POLÍTICA DE IDENTIFICACIÓN ELECTRÓNICA

DOC-ICPP-09

Versión 1.0

CONTROL DOCUMENTAL

Documento	
Título: POLÍTICA DE IDENTIFICACIÓN ELECTRÓNICA	**Nombre Archivo:** DOC-ICPP-09 Vers 1.0
Código: DOC-ICPP-09	**Soporte Lógico:** https://www.acraiz.gov.py/
Fecha: 24/06/2024	**Versión:** 1.0

Registro de cambios		
Versión	**Fecha**	**Motivo de cambio**
1.0	24/06/2024	Versión inicial

Distribución del documento	
Nombre	**Área**
Ministerio de Industria y Comercio (MIC)	Dirección General de Comercio Electrónico (DGCE)
PSC	Prestadores de Servicios de Confianza
PCSC	Prestadores Cualificados de Servicios de Confianza
Documento Público	https://www.acraiz.gov.py/

Control del documento	
Elaborado por: JENNY RUÍZ DÍAZ	Firmado electrónicamente por: JENNY ELIZABETH RUIZ DIAZ LEZCANO Cédula de Identidad: 1227372 Certificado emitido por CODE100 S.A. Date: 16/7/2024 14:17:56 -04:00
Verificado por: LUJÁN OJEDA	MARIA LUJAN OJEDA CHAMORRO Firmado digitalmente por MARIA LUJAN OJEDA CHAMORRO
Aprobado por: LUCAS SOTOMAYOR	LUCAS ATILIO SOTOMAYOR LLANO Firmado digitalmente por LUCAS ATILIO SOTOMAYOR LLANO

Contenido

1. INTRODUCCIÓN

La identificación electrónica (IDe) es el proceso mediante el cual se utilizan datos de identificación de una persona en formato electrónico, que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica, conforme a lo dispuesto en el art. 4° de la Ley N° 6822/2021.

La expedición de medios de IDe (m-IDe) es un servicio de confianza que permite identificar y autenticar personas físicas y jurídicas cuya comprobación de identidad se encuentre basada en un sistema de IDe.

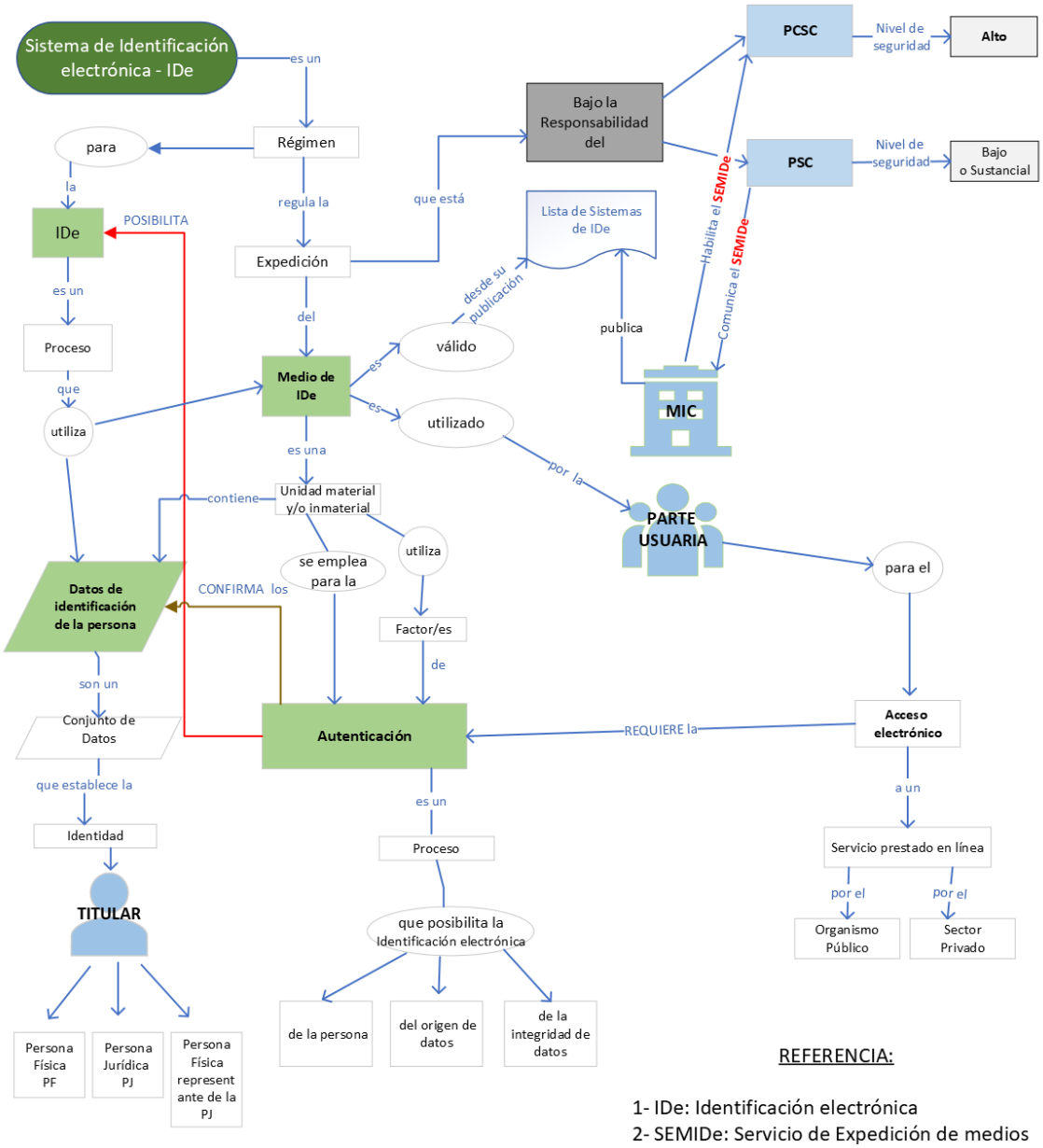
Los sistemas de IDe cuentan con diversos niveles de seguridad y deberán ser provistos por un Prestador de Servicios de Confianza (PSC). Un sistema de IDe debe especificar los niveles de seguridad bajo, sustancial y alto para los m-IDe expedidos en virtud del mismo.

La referida Ley igualmente establece la equivalencia entre la identificación presencial y aquella realizada por medios electrónicos seguros permitiendo así la identificación fehaciente de la persona. Dicha equivalencia es exclusiva del sistema de IDe con nivel de seguridad alto, conforme los criterios establecidos por la Autoridad de Aplicación (AA), basado en un m-IDe expedido por un Prestador Cualificado de Servicios de Confianza (PCSC).

Los niveles de seguridad de los sistemas de IDe deberán ajustarse a las etapas de inscripción, gestión de medios de IDe, autenticación, gestión y organización definidas en el presente documento, así como al protocolo de federación definido.

Esta Política establece las especificaciones, normas y procedimientos técnicos mínimos relacionados con los niveles de seguridad aplicables a la expedición de los m-IDe, en el marco de un sistema de IDe, en concordancia con las disposiciones de la Ley N° 6822/21, cuyo cumplimiento es de carácter obligatorio.

El siguiente esquema representa el Servicio de expedición de m-IDe en virtud de un sistema de IDe:



La presente política fue elaborada siguiendo el marco normativo vigente, las guías y recomendaciones para proteger la identidad digital del NIST en su publicación SP 800-63 y el reglamento de ejecución UE 2015/1502 relativo a IDe.

1.1. CONSIDERACIONES GENERALES

En todos los casos el periodo de vigencia del m-IDe no será superior a cuatro (4) años.

El m-IDe en el nivel de seguridad alto estará contenido un Módulo Criptográfico (Software o Hardware) que contiene los datos de IDe deberá estar asociado obligatoriamente a un Certificado Cualificado expedido por un PCSC y conforme al ítem 4 del DOC-ICPP-06 e ítem 6 del DOC-ICPP-03. En este sentido, todos los certificados emitidos en el ámbito de la ICPP, siempre y cuando se encuentren vigentes y el PCSC tenga habilitado el servicio de expedición de medios de identificación electrónica serán considerados como m-IDe de nivel de seguridad alto.

Los PSC o PCSC podrán percibir una prestación económica por el servicio de expedición de m-IDe. Asimismo, el Centro de Intercambio de Información (CII) podrá establecer tarifas correspondientes por el servicio ofrecido, el cual no se aplicará para los Organismos y Entidades del Estado.

En todos los casos los PCSC deben dar cumplimiento a los documentos aplicables que rigen a la Infraestructura de Clave Pública del Paraguay (ICPP). En la presente política se señalan de manera referencial algunos de estos documentos en diferentes puntos, sin embargo, son de cumplimiento obligatorio.

1.2. DEFINICIONES

Las siguientes definiciones se encuentran relacionadas al servicio de IDe previsto en la Ley N° 6822/2021 y son utilizadas a lo largo del presente documento, y, por lo tanto, son citadas también aquí.

1. **Agente de registro:** persona responsable de la realización de las actividades inherentes a la AR. Realiza la identificación de los solicitantes en la solicitud de expedición/revocación de medios de identificación.
2. **Autoridad de Registro**: entidad responsable de tramitar las distintas solicitudes inherentes a medios de identificación, identificar al solicitante y remitir las solicitudes al PSC o PCSC. La AR puede ser propia o delegada a un tercero.
3. **Autenticación electrónica**: un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica.
4. **Biometría:** tecnología para la verificación y autenticación de identidad que ofrece precisión y seguridad a servicios que buscan mayores niveles de seguridad.
5. **Certificado cualificado de firma electrónica:** un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el artículo 43 de la presente ley.
6. **Certificado cualificado de sello electrónico:** un certificado de sello electrónico que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el artículo 53 de la presente ley.

