ACEPTA

Empresas
a velocidad
digital

PO01

Política de Biometría

Febrero de 2016

RESPONSABLES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Certificación y Seguridad	- Gerente de Certificación y Seguridad - Oficina Técnica	Gerente General

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
Política de Biometría - PO01	1.0	Primera versión	22-2-2016
Política de Biometría - PO01	4.0	Revisión anual	01-10-2016
Política de Biometría - PO01	5.0	Revisión anual	01-10-2017
Política de Biometría - PO01	6.0	Revisión anual	01-10-2018
Política de Biometría - PO01	7.0	Revisión anual	01-10-2019
Política de Biometría - PO01	8.0	Revisión anual	01-10-2020
Política de Biometría - PO01	9.0	Revisión anual	15-03-2022
Política de Biometría - PO01	10.0	Revisión anual	15-03-2023

Política de Biometría - PO01	10.1	Ajuste punto 1.5	03-07-2023
Política de Biometría - PO01	11.0	Revisión anual	30-04-2024

CLASIFICACIÓN DEL DOCUMENTO

NIVEL DE CRITICIDAD: Baja **NIVEL DE CONFIDENCIALIDAD: Pública**
NOTA DE CONFIDENCIALIDAD: Se encuentra disponible ante su solicitud.

CONTROL DE DIFUSIÓN

AUTOR/ES: Gerencia de Certificación y Seguridad
DISTRIBUCIÓN: • Sitio web • Ministerio de Economía

REFERENCIAS

Documentos Internos	
Título	**Nombre del archivo**
Documentos Externos	
Ley N° 19.628 Guía-de-Evaluación-Procedimientos-de-Acreditación-PSC-BIO-v1.1 Reglamento DS181	

ÍNDICE

1. Introducción

1.1 Presentación

Este documento presenta la Política de Biometría de Acepta; la cual incorpora las reglas a los que se sujeta los servicios de certificación que presta Acepta y que están relacionadas con la gestión de los datos usados en la creación y la verificación de los elementos biométricos que son gestionados por esta empresa, las condiciones asociadas al enrolamiento, verificación, uso, suspensión y la revocación de los datos biométricos asociados a un titular, todo lo cual se encuentra definido en esta política. Se describe además los papeles, responsabilidades y relaciones entre el usuario final y Acepta, siendo este documento un complemento a la Declaración de Prácticas de Biometría de Acepta.

La Política de Biometría referida en este documento se utilizará para el enrolamiento, verificación de identidad y uso de los datos biométricos generados por Acepta. Mediante los datos biométricos capturados por Acepta, a través de los sensores de captura biométrica que se indican en esta Política de biometría, se generarán los patrones y/o minucias de comparación a ser utilizados por terceros durante el proceso de verificación de identidad.

Cabe indicar que la presente Declaración de Políticas de Biometría se ha generado siguiendo las especificaciones del documento de la "Guía de evaluación procedimiento de acreditación PSC BIO" definido por el Ministerio de Economía para este tipo de documentos. Estas políticas son las que se prosigue en detallar, y están disponibles en el Sitio WEB de Acepta para conocimiento público.

Esta Política de Biometría asume el manejo de conceptos básicos de Infraestructura biométrica, en caso contrario se recomienda estudiar estos conceptos, previo a continuar con la lectura del presente documento.

1.1.1 Sobre las Políticas de Certificación

Las políticas de certificación aquí descritas establecen el ciclo de vida de los servicios biométricos que provee Acepta, que como antes se ha mencionado incluyen desde la gestión de la solicitud de enrolamiento, la verificación y validación de la información proporcionada, pasando por la generación, validación de identidad, uso, administración de la información biométrica, su suspensión y su revocación. Es decir son aquellas políticas que dan seguridad y confianza a los servicios biométricos provistos por Acepta.

1.1.2 Alcance

El alcance de la Declaración de Políticas de Certificación de biometría detalla las condiciones de los servicios que presta Acepta a sus clientes como autoridad de PSC de Biometría.

1.1.3 Referencias

La presente Declaración de Políticas de Biometría se ha generado siguiendo las especificaciones del documento "Guía de evaluación procedimiento de acreditación PSC BIO" definido por el Ministerio de Economía para este tipo de documentos.

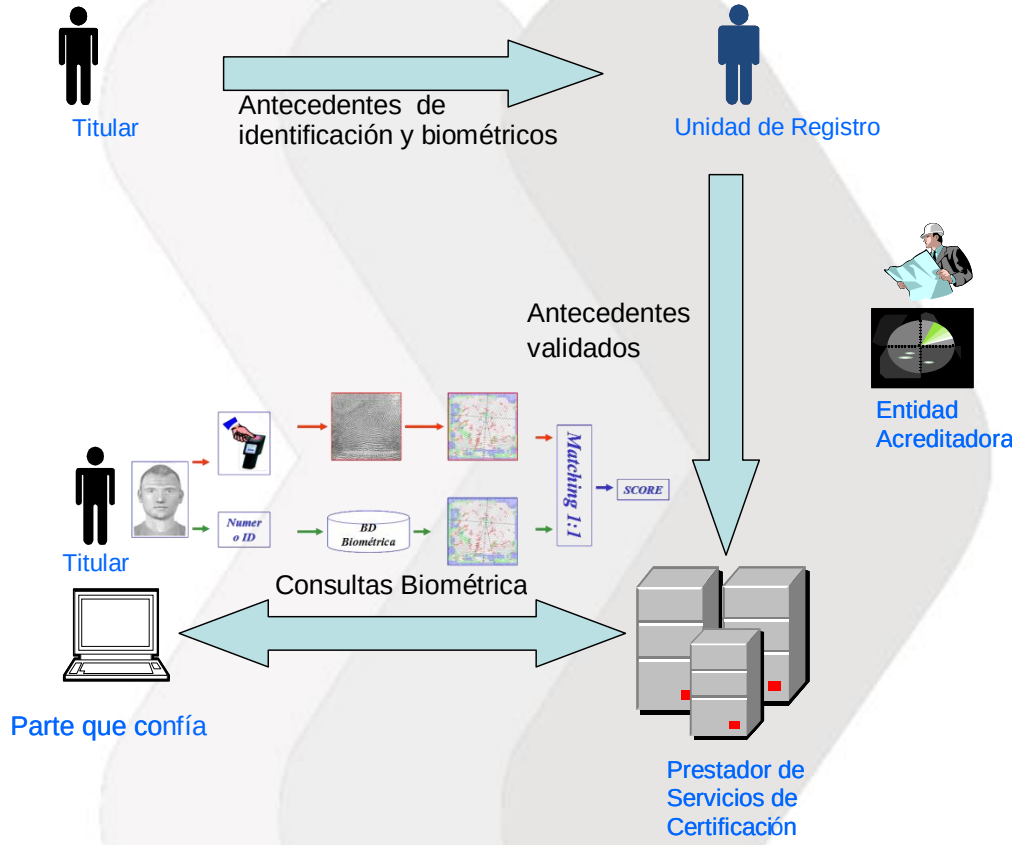
1.2 Identificación

El presente documento se denomina “Políticas de Biometría de Acepta”, las que internamente se citan como CPB y están registradas con el número único internacional (OID) 1.3.6.1.4.1.6891.300.

En las CPS de Acepta, sección “1.2 Identificación”, se presenta la lista completa de OIDs administrados por Acepta.

