ACEPTA

Empresas
a velocidad
digital

PO02

Declaración de Prácticas 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
Declaración de Practicas de Biometría - PO02	1.0	Primera versión	23-2-2016
Declaración de Practicas de Biometría - PO02	4.0	Revisión anual	01-10-2016
Declaración de Practicas de Biometría - PO02	5.0	Revisión anual	01-10-2017
Declaración de Practicas de Biometría - PO02	6.0	Revisión anual	01-10-2018
Declaración de Practicas de Biometría - PO02	7.0	Revisión anual	01-10-2019
Declaración de Practicas de Biometría - PO02	8.0	Revisión anual	01-10-2020
Declaración de Practicas de Biometría - PO02	9.0	Revisión anual	15-03-2022
Declaración de Practicas de Biometría - PO02	10.0	Revisión anual	15-03-2023

Declaración de Practicas de Biometría - PO02	10.1	Ajuste punto 1.5	03-07-2023
Declaración de Practicas de Biometría - PO02	10.2	Corrección a punto 5.2 producto de IAO 2023	03-10-2023
Declaración de Practicas de Biometría - PO02	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

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 las Prácticas de Certificación de Biometría de Acepta (CPSB); 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 estas prácticas. Se describe además los papeles, responsabilidades y relaciones entre el usuario final y Acepta, siendo este documento un complemento a la Política de Biometría de Acepta. Estas prácticas son una descripción detallada de los procedimientos que Acepta declara convenir en la prestación de sus servicios de certificación biométrica, cuando enrola, verifica y hace uso de datos biométricos de un titular, en su rol de Prestador de Servicios de Certificación (PSC).

Las Prácticas de Certificación de Biometría de Acepta 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. También se describen aquí las medidas de seguridad técnica y organizativa, los perfiles y los mecanismos de información que permiten verificar y administrar la información biométrica capturada, así como el asegurar que el proceso de enrolamiento, verificación y uso de los datos biométricos es llevado a cabo en un ambiente seguro y que puede dar total confianza a los usuarios de la calidad de los servicios biométricos proporcionados por Acepta.

Cabe indicar que la presente Declaración de Prácticas 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 prácticas son las que se prosigue en detallar, y están disponibles en el Sitio WEB de Acepta para conocimiento público.

Esta Declaración de Prácticas 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 Prácticas de Biometría

Las prácticas 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 prácticas que dan seguridad y confianza a los servicios biométricos provistos por Acepta.

1.1.2 Alcance

El alcance de la Declaración de Prácticas 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 Prácticas 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 "Prácticas de Certificación de Biometría de Acepta", las que internamente se citan como CPSB y están registradas con el número único internacional (OID) 1.3.6.1.4.1.6891.301.

Acepta tiene el identificador (OID) 1.3.6.1.4.1.6891 el cual está registrado en la Internet Assigned Number Authority (IANA). Este número identifica únicamente a Acepta en un contexto global.