7. **Certificado de firma electrónica:** una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona.
8. **Certificado de sello electrónico:** una declaración electrónica que vincula los datos de validación de un sello con una persona jurídica y confirma el nombre de la misma.
9. **Contraseña**: autenticador secreto memorizado por el usuario.
10. **Contrato de prestación de servicios:** Contrato suscrito entre el PSC o el PCSC, según corresponda el nivel de seguridad del sistema de identificación, y el titular del medio de identificación, en el cual se establecen los derechos, obligaciones y responsabilidades de las partes con respecto a la prestación del servicio de expedición de medios de identificación en virtud de un sistema de identificación electrónica. Este contrato requiere la aceptación explícita de las partes intervinientes.
11. **Datos de identificación de la persona**: un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica.
12. **Dispositivo cualificado de creación de firma electrónica:** un dispositivo de creación de firmas electrónicas que cumple los requisitos establecidos en el artículo 44 de la presente ley.
13. **Dispositivo cualificado de creación de sello electrónico:** un dispositivo de creación de sellos electrónicos que cumple con los requisitos establecidos en el artículo 54 de la presente ley.
14. **Dispositivo de creación de firma electrónica:** un equipo o programa informático configurado que se utiliza para crear una firma electrónica.
15. **Dispositivo de creación de sello electrónico:** un equipo o programa informático configurado que se utiliza para crear un sello electrónico.
16. **Factor de autenticación**: un factor confirmado como vinculado a una persona (algo que sabe, algo que tiene y algo que es), que se encuentra en alguna de las categorías siguientes:
    a. **Factor de autenticación basado en la posesión**: factor de autenticación en el que el sujeto está obligado a demostrar posesión del mismo;
    b. **Factor de autenticación basado en el conocimiento**: factor de autenticación en el que el sujeto está obligado a demostrar conocimiento del mismo;
    c. **Factor de autenticación inherente**: factor de autenticación que se basa en un atributo físico de una persona física del cual el sujeto está obligado a demostrar su posesión;
17. **Fuente auténtica**: cualquier fuente, independientemente de la forma, en la que se pueda confiar para proporcionar datos, información o pruebas exactos que se puedan utilizar para demostrar la identidad;

18. **Identificación electrónica**: proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.
19. **Medios de identificación electrónica**: una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.
20. **Módulo criptográfico**: software o hardware criptográfico que genera y almacena claves criptográficas
21. **Nivel de Seguridad:** categoría que transmite el grado de confianza de que la identidad reclamada por el solicitante es su identidad real.
22. **Nombre de usuario**: Nombre elegido por la persona o generado por el PSC o PCSC.
23. **One Time Password (OTP)**: Contraseña de un solo uso
24. **Parte usuaria:** la persona física o jurídica que confía en el servicio de confianza.
25. **PIN:** valor numérico secreto que el usuario debe elegir y memorizar.
26. **Prestador cualificado de servicios de confianza**: un prestador de servicios de confianza que presta uno o varios servicios de confianza cualificados y al que el organismo de supervisión ha concedido la habilitación.
27. **Prestador de servicios de confianza:** una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.
28. **Prueba de identidad**: evidencia que permite establecer que una persona es en realidad quien dice ser con un nivel de certeza determinado.
29. **Servicio de confianza:** el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios, d) servicio de expedición de medios de identificación en virtud a sistemas de identificación electrónica.
30. **Servicio de confianza cualificado:** el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en: a) la creación, verificación y validación de firmas electrónicas cualificadas, sellos electrónicos cualificados, sellos cualificados de tiempo electrónicos, servicios cualificados de entrega electrónica certificada y certificados relativos a estos servicios, y/o b) la creación, verificación y validación de certificados cualificados para la autenticación de sitios web, y/o c) la preservación de firmas, sellos o certificados cualificados electrónicos relativos a estos servicios, d) servicio de expedición de medios de identificación en virtud a sistemas de identificación electrónica con nivel de seguridad alto.
31. **Sistema de identificación electrónica**: un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las

personas físicas o jurídicas o a una persona física que representa a una persona jurídica.

32. **Sistema de gestión de la seguridad de la información**: conjunto de procesos y procedimientos diseñados para gestionar a niveles aceptables los riesgos relacionados con la seguridad de la información.
33. **Solicitante:** Persona solicitante de un medio de identificación.
34. **Responsable autorizado:** Persona física autorizada expresamente para representar a la persona jurídica solicitante.

1.3. SIGLAS Y ACRÓNIMOS

Tabla Nº 1 - Siglas y Acrónimos

Sigla/Acrónimo	Descripción
AA	Autoridad de Aplicación
AGR	Agente de Registro
AR	Autoridad de Registro
CII	Centro de Intercambio de Información
DGCE	Dirección General de Comercio Electrónico
FA	Factor de autenticación
IDe	Identificación electrónica
m-IDe	Medio de Identificación electrónica
MIC	Ministerio de Industria y Comercio
MITIC	Ministerio de Tecnologías de la Información y Comunicación
OEC	Organismo de Evaluación de la Conformidad
OTP	Autenticación con contraseña de un solo uso por sus siglas en inglés one time password
PIE	Política de Identificación Electrónica
PSC	Prestador de Servicios de Confianza
PCSC	Prestador Cualificado de Servicios de Confianza
PSS	Prestador de Servicios de Soporte
PU	Parte Usuaria
URL	Localizador de Recursos Uniforme, por sus siglas en inglés Uniform Resource Locator

2. NOMBRE E IDENTIFICACIÓN DEL DOCUMENTO

En este ítem debe ser identificada la Política de Identificación Electrónica (PIE), indicando como mínimo el nombre, versión, fecha de aprobación, localización y el OID (Object Identifier) del documento.

2.1. Administración de la Política de Identificación

En este ítem el PSC o PCSC debe incluir:

- Datos mínimos como: el nombre, la dirección física, dirección de correo electrónico oficial, números de teléfono, página web y otra información del PSC o PCSC responsable de la PIE.
- Datos de una persona de contacto: el nombre, números de teléfono y la dirección de correo electrónico.

2.2. Procedimiento de Aprobación de la Política

Los procedimientos para la aprobación de la PIE del PCSC son establecidos a criterio de la AA.

2.3. Uso apropiado

Los usos habilitados y restricciones para la utilización del m-IDe que contiene los datos de IDe, deben ser comprendidos a partir de lo dispuesto en la presente política y por las condiciones de uso establecidas por cada PSC o PCSC según corresponda.

De conformidad al Artículo 29, inciso 2, de la Ley 6822/21, cuando la ley requiera o permita que se identifique a una persona, ese requisito se dará por cumplido respecto al sistema de IDe si se utiliza un nivel de seguridad alto, expedido por un prestador cualificado de servicios de confianza.

Los usos de los m-IDe que contienen los datos de IDe en el sector privado serán utilizados según el análisis de riesgo de cada entidad; respecto a la administración pública deberán ajustarse a los lineamientos determinados por el Ministerio de Tecnologías de la Información y Comunicación (MITIC).

3. ACTORES

3.1. Autoridad de Aplicación

El Ministerio de Industria y Comercio (MIC) es AA de la Ley N° 6822/2021 "DE LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS TRANSMISIBLES ELECTRÓNICOS" y en ese sentido tiene la atribución de dictar las resoluciones que fueren necesarias en consonancia con la Ley, y su Decreto reglamentario para el adecuado funcionamiento y la eficiente prestación de los Servicios de Confianza para la expedición de m-IDe que contienen los datos de IDe en virtud de un sistema de IDe; y en ese carácter también es el órgano encargado de habilitar a los PCSC cuyos sistemas de IDe se basen en un nivel de seguridad alto.

Además ejerce todas las prerrogativas de control y supervisión necesarias para la implementación de la normativa vigente al respecto.

3.2. Prestadores de Servicios de Confianza

Es una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza. Esta política rige para la prestación del servicio de expedición de medios de identificación en virtud de sistemas de identificación electrónica y emisión de aserciones derivadas de datos de identificación contenidos en dichos medios. A continuación se describen los tipos de Prestadores según el nivel de seguridad exigido:

NIVEL DE SEGURIDAD	TIPO DE PRESTADOR	REQUERIMIENTO ANTE LA AA
Expide m-IDe en virtud a sistemas de IDe con nivel de seguridad **BAJO**	PSC	Comunicar la prestación del servicio
Expide m-IDe en virtud a sistemas de IDe con nivel de seguridad **SUSTANCIAL**		
Expide m-IDe en virtud a sistemas de IDe con nivel de seguridad **ALTO**	PCSC	Solicitar habilitación para prestar el servicio

3.2.1. Autoridad de registro

La Autoridad de Registro (AR) es la entidad vinculada a un PSC o PCSC responsable de tramitar las distintas solicitudes de expedición de m-IDe. Esta tarea es realizada a través de un Agente de Registro (AGR), quien tiene a cargo la responsabilidad de realizar el proceso de Inscripción, descrito en el punto **6.1.1**

TIPO DE PRESTADOR	DESCRIPCIÓN
PSC	La AR no requiere de comunicación ni habilitación a la AA.
PCSC	Cada AR requiere habilitación por parte de la AA, para el efecto, en este ítem debe identificar la dirección de la página web (URL) y datos permanentemente actualizados referentes a las AR*

*La AR puede ser propia del PCSC, o puede ser delegada a un tercero, en el caso de AR vinculada a un PCSC, su funcionamiento deberá ser autorizado por la AC Raíz-Py con la habilitación correspondiente. Las AR delegadas son autoridades de registro vinculadas a un PCSC mediante un acuerdo operacional, conforme lo dispuesto en el ítem 8 del DOC-ICPP-05 [2].

El PCSC deberá igualmente publicar información referente a:

- Lista de todas las AR habilitadas
- Lista de las AR que se han inhabilitado por el PCSC, indicando la fecha de la inhabilitación.

3.3. Titular del medio de identificación electrónica

En este ítem se especifican las personas físicas o jurídicas que podrán ser titulares del m-IDe que contienen los datos de IDe emitidos por el PSC o PCSC según corresponda.