1.3 Comunidad y Aplicabilidad

Los servicios de biometría de Acepta están insertos en una infraestructura en que se relacionan distintas entidades. Básicamente existen 5 tipos: Autoridad Certificadora o Prestador de Servicios de Certificación (PSC), Registro (UR), titulares, terceras partes que confían en los datos biométricos y entidades acreditadoras. La siguiente figura muestra dicha relación:



1.3.1 Comunidad de usuarios

- **Titulares**: Son las personas para los cuales se realiza el procedimiento de enrolamiento biométrico, almacenando la información de dicho titular en los sistemas de Acepta para futuras verificaciones de identidad realizadas por terceros.

- **Unidades de Registro (UR)**: La recepción y procesamiento de las solicitudes enrolamiento biométrico es realizada por una o más unidades de registro. Estas efectúan la verificación de los antecedentes y de la identidad de los suscriptores que es enrolado en los sistemas biométricos de Acepta. Estas UR son parte de Acepta u organismos independientes, pero que establecen y llevan a cabo sus operaciones sobre la base de una acreditación con Acepta.

Cabe señalar que un PSC puede por sí mismo realizar el papel de UR, vale decir, recibir directamente las solicitudes de enrolamiento.

- **Prestador de Servicios de Certificación o Autoridad Certificadora**: Es la organización que opera y controla el funcionamiento de los procesos de enrolamiento, verificación, uso, así como también informa el estado de los datos biométricos de cada titular que ella ha enrolado; en este caso es Acepta.

  Adicionalmente, Acepta puede acreditar a una o más "Autoridades Certificadoras" (PSC), para que enrolen y verifiquen datos biométricos, bajo las mismas políticas y procedimientos de Acepta. Para ello, Acepta emite un certificado del tipo de "Prestador de Servicios de Certificación", con el cual el PSC acreditado puede firmar los datos biométricos de sus titulares enrolados y que han de ser verificados por los suscriptores finales.

- **Tercera parte que confía**: Son aquellas entidades, que enfrentadas a un posible titular de datos biométricos de Acepta, requieren verificar que dicha persona es quien dice ser. La parte que confía debe contar con mecanismos que le permitan contrastar la impresión dactilar capturada en vivo contra aquella almacenada pro la PSC de Acepta.; verificando tanto la identidad como la vigencia del dato biométrico contra el cual está comparando.

- **Entidad Acreditadora**: En algunos tipos de operaciones biométricas, la comunidad de usuarios requiere de un organismo independiente y de confianza que acredite que las políticas y prácticas de biometría de la PSC, de manera que ellas sean coherentes con las necesidades de verificación de identidad, de seguridad de la información, correcto uso y privacidad de la información, así como que el PSC cumple cabalmente con dichas políticas y prácticas. Por ejemplo, para los servicios biométricos, la entidad acreditadora es el Ministerio de Economía.

Los usuarios que se enrolen o verifiquen la identidad de un titular, a través de medios biométricos, deben conocer y estar en conformidad con lo establecido en estas Políticas y Prácticas del Proveedor de Servicios de Certificación.

1.4 Aplicabilidad de los datos biométricos

Los datos biométricos gestionados por Acepta se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Declaración de Políticas de Biometría, en las correspondientes Prácticas de Certificación Biométrica y en concordancia con la normativa vigente.

1.4.1 Tipos y usos de los datos biométricos

Acepta define distintos tipos de enrolamiento biométrico, definiendo para cada tipo un nivel de seguridad, restricciones y requerimientos específicos respecto a las medidas tomadas para la autentificación, mecanismos de verificación de identidad, revocación y utilización de los datos biométricos. Los usuarios deberán elegir la clase de registro biométrico que más se ajuste a sus necesidades.

El uso que se ha definido para los datos biométricos gestionados por Acepta, son el verificar la identidad de una persona, determinando si ella es quien dice ser. Esta verificación puede ser parte de

cualquier proceso en que un mandante requiera asegurar la identidad de un titular, sin necesidad de que el mandante se encuentre presencialmente en cada punto de verificación de identidad. En este caso Acepta, actuando como mandado, realizará la comparación automática del dato biométrico capturado en vivo, respecto de aquel que ha sido registrado en el proceso inicial de enrolamiento del titular. El resultado de esta comparación será una aprobación o rechazo de identidad sujetos a los niveles de FRR (Falso rechazo) o FAR (Falsa Aceptación) declarados pro Acepta.

El conjunto de normas que regulan la aplicabilidad de los datos biométricos, en determinados ambientes y comunidades se denomina "Política de Biometría" o CPB. Acepta posee una política de biometría asociada a cada tipo de registro biométrico que provee.

Los datos biométricos gestionados por Acepta se han ajustado para soportar las siguientes necesidades de seguridad:

1. **Autentificación:** proporciona suficientes garantías respecto a la identidad del titular del dato biométrico, al requerirse la presencia del titular junto con su Cédula Nacional de Identidad al momento de realizar el primer enrolamiento.
2. **Integridad de mensajes:** los datos biométricos son almacenados y firmados con certificado de firma electrónica avanzada de la PSC, lo que permiten validar si el contenido del dato biométrico ha sido alterado en el tiempo transcurrido desde su generación.
3. **Verificación de identidad:** las firmas biométricas ofrecen los medios de respaldo para demostrar fehacientemente, la autenticidad de un mensaje.

1.4.2 Usos Prohibidos

Los datos biométricos se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente Política de Certificación, y de acuerdo a la normativa vigente. Cualquier uso diferente a los indicados está expresamente prohibido.

1.4.3 Contenido de los datos biométricos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación biométrica de Acepta.

1.5 Detalle de los contactos y administración de la PSC

Cualquier consulta puede ser realizada al siguiente contacto:

- **Nombre**: Acepta.com S.p.A.
- **Dirección**: Enrique Foster Sur N°20 piso 5, Las Condes, Santiago de Chile
- **Portal de Clientes**: https://acepta.portalbeaware.com/login
    - Cree su cuenta con su Nombre, apellido, RUT y mail
    - Recibirá mail de confirmación
    - Una vez confirmado el mail, recibirá su clave
    - Ingrese su caso ingresando con su mail y clave registradas
- **Número telefónico**: (+56-2) 24968100
- **Autoservicio de asistencia**: https://asistencia.acepta.com/

1.6 Definiciones y Acrónimos

El alcance de las definiciones del documento de Políticas de Certificación, se entenderá como:

- **Autoridad de Certificación:** Es aquella entidad que en conformidad con la legislación vigente de firma electrónica, emite certificados electrónicos
- **Unidad de Registro:** Es aquella Unidad designada por Acepta que realiza la verificación de identidad de los solicitantes de enrolamiento biométrico.
- **Dato biométrico:** Cualquier rasgo físico intrínseco de un titular
- **Declaración de Prácticas de Certificación:** Declaración de Acepta, respecto a aquellas prácticas, a nivel de sistemas y de personal, que en base a sus buenas prácticas dan seguridad y confianza a los datos biométricos y servicios provistos por Acepta.
- **Firma electrónica avanzada:** Es aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera exclusiva tanto al suscriptor, como a los datos a que se refiere, y por haber sido creada por medios que mantiene bajo su exclusivo control.
- **Prestador de Servicios de Certificación (PSC):** Es aquella entidad que en conformidad con la legislación vigente de firma electrónica, emite certificados electrónicos, marca de tiempo o de biometría
- **Política de biometría:** Es el conjunto de reglas que indican la aplicabilidad de un dato biométrico a una comunidad en particular y/o clase de aplicación con requerimientos de seguridad comunes. Es el documento que completa la Declaración de Prácticas de Certificación biométrica, estableciendo las condiciones de uso y los procedimientos seguidos por Acepta para gestionar sus datos biométricos.
- **Titulares:** Son las personas para los cuales se realiza el procedimiento de enrolamiento biométrico, almacenando la información de dicho titular en los sistemas de Acepta para futuras verificaciones de identidad realizadas por terceros.
- **Terceras partes que confían:** Aquellas personas que depositan su confianza en la PSC de Acepta, durante el proceso de enrolamiento o de verificación de identidad, según lo descrito en esta Declaración de Prácticas de Certificación de biometría y en las Políticas de biometría.

