizan las siguientes modificaciones:<br>• Se modifica plazo de reembolso para solicitudes canceladas por el usuario, en los puntos 4.1.3.5.3.1.1. y 4.1.3.5.1.2.1.1.<br>• Se agrega punto 4.1.3.4.3.4 Fecha de nacimiento, en los datos solicitados en el formulario de solicitud. |
| 017 | 22/01/2026 | Gerente MicroeDoc | Se realizan las siguientes modificaciones:<br>• Se incluye Punto 14 Fiabilidad del Mecanismo Complementario de Verificación de Identidad para Emisión de Firma Electrónica Avanzada en Línea<br>• Referencias utilizadas en el Punto 14 se incluyen en el apartado 16 Documentos de referencia |
| 018 | 26/05/2026 | Gerente MicroeDoc | Se modifica 4.1.1. Registro Presencial en las Oficinas del PSC quitando del formulario de solicitud los campos Empresa y Cargo. |
| 019 | 12/08/2026 | Gerente MicroeDoc | Se realizan las siguientes modificaciones:<br>• Cambio de Logo Microsystem<br>• Cambio en vigencia de certificados agregando certificado de 30 y 7 días de vigencia.<br>• Cambio en proceso 4.1.3 Registro en Línea a través del Sistema ClaveÚnica, en punto relativo a activación del certificado. |

Public



**NOTA:** Las copias impresas de este documento pasan a constituir **COPIAS NO CONTROLADAS**, a menos que cuenten con el timbre **CONTROLADO** del departamento Quality Management (Q.M.Dept) de Microsystem en original.