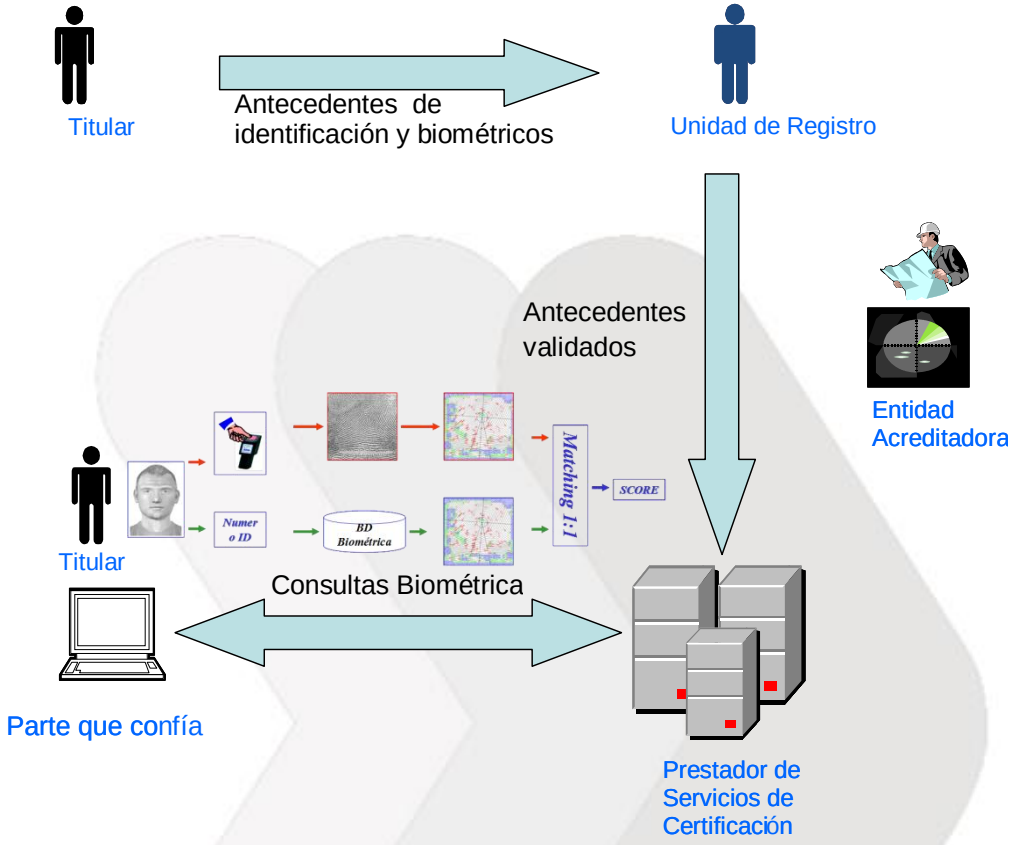
Este documento se encuentra disponible, en forma pública, en https://sovos.com/es/politicas-y-practicas/.

Las prácticas de biometría de las PSC de Acepta y de cada política de la PSC, están registradas con un número único internacional, llamado Object Identifier (OID). La siguiente tabla resume todos los OID administrados por Acepta:

Descripción	OID
Prácticas de Certificación	1.3.6.1.4.1.6891.1
Políticas de certificados Clase 3	1.3.6.1.4.1.6891.2
Políticas de certificados de Firma Electrónica Avanzada	1.3.6.1.4.1.6891.3
Políticas de certificados de Sitio Web	1.3.6.1.4.1.6891.4
Extensión para indicar declaraciones del titular de un certificado X.509	1.3.6.1.4.1.6891.9
Extensión para certificados X.509 en la que se incluye el XML de un CAF.	1.3.6.1.4.1.6891.50.1
Identificador permanente administrado por Acepta para nombrar Servidores.	1.3.6.1.4.1.6891.100.1
Identificador permanente administrado por Acepta para nombrar Servicios.	1.3.6.1.4.1.6891.100.2
Políticas de Timestamp	1.3.6.1.4.1.6891.200
Prácticas de Timestamp	1.3.6.1.4.1.6891.201
Políticas de Biometría	1.3.6.1.4.1.6891.300
Prácticas de Biometría	1.3.6.1.4.1.6891.301

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 por 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 Prácticas de Biometría, en las correspondientes Políticas de 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 por 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.

A continuación se muestra un resumen de los tipos de datos biométricos gestionados por Acepta:

Tipo	Características generales	Usos típicos
Impresión dactilar Persona Natural sin verificación 3era parte	• Registro presencial. • Verificación manual de los datos capturados v/s los contenidos en la cédula de identidad	• Verificación de identidad en rubros tales como: ○ Salud ○ Comercio
Impresión dactilar Persona Natural con verificación 3era parte	• Registro presencial. • Verificación automática de los datos capturados v/s los contenidos en la cédula de identidad • Verificación de estado de cédula	• Verificación de identidad en rubros tales como: ○ Salud ○ Comercio • Firma electrónica de documentos privados

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

Actualmente los datos biométricos capturados por la PSC de Acepta corresponden a impresiones dactilares planas, siguiendo ellas los siguientes formatos:

- Intercambio de información biométrica: Comunicación http con el contenido encriptado con AES con llave simétrica
- Formato de Minucias: La mayoría de nuestras minucias se encuentra en el formato propietario de Digital Persona platinum y onetouch, además la plataforma soporta otros formatos como el ansi 378

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 Prácticas 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 opere 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 en su punto 3.1.2, en lo que refiere a la actividad de enrolamiento. En particular, deberán efectuar con la máxima prolijidad el proceso de enrolamiento de un dato biométrico y la asociación del mismo al RUN del titular. Para ellos verificarán manual o automáticamente la relación entre el documento nacional de identidad presentado por el titular respecto al portador del mismo, de manera de asegurar que la persona portadora de dicho documento es quien dice ser.

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.

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 (ver 1.4.1).

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.

2.1.9 Obligaciones de los Repositorios

Acepta mantendrá un repositorio, el cuál permita almacenar los datos biométricos, producto de un enrolamiento, o los resultados asociados a una verificación de identidad biométrica. Adicionalmente este repositorio mantendrá la identificación (RUN) de los titulares enrolados, así como la lista de aquellos datos biométricos que han sido revocados, ya sea por decisión del titular y/o por el haber detectado un dato biométrico incorrectamente asociado a un titular. La información contendida en este

repositorio se mantiene encriptado, pudiendo adicionalmente firmarse los datos en ella almacenados a través de una firma electrónica de la PSC.

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 o resultado biométricos 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.

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 CPSB 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

Acepta queda exenta de responsabilidad en caso de pérdida o perjuicio, en los servicios que presta, producto de:

- Guerra, desastres naturales o cualquier otro caso de fuerza mayor.

Los cuales le hagan imposible proveer los servicios biométricos aquí descritos.

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.

Cualquier diferencia, dificultad, problema o controversia que pueda surgir entre Acepta y los titulares o con los terceros interesados que adhieran a las CPSB de Acepta con motivo de la validez, eficacia, interpretación, nulidad, cumplimiento o incumplimiento de estas CPSB o de la actividad de certificación biométrica será resuelta definitivamente por un árbitro mixto, quien tramitará como árbitro arbitrador pero que fallará conforme a derecho. El fallo del árbitro será en única y definitiva instancia, sin que en contra de sus resoluciones y fallo, ya sean de substanciación o de medidas precautorias o bien el fallo definitivo, proceda ningún recurso. El arbitraje se llevará a cabo en la ciudad de Santiago. El árbitro estará solamente obligado a constituir legalmente el arbitraje, a oír a las Partes en conjunto o separadamente, según él lo decida, a recibir las pruebas que se presenten y a dictar su sentencia oportunamente. Las resoluciones se notificarán por carta certificada dirigidas a las Partes o a sus representantes designados en esta escritura o en el respectivo proceso, a las direcciones que ellos señalen en tales instrumentos, salvo la primera notificación del proceso y la de la sentencia definitiva que deberán notificarse en conformidad a las reglas establecidas para dichas resoluciones en el Título Sexto, del Libro Primero, del Código de Procedimiento Civil. El árbitro designado podrá actuar cuantas veces fuere requerido, por asuntos diferentes, promovidos por cualquiera de las Partes, y en caso de ausencia o impedimento acreditada a juicio del sustituto, éste podrá intervenir de inmediato, en carácter de subrogante, en el estado en que el asunto se encuentre, sin otro requisito que aceptar el cargo. El respectivo proceso podrá continuarse incluso en una copia autorizada de los autos que cualquiera de las Partes presentare ante el sustituto. La evidencia de haberse ausentado del país el árbitro en ejercicio por más de treinta días sin haber regresado, o de impedimento de otra naturaleza acreditado ante el sustituto por medios idóneos y que dure más de treinta días será considerado como ausencia del árbitro.

El árbitro deberá ser designado de común acuerdo por las Partes, dentro del plazo máximo de 15 días hábiles. A falta de acuerdo respecto de la persona que actuará en el cargo, el árbitro deberá tener el carácter de mixto y su designación será efectuada, a solicitud escrita de cualquiera de las Partes por la Justicia Ordinaria, debiendo recaer la designación en una persona que haya sido Ministro o Abogado

Integrante de la Excelentísima Corte Suprema de Justicia, o bien, Profesor de las cátedras de Derecho Civil o Comercial de las Facultades de Derecho de las Universidades de Chile, Católica de Santiago o Católica de Valparaíso, excluidos quienes hubieren asesorado o prestado servicios a cualquier título a alguna de las partes en el bienio inmediatamente anterior.