Acrónimos

- AC: Autoridad Certificadora
- UR: Unidad de Registro
- CPB: Políticas Biométricas
- CPS: Certification Practice Statement
- CPSB: Prácticas de certificación biométricas
- OID: Object Identifier
- PSC: Prestador de Servicios de Certificación

2 Requerimientos Generales

2.1 Obligaciones

Acepta, en su calidad de Prestador de Servicios de Certificación de Biometría, se obliga a realizar las siguientes actividades en la prestación de sus servicios:

1. Contar con reglas sobre políticas de biometría y prácticas de certificación biométrica que sean objetivas y no discriminatorias y comunicadas a los usuarios de manera sencilla y en idioma castellano.
2. Contar con un registro fidedigno de los antecedentes proporcionados por titulares de datos biométricos al momento de comprobarse fehacientemente su identidad.
3. Comprobar fehacientemente la identidad del titular durante el proceso de enrolamiento biométrico.
4. Mantener un registro de acceso público de los datos biométricos, en el que quede constancia de la identificación de los titulares enrolados y de aquellos datos biométricos que queden sin efecto, sea por revocación de los mismos.
5. Tratar los datos personales recolectados con ocasión de la actividad de certificación dando cumplimiento a lo dispuesto en la Ley 19.628 sobre protección de la vida privada.
6. En el caso de cesar voluntariamente en su actividad, comunicarlo previamente a los titulares de los datos biométricos capturados y, en caso de no existir oposición de los titulares, transferir los datos biométricos a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, deja sin efecto los datos biométricos respecto de los cuales el titular se haya opuesto a la transferencia.
7. Publicar en el home del sitio web de Acepta las resoluciones de la Entidad Acreditadora que la afecten.
8. Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que dará a los datos biométricos, especificando, de ser el caso, si los va a transferir y a quién, o si los datos biométricos quedarán sin efecto.
9. Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento concursal de liquidación o que se encuentre en cesación de pagos.
10. Cumplir con las demás obligaciones legales, especialmente las establecidas en la ley N° 19.799, su reglamento, y las leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada.
11. Ejecutar la actividad de certificación de conformidad a lo dispuesto en esta Declaración de Prácticas de Certificación biométrica.
12. Realizar el enrolamiento y verificación de identidad con mecanismos tecnológicos que garanticen que el proceso de certificación es realizado adecuadamente y que cumplen con los requisitos establecidos por la Entidad Acreditadora.
13. Revocar los datos biométricos en los cuales se vea comprometida la confianza respecto a la veracidad de su contenido.

2.1.1 Obligaciones de la PSC de Acepta

La PSC Acepta, se obliga a cumplir las ¨Prácticas de certificación biométrica, verificando qué clientes pueden hacer uso del dato biométrico capturado durante el proceso de enrolamiento definido por las mismas prácticas. Del mismo modo, se obliga a realizar un adecuado proceso de enrolamiento, de manera que el dato biométrico quede asociado de manera correcta con el titular de dicho dato biométrico. Para esto hará uso de información complementaria tales como el estado de la cédula de identidad, la información biométrica contenida en esta última, u otro elemento que le permita de manera fehaciente realizar un primer registro del titular. Acepta se obliga además a utilizar los datos biométricos sólo para el uso que el titular de dichos datos haya autorizado, manteniendo la integridad, confidencialidad y disponibilidad de los mismos así como cumpliendo con la regulación vigente sobre privacidad de datos personales.

2.1.2 Obligaciones de Unidad de Registro Biométrico UR

Cada UR que operé como servicio de la PSC acreditada deberá cumplir las normas y ser consistente con lo establecido en el documento de Prácticas de Certificación Biométrica de la PSC.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.1.3 Obligaciones del Titular

Los Titulares que sean objeto de un enrolamiento y captura biométrica en los sistemas de la PSC de Acepta, se obligan a conocer las políticas y prácticas de certificación biométrica y entregar antecedentes fidedignos al momento de la solicitud.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.1.6 Obligaciones los Usuarios

Los usuarios que hagan uso de la verificación de identidad biométrica provista por la PSC de Acepta, y que deposite su confianza en dicha verificación deberán conocer el alcance de uso de la verificación de identidad provista por Acepta.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.1.7 Confianza en los datos biométricos y la verificación de identidad

Las partes que consideren confiar en los datos biométricos así como en la verificación de identidad provista por Acepta deberán tener conocimiento de las normas legales que sigue el Proveedor de Servicios de Certificación, verificar la autenticidad de su firma y asegurar el estado de la firma con que se protegen los datos biométricos capturados por la PSC.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.1.9 Obligaciones de los Repositorios

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.2. Responsabilidades Legales

Acepta será responsable de los daños y perjuicios que en el ejercicio de su actividad ocasionen la verificación de identidad por ella provista. Corresponderá al prestador de servicios demostrar que actuó con la debida diligencia en el proceso de verificación de identidad solicitada.

Sin perjuicio de lo dispuesto en el párrafo anterior, Acepta no será responsable de los daños que tengan su origen en el uso indebido o fraudulento de un dato biométrico o resultado biométrico provisto por Acepta.

En ningún caso la responsabilidad que pueda emanar de una verificación de identidad de la PSC de Acepta, comprometerá la responsabilidad pecuniaria del Estado.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.2.1 Responsabilidad Pecuniaria

Las responsabilidades que afectan la operación de Acepta se encuentran establecidas y limitadas a lo señalado en el artículo 14 de la Ley 19.799.

En todo caso, la responsabilidad de Acepta cualquiera sea la naturaleza de la acción o reclamo y salvo que medie dolo o culpa grave atribuible a ésta, quedará limitada como máximo al monto correspondiente a UF5.000 (cinco mil unidades de fomento), monto asegurado de conformidad con lo dispuesto en el artículo 14 de la Ley 19.799 y el artículo 12 del Decreto Supremo 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción.

La actividad de certificación biométrica se encuentra limitadas al ciclo de vida del dato biométrico, esto es:

1. Enrolamiento. Proveer todas las condiciones necesarias para que durante el enrolamiento de un titular, se pueda requerir y proporcionar toda la información necesaria para el correcto enrolamiento del mismo. Una vez que el prestador de servicios de certificación recibe la información asociada al enrolamiento, debe proceder a la aprobación de la misma, y para ello deberá comprobar los antecedentes que le han sido declarados, debiendo comprobar en la forma señalada en esta CPB y, especialmente la identidad del solicitante.

2. Firma del dato biométrico. Una vez que se ha efectuado el registro del solicitante y se ha verificado la exactitud de los datos proporcionados, el prestador de servicios de certificación procede a firmar el dato biométrico a fin de asegurar su integridad.

3. Publicación y archivo. Una vez que se ha efectuado el enrolamiento, validación de la data, el registro y firma del dato biométrico, la PSC de Acepta hará público la identificación de este registro en un acceso público.

4. Revocación. Hacer cesar la vigencia del dato biométrico, de manera temporal o definitiva, según sea el caso en la forma descrita en esta CPS.

2.2.2 Fuerza Mayor

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.2.3 Responsabilidad de la PSC y UR

Aplica el régimen de responsabilidad establecido en 2.2, no siendo pertinente diferenciar entre la responsabilidad de la PSC y la UR.