3.4. Parte usuaria

Cualquier proveedor de servicios (PS) distinto a los servicios de confianza, sea persona física o jurídica; que confía en el servicio de expedición de m-IDe será considerada parte usuaria. La PU verifica, mediante una integración técnica, el nivel de seguridad y los datos del titular del m-IDe y lo utiliza para otorgar los accesos a sus servicios. Es su responsabilidad requerir el nivel de seguridad adecuado para la IDe de las personas, en la prestación de sus servicios, conforme a lo dispuesto en el ítem 6.

3.5 Centro de Intercambio de Información (CII)

El MITIC podrá actuar como intermediario, constituyéndose en un Centro de Intercambio de Información (CII) entre el PSC o PCSC y la parte usuaria, en dicha función se encargará de dirigir la consulta actuando de certificador, mediante una integración técnica y de confianza entre ambos sistemas.

3.6 Otros participantes

3.6.1. Prestadores de Servicios de Soporte (PSS)

En este ítem se identifica la dirección de página web (URL), donde deberán estar publicados los datos referentes a los PSS vinculados al PSC o PCSC, sea directamente o sea por intermedio de sus AR.

Los PSS son entidades externas a las que recurren los PSC o PCSC o la AR para desempeñar actividades descritas en esta PC y se clasifican en tres categorías, conforme al tipo de actividades prestadas:

a) disponibilización de infraestructura física y lógica;
b) disponibilización de recursos humanos especializados; y
c) disponibilización de infraestructura física y lógica y de recursos humanos especializados.

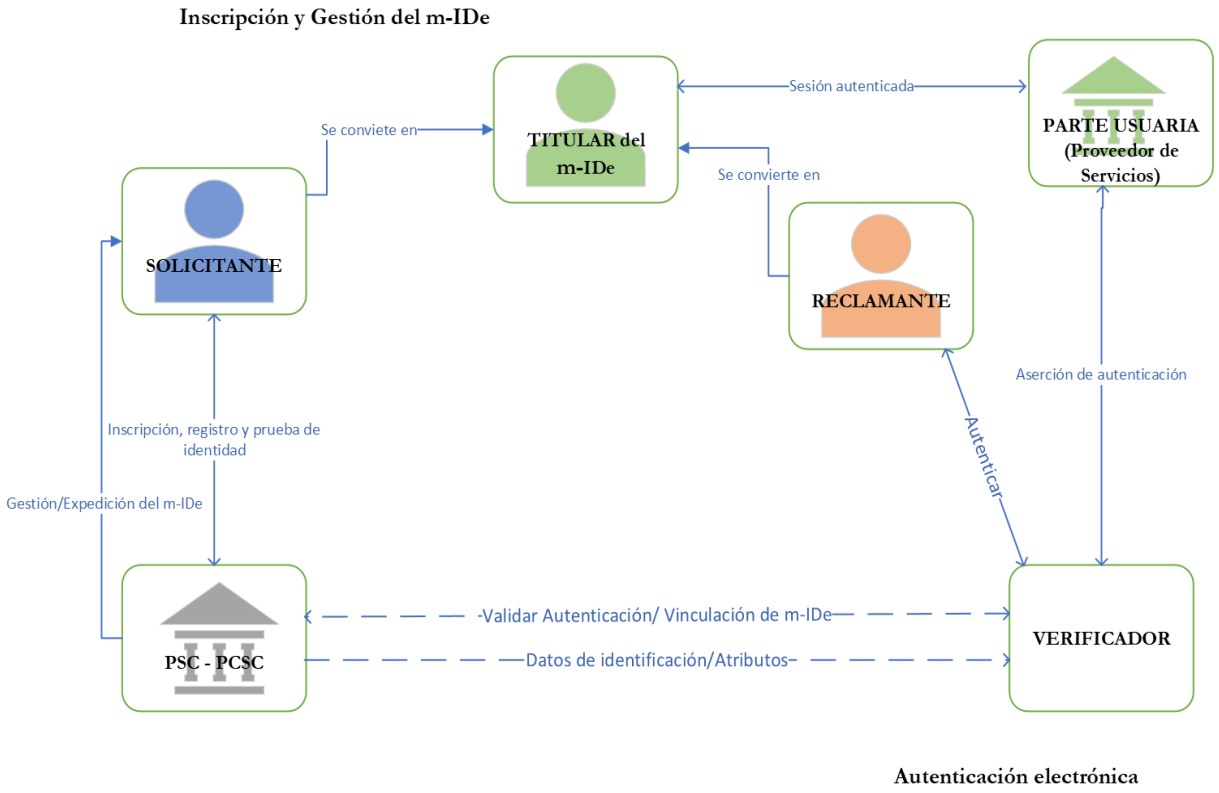
El PSC o PCSC deberá mantener las informaciones arriba citadas siempre actualizadas. El funcionamiento de un PSS vinculado a un PCSC mediante un acuerdo operacional, deberá ser autorizado por la AC Raíz-Py.

El PSC o PCSC deberá publicar información referente a:

- Lista de todos los PSS habilitados
- Lista de los PSS que se han inhabilitado por el PSC o PCSC, indicando la fecha de la inhabilitación.

4. RÉGIMEN PARA LA IDENTIFICACIÓN ELECTRÓNICA

MODELO DE IDENTIDAD ELECTRÓNICA



Del lado izquierdo del diagrama se muestra el proceso de inscripción y gestión del m-IDe. La secuencia habitual de interacciones es la siguiente:

1. Una persona, ya sea física o jurídica, puede solicitar un m-IDe basado en un Sistema de IDe de un PSC si busca un nivel bajo o sustancial de seguridad, o en un Sistema de IDe de un PCSC si requiere un nivel alto de seguridad. Para ello se somete a un proceso de inscripción, registro, prueba y verificación de identidad.
2. El PSC o PCSC valida y verifica los documentos presentados y las pruebas de identidad y en caso exitoso, vincula, expide y gestiona un m-IDe que contiene los datos de identificación de la persona solicitante y que se utilizará para la autenticación de servicios en línea. El solicitante pasa a ser titular de un m-IDe.
3. Se configura el mecanismo de autenticación requerido según el nivel de seguridad.

En el lado derecho del diagrama, se muestra el proceso mediante el cual un titular utiliza un m-IDe para autenticarse en un servicio en línea proporcionado por la Parte Usuaria (PU). El titular de un m-IDe se convierte en un reclamante cuando necesita autenticarse ante un verificador. Las interacciones son las siguientes:

4. El Titular de un m-IDe, en calidad de reclamante, demuestra la posesión y el control del m-IDe al PSC o PCSC, que actúa como verificador, a través de un protocolo de

autenticación. El PSC o PCSC valida los datos de identificación que vinculan la identidad del titular con su m-IDe. Opcionalmente, puede obtener atributos del reclamante.

5. El PSC o PCSC, en su función de verificador, proporciona una aserción sobre el titular del m-IDe como suscriptor del servicio de la PU. Esta aserción puede ser utilizada por la PU para tomar una decisión de autorización.
6. Por último, se establece una sesión autenticada entre el Titular del m-IDe y la PU.

El modelo de IDe descrito en este apartado representa las tecnologías y arquitecturas actualmente disponibles en el mercado. Sin embargo, también existen modelos más complejos que dividen las funciones entre un mayor número de partes y pueden ofrecer ventajas en ciertos tipos de aplicaciones. Aunque en este documento se haya utilizado el modelo más simple, esto no impide que el PSC o PCSC separen estas funciones. Además, en algunos casos, ciertos procesos de inscripción, prueba de identidad y expedición de m-IDe pueden ser delegados a una Autoridad de Registro (AR).

El PSC o PCSC debe describir en su PIE, el modelo de identificación adoptado, teniendo en cuenta los procedimientos de seguridad detallados en el ítem 6 del presente documento.

4.1 MODALIDADES DE INSCRIPCIÓN

El Proceso de Inscripción del Solicitante de un m-IDe, descrito en el punto 6.1.1 será realizado por el PSC o, el PCSC a través de un AGR en los siguientes términos:

a) en presencia de la persona física solicitante o de la persona física que representa a una persona jurídica; o,

b) de forma remota. La seguridad de que este proceso sea equivalente al presencial será confirmado por un OEC.

En caso de renovación del m-IDe, se aplicarán las mismas condiciones referidas en los puntos a), o b) o:

c) a distancia, utilizando un m-IDe expedido en virtud de un sistema de IDe de nivel de seguridad equivalente al solicitado, para los cuales se haya garantizado la presencia de la persona física previamente a la expedición del m-IDe; o

d) por medio de un certificado de firma electrónica cualificada para persona física o un certificado de sello electrónico cualificado para persona jurídica, expedidos de conformidad con la letra a) o c).

5. DATOS DE IDENTIFICACIÓN Y PRUEBAS DE IDENTIDAD REQUERIDOS

En este ítem se detallan los datos de identificación y pruebas de identidad que representan la identidad reclamada, reconocidas por la AA según el nivel de seguridad que corresponda y el tipo de titular del m-IDe.

La comprobación de los datos de identificación y pruebas de identidad requeridos podrá realizarse presencialmente o de forma remota, siempre que se realice a través de fuentes oficiales de organismos competentes. Estas validaciones deberán incluirse obligatoriamente en el dossier del titular de la identidad electrónica conforme al DOC-ICPP-03 [01] en el caso del PCSC, igualmente el PSC deberá conformar dossier de los titulares.

Los datos de identificación y pruebas de identidad, que no puedan comprobarse conforme a las condiciones del párrafo anterior deberán verificarse:

a) por un AGR que no sea el que realizó el paso de identificación;
b) por la AR delegada o AR propia del PSC/PCSC; y

c) antes de la expedición del m-IDe, debiendo ser revocado inmediatamente en el caso que la verificación no se haya realizado antes del inicio de su validez.