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.

Acepta y sus PSC acreditadas se obligan a mantener dicha información disponible para su acceso público, así como publicar la información consistentemente con las prácticas de confidencialidad estipuladas en este documento, así como de las leyes vigentes.

La disponibilidad de los servicios señalados no podrá ser inferior a un 99,5 % al año, excluyendo de este compromiso, los tiempos de mantención programados o casos de Fuerza mayor indicados en 2.2.2.

La información utilizada para la verificación biométrica se mantiene permanentemente actualizada.

El registro de acceso público de biometría funciona bajo las siguientes normas:

a. La información relativa referente al RUN de los datos biométricos es publicada, a través de sistemas automatizados, en el mismo momento en que éstos son capturados.
b. La información relativa a la revocación de los datos biométricos es publicada dentro de un plazo que no puede exceder de 6 horas laborales (entre 9:00 y 18:00 horas), contada desde la solicitud de revocación realizada de conformidad con el procedimiento indicado en 4.3 de estas CPSB.

2.5 Privacidad y Protección de los Datos

Las Políticas de Privacidad de Acepta se encuentran publicadas en el sitio web de Acepta https://sovos.com/es/politicas-y-practicas/.

2.5.1 Tipos de Información a Proteger

De manera complementaria a lo dispuesto en las Políticas de Privacidad de Acepta, la empresa protege especialmente la siguiente información:

- Información propia de la operación de Acepta y de sus llaves
  - Las claves privadas de las entidades que componen a Acepta.
  - Toda información relativa a las operaciones que lleve a cabo Acepta.
  - Toda información relativa a los controles de seguridad y procedimientos de auditoría.
  - Planes de continuidad de negocio y de emergencia.
  - Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
  - Toda la información clasificada como “CONFIDENCIAL”.
- Información propia del suscriptor capturada durante el registro

- Toda la información de carácter personal proporcionada a Acepta durante el proceso de registro de los suscriptores de certificados o de enrolamiento y verificación biométrica

2.5.2 Tipos de Información que Puede ser Entregada

Acepta considera como información de acceso público y, consecuentemente se encuentra disponible al público en https://sovos.com/es/politicas-y-practicas/ o en las oficinas de la empresa:

- La Declaración de Prácticas de Certificación de Acepta.
- Toda aquella información que y no teniendo un estatuto de protección especial establecido en la ley sea por Acepta clasificada como "PÚBLICA".
- La contenida en los certificados de firma electrónica avanzada, en cumplimiento de lo dispuesto en la Ley 19.799 (Chile).
- La contenida en el registro de acceso público de certificados de firma electrónica avanzada, en cumplimiento de lo dispuesto en la Ley 19.799.

Y en https://asistencia.acepta.com/firma-avanzada.html se encuentra:

- La lista de certificados revocados (CRL).

Pese a la calificación de la información como de acceso público, Acepta se reserva el derecho de imponer medidas y controles de seguridad adecuados y proporcionales con el fin de asegurar la autenticidad e integridad de los documentos, así como de imponer medidas tecnológicas anti copia y de impresión para aquellos que se encuentren soportados electrónicamente.

2.5.3 Información del dato biométrico

Los datos biométricos capturados por Acepta (en este momento la impresión dactilar plana) están en conformidad con lo siguiente.

- Intercambio de información biométrica: Comunicación http con el contenido encriptado con AES con llave simétrica
- Formato de Minucias: La mayoría de nuestras minucias se encuentra en el formato propietario de Digital Persona platinum y onetouch, además la plataforma soporta otros formatos como el ansi 378

2.5.4 Entrega de Información sobre la Revocación de un dato biométrico

La información relativa a la revocación de los datos biométricos es publicada dentro de un plazo que no puede exceder de 6 horas laborales (entre 9:00 y 18:00 horas), contada desde la solicitud de revocación realizada de conformidad con el procedimiento indicado en 4.3 de estas CPSB.