2.3 Interpretación y Resguardos Legales

Acepta declara efectuar sus actividades en conformidad con los principios generales de la legislación chilena y dando cumplimiento a todas y cada una de las leyes aplicables a las actividades desarrolladas por Acepta.

En particular, declara dar estricto cumplimiento a la Ley Nº 19.496, sobre Protección de los Derechos de los Consumidores y la Ley Nº 19.628, sobre Protección de la Vida Privada, cuyo tenor es regular el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.4 Publicación y Repositorios

Acepta publica en su sitio Web en https://sovos.com/es/politicas-y-practicas/, las prácticas de certificación biométrica por ella utilizadas, así como las políticas de biometría (CPB) pertinentes a sus servicios de verificación de identidad biométrica, las cuales están a disposición de los usuarios sin cargo alguno.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.5 Privacidad y Protección de los Datos

Acepta, adhiere y efectúa sus operaciones en conformidad con lo establecido por la Ley Nº 19.628, sobre Protección de la Vida Privada.

Las políticas de privacidad de Acepta se encuentran publicadas en https://sovos.com/es/politicas-y-practicas/ .

2.5.1 Tipos de Información a Proteger

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.5.2 Tipos de Información que Puede ser Entregada

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.5.3 Información del dato biométrico

Los datos biométricos capturados por Acepta están en conformidad con el formato ISO/IEC 19785-1, ISO/IEC 19794-2, ANSI INCITS 377 e ISO/IEC 19794-3.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.5.4 Entrega de Información sobre la Revocación de un dato biométrico

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.5.5 Entrega de Información en virtud de un Procedimiento Judicial

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.5.6 Entrega de Información a Petición del Titular

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

2.6 Derechos de Propiedad Intelectual

Todos los documentos y programas utilizados por Acepta en la Prestación de Servicios de Certificación Biométrica son propiedad intelectual de Acepta.

Los documentos definidos cómo públicos pueden ser reproducidos respetando las restricciones indicadas en cada documento:

- Políticas de privacidad
- Política de biometría
- Prácticas de certificación biométrica

3 Identificación y Autenticación

Tanto las políticas como las prácticas implementadas por Acepta, en la validación de la identidad del titular de un dato biométrico, son presentadas en el documento de políticas biométricas.

3.1 Registro Inicial

3.1.1 Registro de Nombres

Todos los titulares de un dato biométrico requieren un nombre distintivo como se menciona en el estándar X.500, el cual es registrado por la PSC de Acepta; del mismo modo se registrará el RUN o RUT.

Se considerará como válido, en el caso de los nombres, cualquiera que sea aceptado por el Servicio de Registro Civil e Identificación o en el Registro de personas Jurídicas.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

3.1.2 Verificación General

Acepta, como parte del proceso de enrolamiento biométrico, procederá a verificar la identidad de la persona a la cual se asociará el dato biométrico. Para esto el titular se presentará ante un operador de la unidad de registro, o a quien Acepta determine para ejecutar esta función (Servicio de Registro Civil e Identificación o Notarios), quien estará encargado de verificar la identidad de este versus la cédula de identidad presentada.

Respecto a la dirección de correo electrónico del titular, Acepta informa que no garantiza que esta dirección de correo esté vinculada con el titular del dato biométrico, por lo que la confianza en que esta dirección recae sólo en la parte confiante. Acepta, garantiza que la dirección electrónica de correo asociada al titular del dato biométrico, ha sido aportada por el titular al momento de su enrolamiento.

El proceso de enrolamiento de un dato biométrico para un titular sigue la siguiente secuencia:

- ✓ Al presentarse un cliente a efectuar una transacción que requiera verificación de identidad biométrica, se pueden presentar dos situaciones:
  - ➢ Las huellas del cliente ya se encuentra registradas en el sistema biométrico y la verificación de identidad es efectuada comparando automáticamente la impresión capturada en vivo v/s la almacenada en el sistema Biométrico.
  - ➢ Las huellas del cliente no se encuentran registradas en el sistema Biométrico (para un RUN digitado en el sistema, se levantará una aplicación de enrolamiento); por tanto es requisito esencial su verificación de identidad manual y posteriormente su enrolamiento, el cual se detalla a continuación:
    - ✓ El ministro de fe de la unidad de registro, que ha recibido el privilegio de enrolamiento dentro de la institución, solicitará al cliente presentar su documento de identificación (Cédula de identidad en el caso de Chilenos y extranjeros residentes). El agente procederá a comparar la fotografía y datos civiles del cliente, presentes en el documento entregado, respecto a la persona que porta dicho documento. En caso de ser exitosa la verificación de identidad manual, se procederá a:

- ❖ Digitar, por parte del agente, dentro de la pantalla de enrolamiento (activada en este momento):
    - Nombre del cliente
    - Fecha de Nacimiento
    - Sexo
- ❖ Capturar 4 impresiones dactilares en vivo. El sistema Biométrico, pasará de una captura a otra, una vez que haya logrado una imagen con la calidad adecuada para la extracción de su patrón. Lo anterior es señalado con un signo de aprobación de la última captura válida.

  Las cuatro impresiones capturadas, generarán el patrón, contra el cual se realizarán las verificaciones de identidad futuras.

- Es importante señalar que el proceso completo de enrolamiento, toma un tiempo de 30 a 45 segundos de atención por cada cliente.

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

3.2 Re-enrolamiento

Por motivo de seguridad, es que Acepta no procede a realizar la re enrolamientos automáticos de datos biométricos de un titular, una vez que dicho dato biométrico existe. Sin embargo, Acepta permite solicitudes de re enrolamiento bajo ciertas circunstancias, clasificando ellas en:

- Rutinarias: Producto del término de cambios significativos en las características de dato biométrico en vivo, el cual hace no posible una comparación AFIS 1 a 1
- Producto de una revocación: En caso que Acepta detecte un dato biométrico mal asociado a un titular podrá revocar su asociación de mutuo propio o a solicitud del titular, procediendo si es pertinente a registrar el nuevo dato biométrico que reemplaza al revocado

Para un mayor detalle, remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

3.3 Verificación de identidad a partir de un dato biométrico revocado

No es posible esta operación, lo anterior de acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

3.4 Requerimiento de Revocación

El proceso de solicitud de revocación de un dato biométrico viene definido por la Política de Certificación Biométrica: La política de identificación para las solicitudes de revocación acepta los siguientes métodos de identificación:

- Por oficio de Acepta ante sospecha fundada de compromiso en el dato biométrico del Titular.
- Presencial con una identificación similar a la primera solicitud de enrolamiento (ver 3.1.2).
- Por medio electrónico, en que el titular debe enviar a Acepta un e-mail firmado con firma electrónica avanzada, siendo la casilla de destino admin-revocaciones@acepta.com, indicando explícitamente el dato biométrico a ser revocado desde la PSC de Acepta
- Por carta certificada, en caso de revocar su dato biométrico, adjuntando además fotocopia de su carnet de identidad.