5.1. PERSONA FÍSICA	
Nivel de Seguridad	**Requerimiento**
5.1.1 BAJO	En el nivel de seguridad bajo se requieren datos de identificación proporcionados por el solicitante tales como: ● Nombres y apellidos ● Número de documento de identidad ● Fecha de nacimiento ● Dirección de correo electrónico ● Número de teléfono/celular Esta lista no es taxativa y podrá el PSC solicitar otros datos de identificación al solicitante.
5.1.2 SUSTANCIAL	En el nivel de seguridad sustancial se requiere además de los datos de identificación proporcionados por el solicitante en el nivel bajo, la presentación de pruebas de identidad tales como: ● Cédula de identidad, o ● Pasaporte En todos los casos los documentos referidos deberán estar vigentes y los datos deben ser plenamente legibles. El PSC podrá solicitar otros datos adicionales a los citados precedentemente, los cuales deberán estar anexos al dossier correspondiente.
5.1.3 ALTO	Para el nivel de seguridad alto se requiere además de los datos de identificación proporcionados por el solicitante en el nivel bajo, la presentación de pruebas de identidad establecidas en el ítem 3.2 del DOC-ICPP-03 [1] así como deberá proporcionar uno de los siguientes datos de identificación biométricas como: ● Huellas dactilares ● Huellas de voz ● Escaneo del iris ● Reconocimiento facial

5.2. PERSONA JURÍDICA	
Nivel de Seguridad	**Requerimiento**
5.2.1 BAJO	En el nivel de seguridad bajo se requieren los datos del responsable autorizado conforme al ítem 5.1.1 así como de la persona jurídica tales como: ● Nombre o razón social ● Número de cédula tributaria o RUC ● Dirección de correo electrónico ● Nombre y apellido del representante legal ● Número de documento de identidad del representante legal ● Nombre y apellido del responsable autorizado ● Número de documento de identidad del responsable autorizado ● Documento que acredite la designación del responsable autorizado conforme a los estatutos o normas correspondientes a su funcionamiento que se encuentren vigentes al momento de la solicitud del m-IDe.
5.2.2 SUSTANCIAL	En el nivel de seguridad sustancial se requiere de la **presentación de documentos** relativos al responsable autorizado conforme al ítem 5.1.2, los señalados en el ítem 5.2.1 además de los siguientes: ● Estatuto o instrumento de creación ● Cédula tributaria o RUC ● Cédula de identidad del representante legal ● Cédula de identidad del responsable autorizado ● Documento que acredite la representación conforme a los estatutos o normas correspondientes a su funcionamiento que se encuentren vigentes al momento de la solicitud del m-IDe.
5.2.3 ALTO	En el nivel de seguridad alto se requiere el cumplimiento del ítem 5.1.3 relativos al responsable autorizado y a la **presentación de documentos** señalados en el ítem 5.2.2.

6. NIVELES DE SEGURIDAD

El PSC o PCSC debe definir en su PIE las especificaciones y procedimientos técnicos según sea el nivel de seguridad que aplica.

La garantía de la identidad de un titular se describe utilizando uno de tres niveles de seguridad. Los sistemas de IDe pueden contar con diversos niveles de seguridad y deberán ser provistos por un PSC o PCSC:

Nivel de Seguridad	Descripción
BAJO	Se refiere a un m-IDe, que establece un grado **limitado** de confianza en la identidad pretendida o declarada de una persona, considerando que en este nivel no es necesario vincular al solicitante con una identidad específica de la vida real. Las pruebas de identidad del solicitante no se validan ni se verifican y requiere un solo FA.
SUSTANCIAL	Se refiere a un m-IDe, que establece un grado **medio** de confianza en la identidad pretendida o declarada de una persona, atendiendo a que en este nivel la prueba de identidad respalda la existencia en el mundo real de la identidad reclamada y que el PSC valida y verifica que el solicitante está asociado adecuadamente con esta identidad en el mundo real. Deben realizarse pruebas de identidad físicamente presentes o remotas, se debe confirmar el sistema de información utilizado como dirección, aplicar controles técnicos y de seguridad. Además se requiere de dos FA.
ALTO	Se refiere a un m-IDe, que establece un grado **superior de confianza** al nivel sustancial en la identidad pretendida o declarada de una persona, considerando además de lo requerido en el nivel sustancial que en este nivel se requieran pruebas de identidad físicamente presentes o remotas conforme al documento DOC-ICPP-17 [3] por un AGR y colección de biometría para comprobar la identidad del solicitante. Las pruebas de identidad deben ser validadas y verificadas por el PCSC.

Las especificaciones técnicas y de seguridad mínimas, normas y procedimientos se establecerán en referencia a la fiabilidad y la calidad de los siguientes elementos:

- El procedimiento para demostrar y comprobar la identidad de las personas físicas o jurídicas que solicitan la expedición de los m-IDe.
- El procedimiento para expedir los m-IDe solicitados.
- El mecanismo de autenticación mediante el cual la persona física o jurídica utiliza los m-IDe para confirmar su identidad a una PU.
- El tipo de PSC que expide los m-IDe.
- Cualquier otro organismo que intervenga en la solicitud de expedición de los m-IDe.
- Las especificaciones técnicas y de seguridad de los m-IDe.
- El protocolo de federación.

En los siguientes apartados se describen las especificaciones técnicas, las normas y los procedimientos, entre otros los controles técnicos, que tendrán como objetivo evitar el uso indebido o alteración de la identidad:

6.1 ESPECIFICACIONES Y PROCEDIMIENTOS TÉCNICOS

6.1.1 Inscripción

Este ítem describe el patrón común en el que un solicitante de un m-IDe se somete a un proceso de inscripción y prueba de identidad, en el cual se recopilan sus pruebas de identidad y datos de identificación, se vinculan de manera única a una sola identidad dentro de una población o contexto específico, y luego se validan y verifican, conforme al nivel de seguridad.

El único objetivo de la prueba de identidad es garantizar que el solicitante sea quien dice ser con un nivel establecido de certeza. Esto incluye la presentación, validación y verificación de los atributos mínimos necesarios para lograr la prueba de identidad.

Cuando se prueba la identidad de un titular, los resultados esperados son:

- Vincular la identidad reclamada a una identidad única dentro del contexto de la población de usuarios a los que presta servicios el PSC o PCSC.
- Validar que toda prueba de identidad proporcionada sea correcta y genuina (por ejemplo, no falsificada).
- Validar que la identidad reclamada exista en el mundo real.
- Verificar que la identidad reclamada esté asociada con la persona real que proporciona la prueba de identidad.

6.1.1.1. Solicitud y registro

Nivel de Seguridad	Elementos necesarios
BAJO, SUSTANCIAL Y ALTO	1. El solicitante debe conocer y aceptar expresamente el contrato de prestación de servicios de confianza el cual contiene los términos de uso de los m-IDe, incluidas las recomendaciones de seguridad de éstos. 2. Recopilar los datos de identificación pertinentes.

6.1.1.2. Prueba, validación y verificación de la identidad (persona física)

Nivel de Seguridad	Elementos necesarios
BAJO	Los PSC deberán cumplir obligatoriamente los siguientes requisitos, precedente a la expedición de un m-IDe: ● **PRESENCIA:** sin requisitos. ● **DATOS:** sin requisitos. ● **PRUEBA:** ○ El solicitante de un m-IDe declara estar en posesión de pruebas de identidad reconocidas conforme al ítem 5.1.1. ○ Se supone que las pruebas de identidad son auténticas **o** pueden verificarse con una fuente auténtica y las pruebas parecen ser válidas. ● **VALIDACIÓN:** No se realiza validación ● **VERIFICACIÓN:** No se realiza verificación ● **CONFIRMACIÓN DE DIRECCIÓN:** sin requisitos. ● **COLECCIÓN BIOMÉTRICA:** No se realiza colección biométrica ● **CONTROLES DE SEGURIDAD:** no aplica
SUSTANCIAL	Se debe cumplir obligatoriamente una de las alternativas indicadas en los puntos 1 a 3: 1. Los PSC deberán cumplir obligatoriamente los siguientes requisitos, precedente a la expedición de un m-IDe: ● **PRESENCIA:** se requiere prueba de identidad remota o en persona. ● **DATOS:** se requiere de datos de identificación mínimos necesarios para lograr la vinculación de la identidad. Se puede utilizar verificación basada en conocimientos para mayor confianza. ● **PRUEBA:** se debe asegurar que el solicitante de un m-IDe está en posesión de pruebas de identidad reconocidas conforme al ítem 5.1.2. ● **VALIDACIÓN:** Se debe: ○ Comprobar que las pruebas de identidad son auténticas, utilizando mecanismos apropiados para confirmar la integridad de los elementos de seguridad física o seguridad criptográfica y que las mismas no son fraudulentas ni modificadas inapropiadamente, o ○ Confirmar que todos los datos de identificación y las pruebas de identidad son válidas en comparación con la información mantenida o publicada por una fuente auténtica. ● **VERIFICACIÓN:** se debe confirmar la propiedad del solicitante de un m-IDe sobre la identidad reclamada mediante comparación física, utilizando tecnologías apropiadas, con una fotografía y con la prueba de identidad más sólida proporcionada para respaldar la identidad reclamada. La comparación física realizada de forma remota debe cumplir con todos los requisitos especificados en el NIST SP 800-63B, Sección 5.2.3.