2.5.5 Entrega de Información en virtud de un Procedimiento Judicial

Acepta sólo podrá comunicar informaciones calificadas como confidenciales o que contengan datos de carácter personal en aquellos casos en los que así se le requiera por la autoridad pública competente y bajo los procedimientos que se han previstos legalmente por el Poder Judicial de la República de Chile o de sus tribunales competentes.

Las obligaciones, prohibiciones y responsabilidades de custodia de información sujeta a secreto, reserva o confidencialidad de acuerdo con la ley y estas CPSB no regirán si media alguna disposición legal o resolución judicial que obligue a entregar al conocimiento de los Tribunales de Justicia, organismos, instituciones o entidades facultadas por la ley para solicitarlos y que actúen dentro del ámbito de sus atribuciones.

Sin perjuicio de lo cual, Acepta le informará al titular, por medio del correo electrónico capturado, la existencia del requerimiento de información, de modo que el titular pueda ejercer sus derechos ante la autoridad competente.

2.5.6 Entrega de Información a Petición del Titular

Acepta entregará la información del titular del dato biométrico que mantiene en sus registros previo ejercicio del derecho de acceso por éste, en la forma establecida en las Políticas de Privacidad de Acepta.

Acepta mantendrá a disposición de cualquier interesado, a través del registro de acceso público de los RUN asociados a los datos biométricos que hayan sido objeto de un enrolamiento.

2.6 Derechos de Propiedad Intelectual

La prestación de los servicios de certificación biométrica, en ningún caso otorga a los partícipes de la comunidad descritos en 1.3 de estas CPSB derecho de propiedad intelectual o industrial alguno. Así, Acepta retiene todos sus derechos de propiedad intelectual e industrial sobre las obras creadas, desarrolladas o modificadas. Ningún derecho de propiedad intelectual o industrial preexistente o que se adquiera o licencie a o por Acepta, se entenderá conferido a los miembros de la comunidad antes citada.

Salvo acuerdo previo, específico y por escrito en contrario celebrado con algún miembro de la comunidad descrita en 1.3 de estas CPS, ninguno de ellos puede publicar o usar logotipos, marcas, marcas registradas, incluso marcas de servicio y patentes, nombres, redacciones, imágenes, símbolos o palabras 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.

La dirección de correo electrónico será aquel que declare el titular al momento de realizarse la comprobación fehaciente de su identidad.

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 encuentran 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.

3.2 Re-enrolamiento

Por motivo de seguridad, es que Acepta no procede a realizar 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 (ver 4.4), 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 de 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

3.3 Verificación de identidad a partir de un dato biométrico revocado

No es posible esta operación.

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 cédula de identidad.

La revocación es el mecanismo a través del cual Acepta deja sin efecto de manera permanente un dato biométrico capturado por él, cesando. Tendrá lugar cuando Acepta constate alguna de las siguientes circunstancias:

- Solicitud del titular del certificado.
- Fallecimiento del titular.
- Resolución judicial ejecutoriada.
- Que el titular haya proporcionado al momento enrolarse información inexacta o incompleta.
- Si el titular no actualiza los datos proporcionados a Acepta al momento enrolarse.

4 Requisitos Operacionales

En este capítulo se describen los requisitos operativos de Acepta, dentro de la prestación de servicios asociados a su PSC, la cual cuenta con los siguientes componentes de sistema:

- **Interfaces:** Acepta, para su servicio biométrico, establece una relación entre la PSC, la Unidad de Registro y el titular. Esta relación se inicia en la captura de los datos relevantes para el proceso de enrolamiento del titular, los cuales son comprobados por el ministro de fe de la Unidad de Registro, ya sea por medio de comprobación manual de dichos datos contra la cédula de identidad vigente del titular, o adicionalmente a través de una verificación automática de dicha cédula contra los datos capturados en vivo y además de la vigencia del instrumento presentado. De ser aprobada esta solicitud de enrolamiento, los datos civiles como biométricos se envía a través de un canal seguro a la PSC, de manera que el titular quede registrado en los sistemas de la PSC a fin de que puedan realizarse verificaciones de identidad en transacciones electrónicas futuras en que se requiera asegurar que es el titular quién está compareciendo en dicha transacción.