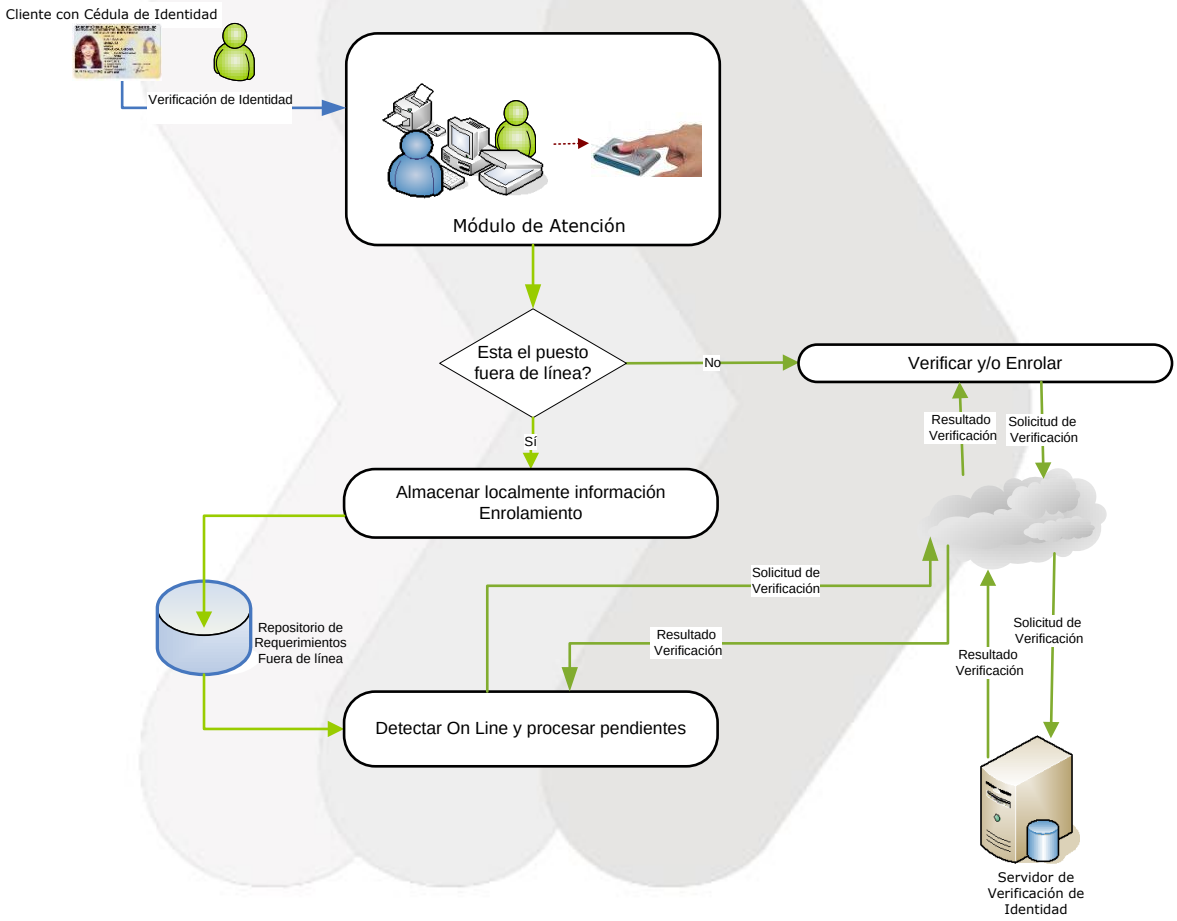
4 Requisitos Operacionales

Las especificaciones de este capítulo son complementadas en el documento de declaración de prácticas de certificación

4.1 Manuales Operacionales

Para cumplir las labores de enrolamiento y verificación de un dato biométrico asociado a un titular, Acepta cuenta con manuales operacionales los cuales guían a los operadores de la unidad de registro en las labores asociadas a su rol. En estos documentos se describen los requisitos operativos pertinentes a las etapas de enrolamiento de un titular. Además, se describe el mecanismo de revocación de dichos datos biométricos.

El siguiente diagrama muestra el proceso de enrolamiento y verificación:



4.2.1 Solicitud de enrolamiento

La solución aquí presentada permite registrar en la Base de Datos la información básica de una persona (nombre, sexo, fecha de nacimiento, etc), así como la de cualquiera de sus dedos (incluso todos si así se desea).

El proceso de ingreso de esta información (denominado enrolamiento) requiere que el sensor de huellas capture cuatro imágenes por cada dedo a enrolar. Una vez obtenidas, el software genera un objeto (denominado patrón) que resume la información de las imágenes. A su vez, selecciona la mejor de las cuatro para generar una imagen comprimida con formato WSQ, estándar definido por el FBI y adoptado por el Servicio de Registro Civil e Identificación chileno (SRCeI).

Ambos objetos son almacenados en la Base de Datos (el patrón en forma encriptado) asociados a la Institución que está efectuando el ingreso (el Enrolador).

Todo el proceso de enrolamiento es automatizado por el sistema biométrico y es definido por una transacción. Una aplicación sólo necesita invocar el servicio, adjuntando algunos parámetros opcionales, tales como la cantidad de dedos a enrolar, o los datos básicos de la persona si ya los ha obtenido previamente. Dentro de esta misma transacción se podrá definir que previo a efectuar el enrolamiento de la impresión dactilar y datos de un nuevo titular, su impresión dactilar pueda ser verificada contra su cédula de identidad, o contra la base de datos actual del sistema biométrico de Acepta.

La transacción de enrolamiento ocurrirá al presentarse un titular a efectuar una transacción que requiera verificación de identidad biométrica y en donde la huellas de dicho titular no se encuentran registradas en el sistema biométricos de Acepta (para un RUN digitado en el sistema, se levantará una aplicación de enrolamiento); por tanto es requisito esencial su verificación de identidad manual o automática contra la cédula de identidad por parte de la unidad de registro y posteriormente su enrolamiento, el cual se detalla a continuación.

El ministro de fe de la unidad de registro, que ha recibido el privilegio de enrolamiento dentro de la institución, solicitará al cliente presentar su documento de identificación. El agente procederá, independiente de tratarse de una cédula de identidad de formato antiguo, a comparar la fotografía y datos civiles del cliente, presentes en el documento entregado, respecto a la persona que porta dicho documento.

De ser exitosa la verificación de identidad por cualquiera de los mecanismos antes descritos, se procederá a:

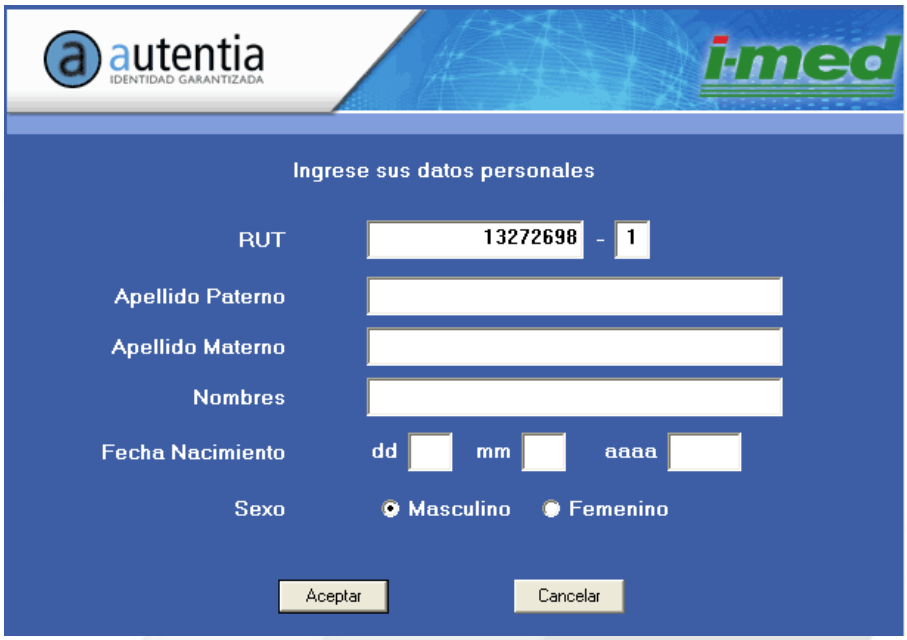
- Completar, por parte del agente, dentro de la pantalla de enrolamiento (activada en este momento):
  - Nombre del titular
  - Fecha de Nacimiento
  - Sexo
  - N° de serie del documento o fecha de vencimiento (de tratarse de un documento de formato antiguo).
  - Mail si corresponde
- Capturar 4 impresiones dactilares en vivo. El sistema biométrico, pasará de una captura a otra, una vez que haya logrado una imagen con la calidad adecuada para la extracción de su patrón. Lo anterior es señalado con un signo de aprobación de la última captura válida.