	● **CONFIRMACIÓN DE DIRECCIÓN:** Se debe requerir al solicitante de un m-IDe que proporcione una dirección física o electrónica durante el proceso de solicitud y registro. El sistema utilizado debe enviar una notificación de verificación a esa dirección, con un código de inscripción o un enlace de confirmación. El solicitante debe recibir el mensaje y usar el código o enlace proporcionado para confirmar que la dirección es válida y le pertenece realmente a efectos de garantizar que se esté comunicando con la persona correcta. En caso de verificación remota, se debe asegurar de que el código de inscripción y la notificación de verificación se envíen a direcciones de registro diferentes. ● **COLECCIÓN BIOMÉTRICA:** opcional ● **CONTROLES DE SEGURIDAD:** se debe tomar medidas para reducir al mínimo el riesgo de que la identidad de la persona no sea la identidad reclamada, teniendo en cuenta por ejemplo, el riesgo de pruebas perdidas, robadas, suspendidas, revocadas o expiradas. Se deberá garantizar que se cumplan los controles mínimos relacionados con la garantía para sistemas de impacto moderado o equivalente. **2.** Cuando los procedimientos utilizados anteriormente por un PSC para una finalidad distinta de la expedición de m-IDe ofrecen una seguridad equivalente a la que proporcionan los establecidos en esta sección para el nivel de seguridad sustancial, no es necesario que el PSC responsable del registro repita esos primeros procedimientos, siempre que dicha seguridad equivalente esté confirmada por un OEC; **3.** En los casos en que los m-IDe se expidan sobre la base de un m-IDe expedidos en virtud de un sistema de IDe válido que tenga el nivel de seguridad sustancial o alto, y teniendo en cuenta los riesgos de que se produzca un cambio en los datos de identificación de la persona, no es necesario repetir los procesos de prueba y verificación de la identidad.
ALTO	Se debe cumplir obligatoriamente una de las alternativas indicadas en los puntos 1 a 3 1. Los PCSC, a través del AGR deberán cumplir obligatoriamente los siguientes requisitos, precedente a la expedición de un m-IDe: ● **PRESENCIA:** se requiere prueba de identidad en persona o remota supervisada conforme a los procedimientos y requisitos técnicos establecidos en el DOC-ICPP-17 [3]. ● **DATOS:** mismos requerimientos establecidos en el nivel sustancial. ● **PRUEBA:** se debe asegurar que el solicitante de un m-IDe está en posesión de pruebas de identidad reconocidas conforme al ítem 5.1.3 ● **VALIDACIÓN:** se debe: ○ Comprobar que las pruebas de identidad son auténticas, utilizando tecnologías apropiadas para confirmar la integridad de los elementos de seguridad física o seguridad criptográfica y que las mismas no son fraudulentas ni modificadas inapropiadamente, y

	○ Confirmar que todos los datos de identificación y las pruebas de identidad son válidas en comparación con la información mantenida o publicada por una fuente auténtica. ● **VERIFICACIÓN:** se debe confirmar la propiedad del solicitante de un m-IDe sobre la identidad reclamada mediante comparación biométrica, utilizando tecnologías apropiadas, con una fotografía y con la prueba de identidad más sólida proporcionada para respaldar la identidad reclamada. La comparación biométrica realizada de forma remota debe cumplir con todos los requisitos especificados en el NIST SP 800-63B, Sección 5.2.3. ● **CONFIRMACIÓN DE DIRECCIÓN:** mismos requerimientos establecidos en el nivel sustancial. ● **COLECCIÓN BIOMÉTRICA:** se debe colectar y registrar datos de identificación biométrica en el momento de solicitud y registro (por ejemplo, las citadas en el ítem 5.1.3) con el propósito de no repudio y re-verificación conforme a las disposiciones establecidas en el NIST SP 800-63B, Sección 5.2.3. Se debe comprobar la validez de las mismas presentadas según una fuente auténtica. ● **CONTROLES DE SEGURIDAD:** Se debe tomar medidas para reducir al mínimo el riesgo de que la identidad de la persona no sea la identidad reclamada, teniendo en cuenta, por ejemplo, el riesgo de pruebas perdidas, robadas, suspendidas, revocadas o expiradas. Se deberá garantizar que se cumplan los controles mínimos relacionados con la garantía para sistemas de impacto alto o equivalente. **2.** Cuando los procedimientos utilizados anteriormente por un PCSC para una finalidad distinta de la expedición de m-IDe ofrecen una seguridad equivalente a la que proporcionan los establecidos en este ítem para el nivel de seguridad alto, no es necesario que el PCSC responsable del registro repita esos primeros procedimientos, siempre que dicha seguridad equivalente esté confirmada por un OEC autorizado por la AA. 3. En los casos en que los m-IDe se expidan sobre la base de un m-IDe expedidos en virtud de un sistema de IDe válido que tenga el nivel de seguridad alto, y teniendo en cuenta los riesgos de que se produzca un cambio en los datos de identificación de la persona, no es necesario repetir los procesos de prueba y verificación de la identidad. Se deben tomar medidas para demostrar que los resultados del procedimiento anterior siguen siendo válidos.

6.1.1.3. Prueba y verificación de la identidad (persona jurídica)

Nivel de Seguridad	Elementos necesarios

BAJO	1. Los PSC deberán cumplir obligatoriamente los siguientes requisitos, precedente a la expedición de un m-IDe: ● **PRESENCIA:** sin requisitos. ● **DATOS:** sin requisitos. ● **PRUEBA:** ○ El solicitante de un m-IDe declara estar en posesión de pruebas relativas a la identidad reclamada de la persona jurídica sobre la base de pruebas reconocidas conforme al ítem 5.2.1. ○ Se supone que las pruebas de identidad son auténticas **o** pueden verificarse con una fuente auténtica y las pruebas parecen ser válidas. ○ Una fuente auténtica no tiene constancia de que la persona jurídica esté en un estado que le impediría actuar como tal. ● **VALIDACIÓN:** No se realiza validación. ● **VERIFICACIÓN:** No se realiza verificación. ● **CONFIRMACIÓN DE DIRECCIÓN:** sin requisitos ● **COLECCIÓN BIOMÉTRICA:** No se realiza colección biométrica ● **CONTROLES DE SEGURIDAD:** no aplica.
SUSTANCIAL	Se debe cumplir obligatoriamente una de las alternativas indicadas en los puntos 1 a 3: 1. Los PSC deberán cumplir obligatoriamente los siguientes requisitos, precedente a la expedición de un m-IDe: ● **PRESENCIA:** se requiere prueba de identidad remota o en persona. ● **DATOS:** se requiere de datos de identificación mínimos necesarios para lograr la vinculación de la identidad. Se puede utilizar verificación basada en conocimientos para mayor confianza. ● **PRUEBA:** se debe asegurar que el solicitante de un m-IDe está en posesión de pruebas de identidad reconocidas conforme al ítem 5.2.2. ● **VALIDACIÓN:** Se debe: ○ Comprobar que las pruebas de identidad son auténticas, utilizando tecnologías apropiadas para confirmar la integridad de los elementos de seguridad física o seguridad criptográfica y que las mismas no son fraudulentas ni modificadas inapropiadamente, o ○ Confirmar que todos los datos de identificación y las pruebas de identidad son válidas en comparación con la información mantenida o publicada por una fuente auténtica. ● **VERIFICACIÓN:** Se debe realizar la vinculación entre los m-IDe de personas físicas y jurídicas conforme al ítem **6.1.1.4.** ● **CONFIRMACIÓN DE DIRECCIÓN:** Se debe requerir al solicitante de un m-IDe que proporcione una dirección física o electrónica durante el proceso de solicitud y registro. El sistema utilizado debe enviar una notificación de verificación a esa dirección, con un código de inscripción o un enlace de confirmación. El solicitante debe recibir el mensaje y usar el código o enlace proporcionado para confirmar que la dirección es válida y le pertenece realmente a efectos de garantizar que se esté

	comunicando con la persona correcta. En caso de verificación remota, se debe asegurar de que el código de inscripción y la notificación de verificación se envíen a direcciones de registro diferentes. ● **COLECCIÓN BIOMÉTRICA:** conforme al ítem **6.1.1.4.** ● **CONTROLES DE SEGURIDAD:** se debe tomar medidas para reducir al mínimo el riesgo de que la identidad de la persona no sea la identidad reclamada, teniendo en cuenta, por ejemplo, el riesgo de pruebas perdidas, robadas, suspendidas, revocadas o expiradas. Se deberá garantizar que se cumplan los controles mínimos relacionados con la garantía para sistemas de impacto moderado o equivalente. **2.** Cuando los procedimientos utilizados anteriormente por un PSC para una finalidad distinta de la expedición de m-IDe ofrecen una seguridad equivalente a la que proporcionan los establecidos en esta sección para el nivel de seguridad sustancial, no es necesario que el PSC responsable del registro repita esos primeros procedimientos, siempre que dicha seguridad equivalente esté confirmada por un OEC autorizado por la AA; **3.** En los casos en que los m-IDe se expidan sobre la base de un m-IDe expedidos en virtud de un sistema de IDe válido que tenga el nivel de seguridad sustancial o alto, y teniendo en cuenta los riesgos de que se produzca un cambio en los datos de identificación de la persona, no es necesario repetir los procesos de prueba y verificación de la identidad.
ALTO	Se debe cumplir obligatoriamente una de las alternativas indicadas en los puntos 1 a 3 1. Los PCSC, a través del AGR deberán cumplir obligatoriamente los siguientes requisitos, precedente a la expedición de un m-IDe: ● **PRESENCIA:** se requiere prueba de identidad en persona o remota supervisada conforme a los procedimientos y requisitos técnicos establecidos en el DOC-ICPP-17 [3]. ● **DATOS:** igual que el requerido en el nivel sustancial. ● **PRUEBA:** Se asegurar que el solicitante de un m-IDe está en posesión de pruebas de identidad reconocidas conforme al ítem 5.2.3 ● **VALIDACIÓN:** Se debe: ○ Comprobar que las pruebas de identidad son auténticas, utilizando tecnologías apropiadas para confirmar la integridad de los elementos de seguridad física o seguridad criptográfica y que las mismas no son fraudulentas ni modificadas inapropiadamente, y ○ Confirmar que todos los datos de identificación y las pruebas de identidad son válidas en comparación con la información mantenida o publicada por una fuente auténtica. ● **VERIFICACIÓN:** Se debe realizar la vinculación entre los m-IDe de personas físicas y jurídicas conforme al ítem 6.1.1.4. ● **CONFIRMACIÓN DE DIRECCIÓN:** igual que el requerido en el nivel sustancial. ● **COLECCIÓN BIOMÉTRICA:** conforme al ítem **6.1.1.4.** ● **CONTROLES DE SEGURIDAD:** Se debe tomar medidas para reducir al mínimo el riesgo de que la identidad de la persona no sea la