  Las cuatro impresiones capturadas, generarán el patrón, contra el cual se realizarán las verificaciones de identidad futuras.

Es importante señalar que la plataforma biométrica tiene la capacidad de almacenar todos los datos que sean necesarios, por lo cual, además de los datos ya mencionados, se pueden capturar datos como dirección, número de cliente, banco, etc. Además, el proceso completo de enrolamiento, toma un tiempo de 30 a 45 segundos de atención por cada titular.

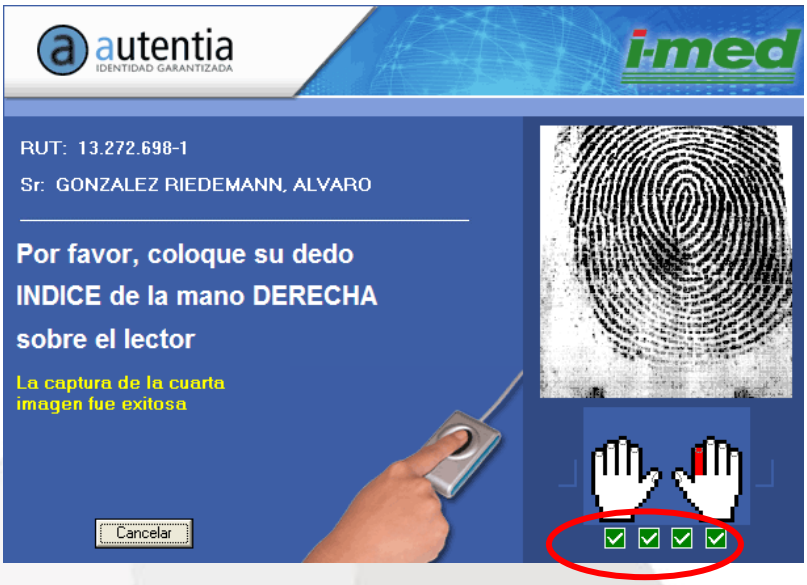
Las siguientes pantallas muestran las etapas del proceso de enrolamiento efectuada por la aplicación biométrica:

- Al titular que no haya sido registrada previamente en la base de datos, se le solicitará **LA CEDULA DE IDENTIDAD DE LA PERSONA** para luego registrarla en el sistema:
  - Los datos personales a completar, serán al menos los siguientes:



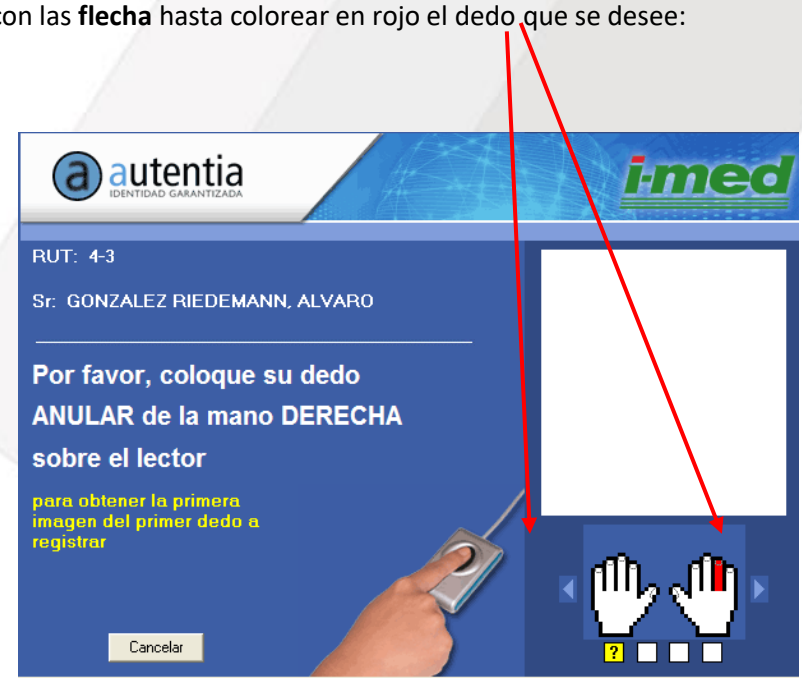
Y también el Nº de serie del documento o fecha de vencimiento (de tratarse de un documento de formato antiguo).

  - A continuación, el titular tendrá que colocar correctamente cuatro veces la huella digital sobre el lector (se indica en la parte inferior de la pantalla si la huella está siendo colocada correctamente. El dedo a enrolar puede ser seleccionado por el operador de la aplicación.



- Si el enrolamiento fue exitoso este será aprobado, de lo contrario será rechazado lo cual puede deberse a las siguientes causas:
  - Que la huella este muy gastada (personas mayores)
  - Que el lector esté sucio o presente problemas.

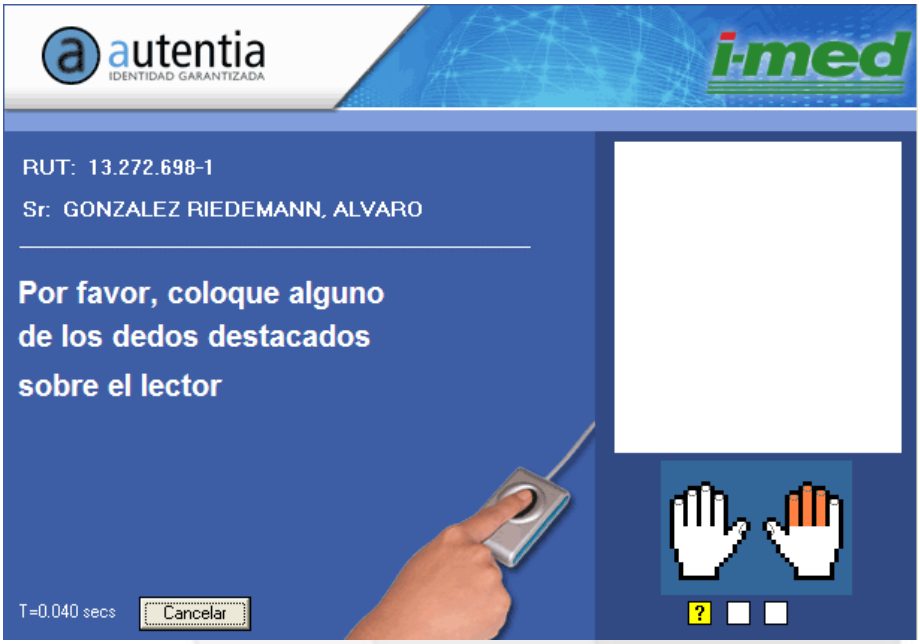
  La solución en este caso es intentar enrolar algún otro dedo, para ello es necesario especificar el dedo que se utilizará en el enrolamiento. Para especificar el dedo a enrolar basta con moverse con las **flecha** hasta colorear en rojo el dedo que se desee:



Es importante hacer notar que todas las transacciones que se realicen quedarán asociadas a la persona a cargo del computador (operador de la unidad de registro) por lo que cualquier suplantación será identificada.

4.2.2 Verificación de identidad

El sistema biométrico de Acepta ofrece la modalidad de verificación. En esta modalidad, se usa el RUN (Nº nacional de la Cédula de identidad) de la persona para obtener de la Base de Datos su información básica y los patrones de los dedos ya enrolados. Estos se muestran por pantalla coloreados, y la persona puede usar cualquiera de ellos para verificarse.



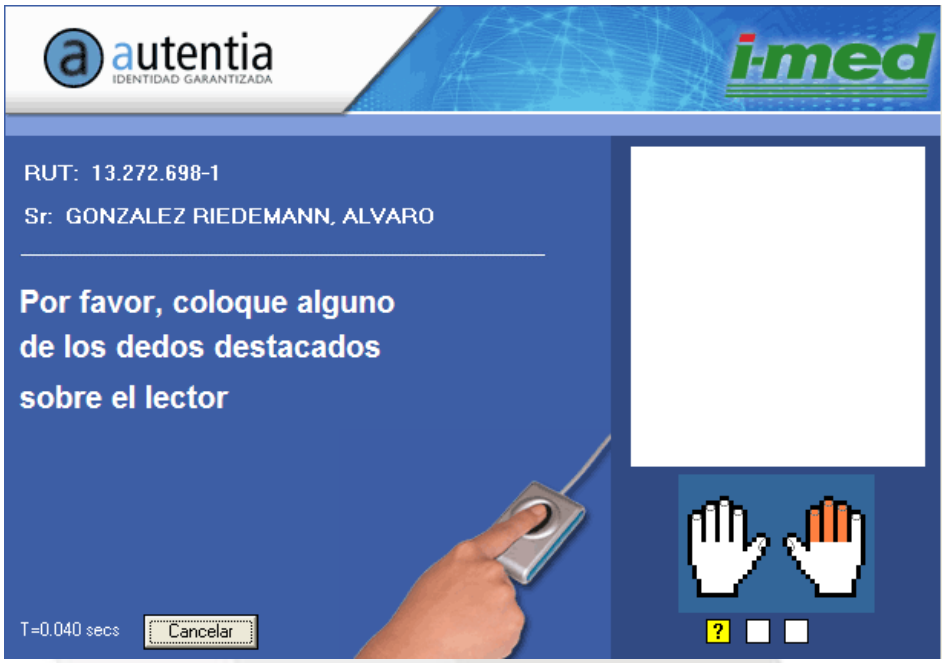
Graduación de la Verificación

Igual que en el caso del enrolamiento, el proceso es automatizado por parte del sistema biométrico, pero la aplicación puede sintonizar diversos aspectos:

- El más importante se refiere al nivel de exigencia que se desea en la calidad de la verificación. Cuando la persona pone un dedo en el sensor, éste captura una imagen de la cual extrae un conjunto de minucias que serán comparadas con las de un patrón candidato. El resultado de la comparación se traducirá en un "puntaje" de correspondencia. La aplicación puede especificar el mínimo exigido, el que, por ejemplo, puede relajar para algunos casos problemáticos (por ejemplo, niños o ancianos) y para ciertas transacciones que no representen gran riesgo (solicitud de certificados, consultas, etc.).
- Por otra parte, la aplicación puede restringir la verificación a los patrones registrados sólo por determinado(s) enrolador(es) o instituciones.
- Finalmente, la aplicación de biometría de Acepta, puede definir transacciones especiales (cursos de acción programable) frente a falsos rechazos -propios de cualquier sistema biométrico- o frente a intentos de suplantación que se presenten en el día a día.

Las siguientes pantallas muestran las etapas del proceso de verificación efectuada por la aplicación biométrica de Acepta:

- Si la persona ya es un titular enrolado en el sistema de verificación biométrica de identidad, se levantará la pantalla indicada, siendo sólo necesario que se coloque la impresión dactilar viva sobre el lector. Después de colocar el dedo sobre el lector podrán ocurrir dos situaciones:



Que la verificación sea aceptada.

- Que la verificación sea rechazada. En este caso se dispondrá de dos oportunidades más (número de intentos configurable) para intentar realizar la verificación de identidad en forma exitosa. Las causas de rechazo de una verificación de identidad corresponden a:
    - Huella poco legible (generalmente ancianos y niños menores de 6 años)
    - Que la huella no corresponda a la registrada (intento de fraude)
    - Que el lector de huella esté sucio o presente problemas.
    - Problemas de calidad en la nueva imagen que se captura en vivo.

Aún cuando los algoritmos (programas) computacionales que efectúan la comparación, son extremadamente seguros y confiables, hay un porcentaje menor de la población para los cuales no es posible efectuar una verificación automática de la identidad (usando el computador). Los casos normalmente son:

- **Persona con piel muy seca**: Como primera medida se recomienda que se humedezcan un poco el dedo antes de colocarlo en el escáner. Normalmente esto es suficiente para superar el problema.
- **Personas con heridas en los dedos**: Si tienen más de un dedo registrado en el sistema, probar con el que este en mejor condición, sino intentar que el dedo cubra la mayor superficie del área de lectura del escáner.
- **Niños menores de 6 años**: Para niños menores de 6 años normalmente se presentan problemas para capturar su huella, ya que ellas están poco marcadas.

De la buena calidad de la captura (enrolamiento) dependerá lo fácil que resulte a futuro efectuar una verificación de identidad exitosa y rápida. Cómo criterios generales a considerar se debe:

- Colocar el dedo sobre el lector cubriendo la mayor área posible. Por ejemplo:

- Si el dedo no permite obtener una buena imagen, humedecer este. Con esto se logra mejoras sustanciales en la captura.

Es importante recalcar que en todo sistema biométrico existe la probabilidad de presentarse Falsos Rechazos con la nueva captura en vivo de la impresión del cliente (por ejemplo ante daños que ha tenido la persona en su dedo posterior a la fecha de enrolamiento).

4.2.3 Algoritmo de reconocimiento de impresión dactilar

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

4.3 Revocación del dato biométrico

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

4.4 Renovación de datos biométricos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5 Controles de Personas, Físicos y de Procedimientos

5.1 General

En este capítulo se describen los controles físicos, de procedimientos y de personal que utiliza la PSC de Acepta en los procesos de identificación, emisión, revocación, auditoría y almacenamiento de sus certificados, marcas de tiempo o datos biométricos.

5.2 Data Center

Los sistemas e infraestructura del Servicio de Emisión de Certificados, se encuentra alojado en un Sitio Principal y uno secundario. Las características generales del recinto Principal comprenden una Zonificación en Alta Criticidad (Sitio de Producción) y una Zona de Media Criticidad (recintos de Operaciones y Cintoteca). Estos sitios poseen una infraestructura diseñada para garantizar la seguridad de los equipamientos.

- Zona Alta Criticidad: Sitio de Producción:
  - El espacio físico blindado en su perímetro desprotegido de muros estructurales del edificio.
  - Sistema de esclusas mediante puerta corta fuego y blindada opaca y vidriada blindada.
  - Acceso restringido.
  - Sistema de video vigilancia.
  - Piso falso de 30cm de altura con cámara plena para distribución de aire para climatización de todos los equipos de la sala.
  - Acceso por rutas físicas redundantes para fibras ópticas carriers.
  - Equipos de Climatización precisa redundantes en configuración 1+1.
  - Equipos de energía ininterrumpida UPS redundantes en configuración 1+1 . La iluminación de la sala se encuentra respaldada por el sistema UPS y el grupo electrógeno.
  - Sistema autónomo de detección y extinción de incendios en base a gas FM-200.
  - Soporte generación autónoma de energía de emergencia mediante Grupo Electrógeno de operación continua. Todos los equipos están respaldados.