	identidad reclamada, teniendo en cuenta, por ejemplo, el riesgo de pruebas perdidas, robadas, suspendidas, revocadas o expiradas. Se deberá garantizar que se cumplan los controles mínimos relacionados con la garantía para sistemas de impacto alto o equivalente. 2) Cuando los procedimientos utilizados anteriormente por un PCSC para una finalidad distinta de la expedición de m-IDe ofrecen una seguridad equivalente a la que proporcionan los establecidos en esta sección para el nivel de seguridad alto, no es necesario que el PCSC responsable del registro repita esos primeros procedimientos, siempre que dicha seguridad equivalente esté confirmada por un OEC autorizado por la AA. Se deben tomar medidas para demostrar que los resultados del procedimiento anterior siguen siendo válidos. 3) En los casos en que los m-IDe se expidan sobre la base de un m-IDe expedidos en virtud de un sistema de IDe válido que tenga el nivel de seguridad alto, y teniendo en cuenta los riesgos de que se produzca un cambio en los datos de identificación de la persona, no es necesario repetir los procesos de prueba y verificación de la identidad. Se deben tomar medidas para demostrar que los resultados del procedimiento anterior siguen siendo válidos.

6.1.1.4. Vinculación entre los medios de identificación de personas físicas y jurídicas

El responsable autorizado de la persona jurídica será el solicitante y responsable del m-IDe de una persona jurídica, y tendrá el control del mismo. Como tal, deberá acreditar dicha atribución. El representante legal podrá ser el representante autorizado.

En todos los casos, para la vinculación de los m-IDe de una persona física y los m-IDe de una persona jurídica, deberá ser posible suspender y/o revocar una vinculación y la vinculación se realizará de la siguiente manera:

Nivel de Seguridad	**Elementos necesarios**
BAJO	1. Se debe verificar que las pruebas y datos de identidad de la persona física que actúa en nombre de la persona jurídica se hayan realizado en el nivel bajo o superior. conforme al ítem 6.1.1.2 2. La vinculación se ha establecido sobre la base de las pruebas presentadas para la identificación de la persona jurídica
SUSTANCIAL	1. Se debe verificar que las pruebas y datos de identidad de la persona física que actúa en nombre de la persona jurídica se hayan realizado en el nivel sustancial o alto conforme al ítem 6.1.1.2. 2. La vinculación se ha establecido sobre la base de las pruebas presentadas para la identificación de la persona jurídica, lo que ha dado lugar al registro del mismo por el PSC responsable.
ALTO	Punto 2 del nivel sustancial, además de lo siguiente: 1. El AGR debe verificar que las pruebas y datos de identidad de la persona física que actúa en nombre de la persona jurídica se hayan realizado en el nivel alto conforme al ítem 6.1.1.2. 2. La vinculación se ha verificado sobre la base del RUC que representa a la persona jurídica y sobre la base de información que representa de manera exclusiva a la persona física a partir de una fuente auténtica.

6.1.2. Gestión de medios de identificación

6.1.2.1. Diseño y características de los medios de identificación

Requisito	Nivel bajo	Nivel sustancial	Nivel alto
Diseño del medio de IDe	El m-IDe está diseñado de forma que el PSC toma medidas razonables para asegurar de que solo se utiliza bajo el control o la posesión de la persona a la que pertenece.	El m-IDe está diseñado de forma que se puede suponer que sólo se utilizará bajo el control o la posesión de la persona a la que pertenece.	El m-IDe está diseñado de modo que la persona a la que pertenece lo puede proteger de manera fiable contra la utilización por otros y que sólo se utilizará bajo el control o la posesión de la persona a la que pertenece, conforme al ítem 6 del DOC-ICPP-03 [1]; y protege contra la duplicación y manipulación, así como contra atacantes con elevado potencial de ataque.
Tipos de autenticadores permitidos	Se requerirá que el m-IDe utilice por lo menos uno de los FA siguientes: ● Memorized Secret:Secreto Memorizable ● Look-up Secret: Secreto de Búsqueda ● Out-of-Band: Fuera de Banda ● Single Factor OTP Device: Dispositivo de OTP de Factor Único ● Single Factor Crypto Software: Software Criptográfico de Factor Único ● Single Factor Crypto Device: Dispositivo	Se requerirá que el m-IDe utilice por lo menos dos de los FA siguientes: ● Multiple Factor OTP Device ● Multiple Factor Crypto Software ● Multiple Factor Crypto Device ● Memorized Secret **más**: ✓ Look-up Secret, ✓ Out-of-Band, ✓ Single Factor OTP Device ✓ Single Factor Crypto Software ✓ Single Factor Crypto Device	Se requerirá que el m-IDe utilice dos o más FA siguientes: ● Multiple Factor Crypto Device ● Single Factor Crypto Device más Memorized Secret ● Single Factor OTP Device más ● Multiple Factor Crypto Software ● Multiple Factor Crypto Device ● Single Factor OTP Device más Single Factor Crypto Software mas Memorized Secret OBS: El Módulo Criptográfico (en Software o en Hardware) que contiene

	Criptográfico de Factor Único ● Multiple Factor OTP Device: Dispositivo de OTP de Múltiples Factores ● Multiple Factor Crypto Software: Software Criptográfico de Múltiples Factores ● Multiple Factor Crypto Device: Dispositivo Criptográfico de Múltiples Factores		lo datos de IDe deberá estar asociado obligatoriamente a un Certificado Cualificado expedido por un PCSC y conforme al ítem 4 DOC-ICPP-06 e ítem 6 DOC-ICPP-03.
Requisitos de autenticador y verificador	● Uso de criptografía aprobada en autenticadores. ● Los autenticadores basados en software pueden detectar compromisos de plataforma y no completar operaciones comprometidas ● Comunicación segura y autenticada entre el reclamante y el verificador	● Uso de criptografía aprobada en autenticadores. ● Validar autenticadores según FIPS 140 Level 1. ● Los autenticadores basados en software deben detectar compromisos de plataforma y no completar operaciones comprometidas. ● Al menos un autenticador debe ser resistente a repeticiones. ● Demostrar intención de autenticación. ● Comunicación a través de canales protegidos. ● Verificadores validados según FIPS 140 Level 1. ● El desbloqueo de dispositivos no debe contar como factor de autenticación.	● Comunicación segura y autenticada entre el reclamante y el verificador. ● Al menos un autenticador debe ser resistente a la suplantación y a repeticiones. ● Todos los procesos de autenticación y reautenticación deben demostrar la intención de autenticación de al menos un autenticador. ● Los autenticadores multifactor utilizados deben ser módulos criptográficos de hardware validados en FIPS 140 Nivel 2 o superior en general con al menos seguridad física FIPS 140 Nivel 3. ● Los dispositivos criptográficos de un solo factor deben ser validados en FIPS

		• Los verificadores deben asegurar que los sensores biométricos cumplan con los requisitos de rendimiento establecidos en el NIST SP 800-63B, Sección 5.2.3.	140 Nivel 1 o superior en general con al menos seguridad física FIPS 140 Nivel 3. • Los verificadores deben ser validados según FIPS 140 Nivel 1 o superior.y resistentes a compromisos del verificador • Los autenticadores y verificadores basados en hardware deben resistir ataques de canal lateral. • El desbloqueo de dispositivos no debe contar como factor de autenticación. • Los verificadores deben asegurar que los sensores biométricos cumplan con los requisitos de rendimiento establecidos en el .NIST SP 800-63B, Sección 5.2.3.
Reautenticación	30 días	12 horas o 30 minutos de inactividad; puede usar 1 (un) factor de autenticación	12 horas o 15 minutos de inactividad; deberá utilizar ambos factores de autenticación
Controles de Seguridad	Se garantizará que se cumplan los controles de seguridad mínimos para sistemas de impacto bájo o su equivalente, conforme a la norma ISO/IEC 27001:2022	Se garantizará que se cumplan los controles de seguridad mínimos para sistemas de impacto moderado o su equivalente, conforme a la norma ISO/IEC 27001:2022	Se garantizará que se cumplan los controles de seguridad mínimos para sistemas de impacto alto o su equivalente, conforme a la norma ISO/IEC 27001:2022
Resistencia **Man-in-the-Middle**	Requerido	Requerido	Requerido
Resistencia	No requerido	No requerido	Requerido

Verifier-impersonation			
Resistencia **Replay**	No requerido	Requerido	Requerido
Intención de autenticación	No requerido	Recomendado	Requerido
Política de retención de registros	Requerido	Requerido	Requerido
Controles de privacidad	Requerido	Requerido	Requerido

6.1.2.2. Expedición, entrega y activación

Nivel de Seguridad	Elementos necesarios
BAJO	Después de la expedición, el m-IDe se entrega a través de un mecanismo mediante el cual se puede suponer que solo llega a la persona prevista.
SUSTANCIAL	Después de la expedición, el m-IDe se entrega a través de un mecanismo mediante el cual se puede suponer que solo se entrega a la persona a la que pertenece.
ALTO	El proceso de activación verifica que el m-IDe solo se entrega a la persona a la que pertenece conforme al ítem 6 del DOC-ICPP-03 [1].