- Zona Criticidad Media: Operaciones:
  - Espacio cerrado de oficinas dotado de puestos de trabajo para personal operación y administración.
  - Acceso restringido mediante tarjeta magnética u botonera con clave.
  - Sistema de Video Vigilancia.
  - Iluminación y puestos de trabajo respaldados por el grupo electrógeno.

- Zona Criticidad Media: Cintoteca:
  - El espacio físico blindado en su perímetro desprotegido de muros estructurales del edificio, alejado del Sitio de Producción.
  - Puerta de acceso corta fuego y de seguridad.
  - Acceso restringido mediante cerradura de seguridad.
  - Sistema autónomo de detección y extinción de incendios en base a gas FM-200.
  - Iluminación respaldada con grupo electrógeno.

Respecto al sitio secundario, sus principales características son:

- Acceso restringido y controlado.
- Climatización full redundante calculada de acuerdo a la carga térmica de la sala.
- Alimentación del sistema eléctrico independiente de otros consumos propios del lugar en que se encuentra ubicado el sitio secundario.
- Sistema de respaldados con UPS redundante y grupo electrógeno.
- Sistema de detección temprana de incendio y extinción vía agente limpio FM-200.
- Sistema de detección de sobre temperatura para monitorear permanentemente el funcionamiento del sistema de Aire Acondicionado.
- Sistema de detección de intrusos.
- Acceso por rutas físicas redundantes para fibras ópticas carriers.
- Acceso a través de una puerta cortafuego de características para resistencia al fuego F-60.
- Sistemas de Circuito Cerrado de Televisión.

Los controles definidos en ambos sitios, para proteger los elementos que forman parte de la solución de Acepta, se basan en procedimientos y estándares de seguridad física para las instalaciones informáticas. Estos a su vez se encuentran elaborados según la norma ISO 27001, para la cual ambos sitios se encuentran certificados.

5.2.1 Seguridad Física Data Center

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.2.2 Sistema de Energía Eléctrica

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.2.3 Sistema de Control Ambiental

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.2.4 Sistema de Extinción y Control de Incendios

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.2.5 Telecomunicaciones

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.2.6 Seguridad Lógica Data Center

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.3 Controles de procedimientos

Los sistemas de información y los servicios de Acepta se operan de forma segura, siguiendo procedimientos preestablecidos.

Para un mayor detalle remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.3.1 Papeles de confianza

Los roles definidos para el control y gestión del sistema son:

- Administrador de Sistemas
- Administrador de Seguridad
- Operador de Unidad de Registro
- Responsable de formación, soporte y comunicación
- Responsable de Seguridad
- Auditor
- Responsable de Documentación

Para un mayor detalle remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.4 Controles de seguridad del personal

5.4.1 Requerimientos de antecedentes y experiencia

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.4.2 Comprobación de antecedentes

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.4.3 Requerimientos de formación y reentrenamiento

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.4.4 Frecuencia de rotación de tareas

No es aplicable para Acepta, ya que las personas mantienen su cargo.

5.4.5 Sanciones

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.4.6 Requerimientos de contratación

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.4.7 Documentación entregada al personal

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.4.8 Control de cumplimiento

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.4.9 Finalización de contratos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.5 Procedimientos de auditoría de seguridad

5.5.1 Tipos de eventos registrados

Los tipos de eventos registrados dependen de las políticas biométricas. En particular se registra:

- Intentos exitosos o fracasados de cambiar los parámetros de seguridad del sistema operativo.
  - Inicio y detención de la plataforma.
  - Intentos exitosos o fracasados de inicio y fin de sesión de administradores.
  - Intentos exitosos o fracasados de crear, modificar o borrar cuentas del sistema.
  - Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
  - Intentos exitosos o fracasados de solicitar, generar, firmar, emitir o revocar datos biométricos
  - Intentos exitosos o fracasados de crear, modificar o borrar información de los titulares de datos biométricos.
  - Intentos exitosos o fracasados de acceso a los sitios principal y secundario por parte de personal autorizado o no.
  - Backup, archivo y restauración.
  - Cambios en la configuración del sistema.
  - Actualizaciones de software y hardware.
  - Mantenimiento del sistema.

5.5.2 Frecuencia de procesamiento del log

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.5.3 Periodo de Retención para el log de auditoría

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.5.4 Protección del log de auditoría

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.5.5 Procedimientos de respaldo del log de auditoría

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.5.6 Evaluaciones de vulnerabilidad

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.6 Políticas para archivo de registros

5.6.1 Documentos archivados

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

- Los registros de auditoría especificados en el punto 5.5 de esta Declaración de Prácticas de Certificación Biométrica.

- Los soportes de backup de los servidores que componen la infraestructura de la AC de Acepta.
- Documentación relativa al ciclo de vida de los certificados
- Acuerdos de confidencialidad
- Contratos suscritos por la Acepta en su función de PSC
- Autorizaciones de acceso a los Sistemas de Información

5.6.2 Requerimientos para "time-stamping" de registros

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.6.3 Sistema de colección de archivos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.6.4 Procedimientos para obtener y verificar información de archivos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.7. Cambio de datos biométricos

Se considera la posibilidad de cambio los datos biométricos del usuario, debiendo para ello generarse un nuevo registro biométrico del mismo.

Para un mayor detalle remítase a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.8 Recuperación en caso de compromiso de los datos biométricos o de desastre

5.8.1 Alteración de los recursos hardware, software y/o datos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.8.4 Instalación de seguridad después de un desastre natural u otro tipo de desastre

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

5.9 Cese de una PSC

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

6 Controles de Seguridad Técnica

6.1 General

En este punto Acepta describe las medidas de seguridad que ha tomado para proteger tanto los datos biométricos enrolados, así como los resultados de las verificaciones de identidad realizadas; a fin de que dicha información sea sólo accesible a las personas autorizadas. También se describe los aspectos técnicos relacionados con la identificación de los usuarios, el registro de los datos biométricos, su revocación, auditoria y almacenamiento.

6.2 Ciclo de vida del dato biométrico

6.2.1 Enrolamiento

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

6.2.2 Verificación de identidad

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

6.2.3 Formato del patrón de huella

De acuerdo a ISO/IEC 19794-3.

6.2.4 Comprobación de la calidad de las impresiones dactilares

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

6.2.5 Fines del uso del dato biométrico

Todo dato biométrico puede ser revocado en uso ya sea por solicitud de su titular, por detectar Acepta una posible suplantación, o simplemente por una renovación de la captura biométrica

6.3 Protección del dato biométrico

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

6.4 Controles de seguridad informática

Actualmente, Acepta cuenta con un plan de seguridad de la información, el cual contempla distintos controles de seguridad, desde un plan de recuperación de desastres hasta los respectivos controles de acceso. Mayor detalle de estos controles son parte del Plan de Seguridad de Acepta.

6.5 Controles técnicos del ciclo de vida

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

6.6 Controles de seguridad de red

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

6.7 Controles de seguridad de los módulos criptográficos y biométricos

De acuerdo a lo especificado en la Declaración de Prácticas de Certificación Biométrica de Acepta.

7 Administración de las CPB

Este capítulo establece los procedimientos aplicables respecto a las modificaciones del presente documento.

7.1 Procedimientos para Modificar las CPB

Las políticas de certificación contenidas en este documento, son administradas y mantenidas rigurosamente por personal especializado y en posiciones de confianza en la compañía.

7.2 Publicación y notificación

Cualquier cambio en el contenido de estas políticas será comunicado al público y usuarios mediante su publicación en el sitio Web de Acepta en https://sovos.com/es/politicas-y-practicas/ .

7.3 Procedimientos de aprobación de las CPB

Estas CPB y las subsecuentes versiones futuras de éste documento están sujetas a la aprobación del Comité de seguridad de Acepta.