6.1.2.3. Suspensión, revocación y reactivación

Nivel de Seguridad	Elementos necesarios
BAJO	1. Es posible suspender o revocar un m-IDe de manera eficaz y oportuna. 2. Se han tomado medidas para impedir la suspensión, revocación o reactivación no autorizadas. 3. La reactivación se llevará a cabo sólo si se siguen cumpliendo los mismos requisitos de seguridad establecidos antes de la suspensión o revocación.
SUSTANCIAL	Igual que el nivel bajo.
ALTO	Igual que el nivel bajo. Circunstancias sujetas al ítem 4.9 del DOC-ICPP-03 [1] para los casos de suspensión y revocación. El PCSC deberá definir el proceso de reactivación.

6.1.2.4. Renovación y sustitución

Nivel de Seguridad	Elementos necesarios
BAJO	Teniendo en cuenta los riesgos de un cambio en los datos de identificación de la persona, la renovación o sustitución debe cumplir los mismos requisitos de seguridad que la prueba y verificación de identidad inicial o basarse en un m-IDe válido del mismo nivel de seguridad o de un nivel superior.
SUSTANCIAL	Igual que el nivel bajo.
ALTO	Nivel bajo, además de lo siguiente: Si la renovación o sustitución se basa en un m-IDe válido, los datos de identificación de la persona se verifican con una fuente auténtica. La renovación deberá estar conforme al ítem 4.6 del DOC-ICPP-03 [1] y del DOC-ICPP-03 [1].

6.1.3. Autenticación

6.1.3.1. Requisitos de Seguridad en Mecanismo de autenticación

La tabla siguiente establece los requisitos por nivel de seguridad con respecto al mecanismo de autenticación, a través del cual la persona física o jurídica utiliza los medios de identificación para confirmar su identidad a la parte usuaria.

Nivel de Seguridad	Elementos necesarios
BAJO	1. La liberación de datos de identificación de la persona va precedida de una verificación fiable del medio de identificación y su validez. 2. Si se almacenan datos de identificación de la persona como parte del mecanismo de autenticación, dicha información deberá ofrecer protección contra la pérdida y contra cualquier peligro, incluido el análisis fuera de línea. 3. El mecanismo de autenticación deberá aplicar controles de seguridad para la verificación de los medios de identificación, por lo que es muy poco probable que actividades como intentos de adivinación, escucha, reproducción o manipulación de la comunicación por un atacante con potencial de ataque básico mejorado puedan alterar los mecanismos de autenticación. El PSC deberá establecer los controles de seguridad necesarios para la referida verificación.
SUSTANCIAL	Nivel bajo, además de lo siguiente: 1. El mecanismo de autenticación aplica controles de seguridad para la verificación de los medios de identificación, por lo que es muy poco

	probable que actividades como intentos de adivinación, escucha, reproducción o manipulación de la comunicación por un atacante con potencial de ataque moderado puedan alterar los mecanismos de autenticación. El PSC deberá establecer los controles de seguridad necesarios para la referida verificación.
ALTO	Nivel sustancial, además de lo siguiente: 2. El mecanismo de autenticación aplica controles de seguridad para la verificación de los medios de identificación, por lo que es muy poco probable que actividades como intentos de adivinación, escucha, reproducción o manipulación de la comunicación por un atacante con potencial de ataque alto puedan alterar los mecanismos de autenticación. El PCSC deberá establecer los controles de seguridad necesarios para la referida verificación.

6.1.3.2. Servicio de Identificación Electrónica

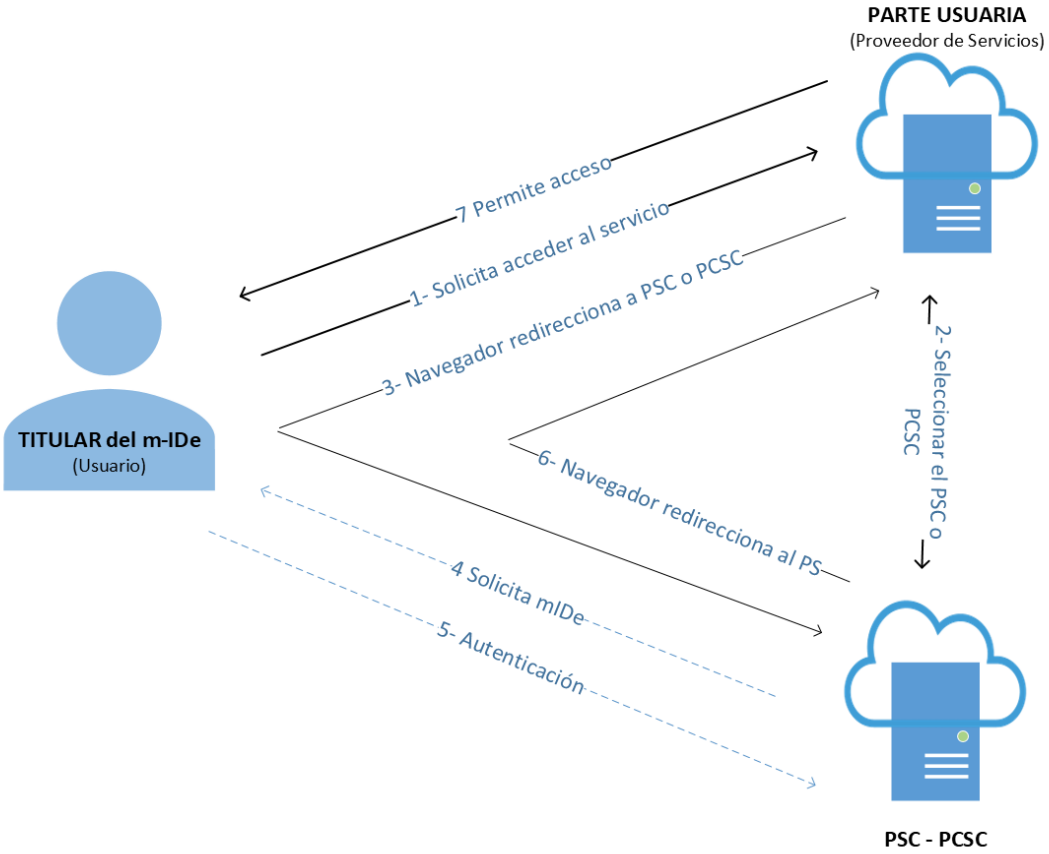
Un PSC o PCSC habilitado para prestar el servicio de expedición de m-IDE en virtud a sistemas de IDe según lo establecido en esta Política, debe contar, como parte de sus sistemas, con un componente conocido como Proveedor de Identidades.

El propósito de este componente es proporcionar a los usuarios registrados en el servicio de IDe un único m-IDe y un punto de autenticación, para acceder a los servicios ofrecidos por la PU. En resumen, brinda el servicio de autenticación a la PU en su condición de Proveedor de Servicio, mediante una integración técnica y de confianza entre ambos sistemas.

El cual concluye después del proceso de autenticación electrónica y la comunicación del resultado de dicho proceso a la PU como proveedor del servicio. Como resultado de este proceso, la PU verifica el nivel de IDe obtenido por el titular en el proveedor de identidad y lo utiliza para otorgar los accesos a sus servicios pertinentes.

Este componente es responsable del proceso técnico de autenticación electrónica de los usuarios Titulares registrados en el servicio de IDe ofrecido por el PSC o PCSC. Por lo tanto, este componente es responsable de:

- Solicitar el m-IDe correspondiente al usuario del servicio de IDe.
- Aceptar o rechazar la autenticación del usuario del servicio de IDe.
- Asignar el nivel de seguridad adecuado a la IDe según las condiciones definidas en la presente política.
- Transmitir el resultado del proceso de autenticación y, por lo tanto, el nivel de IDe del usuario a la PU mediante aserciones.



1. El titular desea acceder a un servicio ofrecido por la Parte Usuaria (PU).
2. La PU selecciona el PSC o PCSC, en el que confía el proceso de autenticación electrónica de sus usuarios. En este punto, a PU puede brindar la opción de elegir entre diferentes PSC o PCSC, o dejar la elección al titular.
3. Después de seleccionar el PSC o PCSC, el titular es redirigido al componente proveedor de identidad del PSC o PCSC para realizar el proceso de autenticación electrónica y presentar el m-IDe correspondiente.
4. El PSC o PCSC solicita al titular el m-IDe necesario para el proceso de autenticación electrónica.
5. El titular lleva a cabo el proceso de autenticación electrónica en el PSC o PCSC, presentando el m-IDe del que es titular.
6. El PSC o PCSC redirige al usuario a la PU con el resultado de la autenticación contenida en una aserción, que incluye el nivel de IDe logrado por el titular en el componente de proveedor de identidad del PSC o PCSC.
7. La PU autoriza o no el acceso a sus servicios, verificando el nivel de IDe obtenido por el usuario titular en el componente proveedor de identidad.

Durante el proceso de autenticación descrito en el ejemplo, se establece una relación de confianza entre el componente proveedor de identidad del PSC o PCSC y la PU para

intercambiar información de autenticación e identificación de los usuarios titulares. En el siguiente punto, se abordarán las consideraciones técnicas y de seguridad para este intercambio de información, conocido como federación.

6.1.3.2. Federación de identidades y aserciones.

La federación es un proceso que permite la transmisión de datos de identificación, autenticación y otros atributos del titular de un m-IDe a través de sistemas en red. En un escenario de federación, el PCS o PCSC, cumple la función de verificador, a través de su componente de Proveedor de Identidades. La PU es la entidad que recibe y utiliza la información proporcionada por este componente del PCS o PCSC. Los sistemas de identificación federados utilizan aserciones para llevar a cabo esta tarea. Las aserciones son afirmaciones realizadas por un PCS o PCSC a una PU, que contienen información sobre el titular de un m-IDe en su papel de suscriptor.

Una aserción normalmente incluye un identificador para el Titular en su calidad de suscriptor, lo que permite la asociación del suscriptor con sus interacciones previas con la PU. Las aserciones pueden incluir adicionalmente valores de atributos o referencias de atributos que caracterizan aún más al suscriptor y respaldan la decisión de autorización en la PU. También pueden estar disponibles atributos adicionales fuera de la aserción como parte del protocolo de federación más amplio.

Estos valores de atributos y referencias de atributos se utilizan a menudo para determinar los privilegios de acceso para el control de acceso basado en atributos (ABAC) o para facilitar una transacción (por ejemplo, dirección de envío).

Se deberán tener en cuenta por parte de los PSC o PCSC las siguientes consideraciones para la implementación de su federación en su componente proveedor de identidades teniendo en cuenta que cada nivel sucesivo incluye y cumple todos los requisitos de los niveles inferiores:

Nivel de Seguridad	Requisito
Bajo	Aserción del portador, firmada por el PSC.
Sustancial	Aserción del portador, firmada por el PSC y cifrada para la PU.
Alto	Aserción del titular de la clave, firmada por el PCSC y cifrada para la PU.

Las consideraciones mencionadas se basan en el estándar NIST SP 800-63C y las cuales deben ser consideradas para su correcta aplicación.

6.1.4 Gestión y organización

Los PSC o PCSC que expidan m-IDe deben contar con prácticas y políticas de gestión de la seguridad de la información documentadas, metodologías de gestión de riesgo para proporcionar garantías de que se aplican prácticas eficaces. En esta sección, todos los requisitos o elementos deberán entenderse como acordes a los riesgos en el nivel determinado.

6.1.4.1 Disposiciones generales

Nivel de Seguridad	Elementos necesarios
BAJO	1. El PSC debe cumplir con los requisitos legales que le incumben en relación con el funcionamiento y la prestación del servicio, incluidos los tipos de información que se pueden solicitar, cómo se realiza la prueba de identidad y qué información se puede conservar. 2. El PSC debe estar en condiciones de demostrar su capacidad para asumir el riesgo de la responsabilidad por daños y perjuicios, así como disponer de los recursos financieros suficientes para seguir funcionando y prestar los servicios. 3. El PSC es responsable del cumplimiento de cualquiera de los compromisos externalizados a otra entidad, así como del cumplimiento de la política del sistema. 4. Los PSC deberán cumplir las obligaciones y responsabilidades establecidas en la Ley N° 6822/2021.
SUSTANCIAL	Igual que el nivel bajo.
ALTO	Igual que el nivel sustancial y además: 1. Los sistemas de IDe deberán contar con un plan de cese eficaz. Dicho plan deberá incluir las suspensiones del servicio de manera ordenada o la continuación por otro proveedor, la manera en que se informa a las autoridades competentes y los usuarios finales, así como detalles sobre cómo se deben proteger, conservar y destruir los registros en cumplimiento de la política del sistema. 2. Cumplir las responsabilidades y obligaciones de los PCSC, conforme al ítem 4.1.2. del DOC-ICPP-03 [1].

6.1.4.2. Avisos publicados e información del usuario

Nivel de Seguridad	Elementos necesarios

BAJO	1. El PSC debe mantener publicada información que incluya todos los términos, condiciones y tarifas aplicables, incluidas las limitaciones de su uso. La definición del servicio incluirá una política de privacidad. 2. El PSC debe poner en práctica políticas y procedimientos apropiados con el fin de garantizar que los usuarios del servicio sean informados de manera oportuna y fiable de los cambios que se produzcan en la definición del servicio y en los términos, las condiciones y la política de privacidad aplicables del servicio de confianza. 3.El PSC debe implementar políticas y procedimientos apropiados que proporcionen respuestas completas y correctas a las solicitudes de información.
SUSTANCIAL	Igual que el nivel bajo.
ALTO	Igual que el nivel sustancial y además conforme al ítem 2 del DOC-ICPP-03 [1]

6.1.4.3. Gestión de la seguridad de la información

Nivel de Seguridad	Elementos necesarios
BAJO	El PSC debe contar con un sistema de gestión de la seguridad de la información eficaz para la gestión y el control de los riesgos para la seguridad de la información.
SUSTANCIAL	Nivel bajo, además de lo siguiente: El sistema de gestión de la seguridad de la información del PSC debe satisfacer normas o principios establecidos para la gestión y el control de los riesgos para la seguridad de la información.
ALTO	Igual que el nivel sustancial y además conforme al ítem 6 del DOC-ICPP-05 [2] e ítem 5 del DOC-ICPP-03 [1].

6.1.4.4. Conservación de información

Nivel de Seguridad	Elementos necesarios
BAJO	1. El PSC debe registrar y mantener la información pertinente mediante un sistema de gestión de registros eficaz y las buenas prácticas en relación con la protección de datos y la conservación de datos. 2. Los registros se deben conservar y proteger durante el tiempo en que sean necesarios para fines de auditoría y de investigación de las infracciones de seguridad, y retención, tras lo cual los registros se destruirán de manera segura.

SUSTANCIAL	Igual que el nivel bajo.
ALTO	Igual que el nivel sustancial y además conforme al artículo 10 de la Ley N° 6822/2021.

6.1.4.5. Instalaciones y personal

La siguiente tabla representa los requisitos relativos a las instalaciones, el personal y los PSS del PSC o PCSC, que desempeñen las funciones reguladas por la presente política. El cumplimiento de cada uno de los requisitos será proporcional al nivel de riesgo asociado al nivel de seguridad indicado.

Nivel de Seguridad	**Elementos necesarios**
BAJO	1. El PSC debe contar con procedimientos que garanticen que el personal cuente con la debida formación, cualificaciones y experiencia en las competencias necesarias para ejecutar las funciones que desempeñan. 2. El PSC debe contar con la dotación de personal suficientes para el funcionamiento y la asignación de recursos al servicio de manera adecuada según sus políticas y procedimientos. 3. Las instalaciones utilizadas por el PSC para la prestación del servicio deberán estar controladas de manera continua y protegidas contra daños causados por fenómenos ambientales, accesos no autorizados y otros factores que puedan afectar a la seguridad del servicio. 4. Las instalaciones utilizadas por el PSC para la prestación del servicio deberán garantizar que el acceso a las zonas que tengan o procesen información personal, criptográfica o confidencial se limita al personal autorizado.
SUSTANCIAL	Igual que el nivel bajo.
ALTO	Igual que el nivel sustancial y además conforme al ítem 5 del DOC-ICPP-03 [1].

6.1.4.6. Controles técnicos

Nivel de Seguridad	**Elementos necesarios**
BAJO	1. El PSC debe contar con controles técnicos proporcionales para gestionar los riesgos que puedan afectar a la seguridad de los servicios y que protejan la confidencialidad, integridad y disponibilidad de la información que se procesa.

	2. El PSC debe contar con canales de comunicación electrónica que se utilizan para intercambiar información personal o confidencial están protegidos contra escucha, manipulación y reproducción. 3. El acceso al material criptográfico confidencial, si se utiliza para expedir m-IDe y autenticación, se limita exclusivamente a aquellas funciones y aplicaciones que requieren estrictamente ese acceso. Deberá garantizarse que dicho material no se almacene nunca de manera continua en forma de texto sin formato. 4. El PSC debe contar con procedimientos para garantizar el mantenimiento de la seguridad a lo largo del tiempo y que sea posible responder a los cambios en los niveles de riesgo, los incidentes y las violaciones de la seguridad. 5. Todos los medios que contienen información personal, criptográfica o confidencial se almacenan, transportan y eliminan de manera segura.
SUSTANCIAL	Igual que el nivel bajo, además de lo siguiente: El material criptográfico confidencial, si se utiliza para la expedición de m-IDe y autenticación, está protegido contra su manipulación
ALTO	Igual que el nivel sustancial y conforme al ítem 5 y 6 del DOC-ICPP-03 [1].

6.1.4.7. Cumplimiento y auditoría

Nivel de Seguridad	Elementos necesarios
BAJO	El PSC debe contar con auditorías internas periódicas cuyo ámbito comprenda todas las partes pertinentes para la prestación de los servicios a fin de garantizar el cumplimiento de las políticas pertinentes.
SUSTANCIAL	El PSC debe contar con auditorías internas o externas periódicas e independientes cuyo ámbito comprenda todas las partes pertinentes para la prestación de los servicios a fin de garantizar el cumplimiento de las políticas pertinentes.
ALTO	El PCSC debe contar con auditorías externas periódicas e independientes cuyo ámbito comprenda todas las partes pertinentes para la prestación de los servicios a fin de garantizar el cumplimiento de las políticas pertinentes conforme a la Ley N° 6822/2021 y al ítem 8 del DOC-ICPP-03 [1].

7. LISTAS DE SISTEMAS DE SISTEMAS DE IDENTIFICACIÓN ELECTRÓNICA

De conformidad a la Ley, la AA mantendrá disponible en su sitio de Internet la Lista de Sistemas de IDe, la cual será aprobada por Resolución Ministerial y contendrá como mínimo la siguiente información:

1) El nombre del Sistema
2) El m-IDe
3) Nivel de seguridad
4) Responsable del sistema
5) Fecha de vigencia

8. DOCUMENTOS DE REFERENCIA

8.1 REFERENCIA EXTERNA

- Ley Nº 6822/2021 "De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos"
- Digital identity Guidelines del NIST SP 800-63
- NIST Special Publication 800-63A
- NIST Special Publication 800-63B
- NIST Special Publication 800-63C
- UK digital identity and attributes trust framework beta version (0.3) - GOV.UK
- Reglamento de ejecución UE 2015/1502R

8.2. REFERENCIAS A DOCUMENTOS QUE COMPONEN LA ICPP

Tabla de Documentos Referenciados

REF.	NOMBRE DEL DOCUMENTO	CÓDIGO
[1]	Directivas obligatorias para la formulación y elaboración de la Declaración de Prácticas de certificación de los Prestadores Cualificados de Servicios de Confianza de la ICPP	DOC-ICPP-03
[2]	Características mínimas de seguridad para las autoridades de registro de la ICPP	DOC-ICPP-05
[3]	Procedimiento de identificación del solicitante de certificados en forma remota en la ICPP	DOC-ICPP-17