  Una comunicación posterior sólo ocurre en el registro de las revocaciones, las que son ingresadas en la PSC de Acepta y cuyo efecto es el modificar la lista pública de datos biométricos revocados.

- **Sistema de directorios para los datos biométricos:** En caso de requerir información asociada al rol único de los titulares enrolados, los interesados pueden acceder, a través de un servidor web, al repositorio que contiene dicha información (ver https://asistencia.acepta.com/buscar-certificado.html).

- **Procesos de Auditoría:** La auditoría sobre la PSC de Acepta, se realizará al menos una vez al año, para garantizar el funcionamiento y seguridad, de acuerdo a las disposiciones contenidas en la Declaración de Prácticas de Certificación de esta PSC.

- **Bases de datos**: La información relevante incluida en la Base de Datos de la PSC de Acepta, que está asociada al proceso de biometría incluye:
  - Solicitudes verificación de identidad y su resultado
  - Datos biométricos enrolados y su estado

- **Privacidad:** Acepta mantiene un compromiso respecto al uso de los datos personales, el cual asegura la confidencialidad de los datos personales de los titulares que se faciliten en el sitio Web https://sovos.com/es/politicas-y-practicas/, ya sea mediante el o los formulario(s) establecido(s) para esos efectos o bien los que sean recogidos por el hecho mismo de navegar por la Web. Acepta únicamente recolectará aquellos datos que han sido entregados voluntariamente por los usuarios, los que serán usados o tratados únicamente para los fines para los cuales dichos datos fueron proporcionados.

- **Entrenamiento del personal:** Como parte de sus actividades, Acepta realiza cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en

el plan de capacitación anual de su PSC. Este plan incluye labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

De igual forma, Acepta para estos requisitos, considera un plan de auditoría que verifica que su modelo incluye:

- **Restricciones de personal**: Acepta filtra adecuadamente los candidatos para el empleo, los contratistas y sus usuarios especialmente en las tareas sensibles y se asegura de que estos sean aptos para los roles que están siendo considerados, de tal forma de disminuir los riesgos de hurto, fraude o mal uso de las instalaciones. Para esto, la Gerencia de Recursos Humanos utiliza procedimientos de requerimiento y comprobación de antecedentes, entregando a cada empleado, al momento del contrato, del Reglamento Interno el cual en uno de sus capítulos indica deberes, obligaciones y sanciones en caso de incumplimiento de las obligaciones del cargo. Todo trabajador de la PSC Acepta, firma un acuerdo de confidencialidad.

- **Procedimientos de recuperación de desastres**: El Plan de Continuidad de Negocio y Gestión de Contingencias de Acepta, tiene por objetivo el proveer un conjunto de políticas y procedimientos, tanto para prevenir como para enfrentar una situación de emergencia en los sistemas de información, así como también, de mantener la continuidad de las operaciones y asegurar la capacidad de responder eficazmente ante un desastre y otras situaciones de emergencia. Este plan contempla un conjunto de escenarios de contingencia, así como una frecuencia de revisión de dicho Plan.

- **Procedimiento de respaldo**: Los respaldos de servidores centrales de la PSC de Acepta, son realizados haciendo uso de medios magnéticos que aseguran la permanencia de la información a lo menos en 5 años. Los respaldos se realizan diariamente, incluyendo un respaldo incremental de los datos administrados por los sistemas de información, así como un respaldo total semanal. Los respaldos mensuales, son mantenidos como históricos.

Finalmente, Acepta considera los siguientes requerimientos de seguridad:

- **Seguridad física de las instalaciones:** Acepta concibe la seguridad física como parte de una política global, que garantiza la protección de los activos del negocio, mitigando el riesgo asociado a las amenazas y vulnerabilidades, de aquellos activos que pueden protegerse físicamente. Estos recursos incluyen el personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general los activos asociados al mantenimiento y procesamiento de la información.

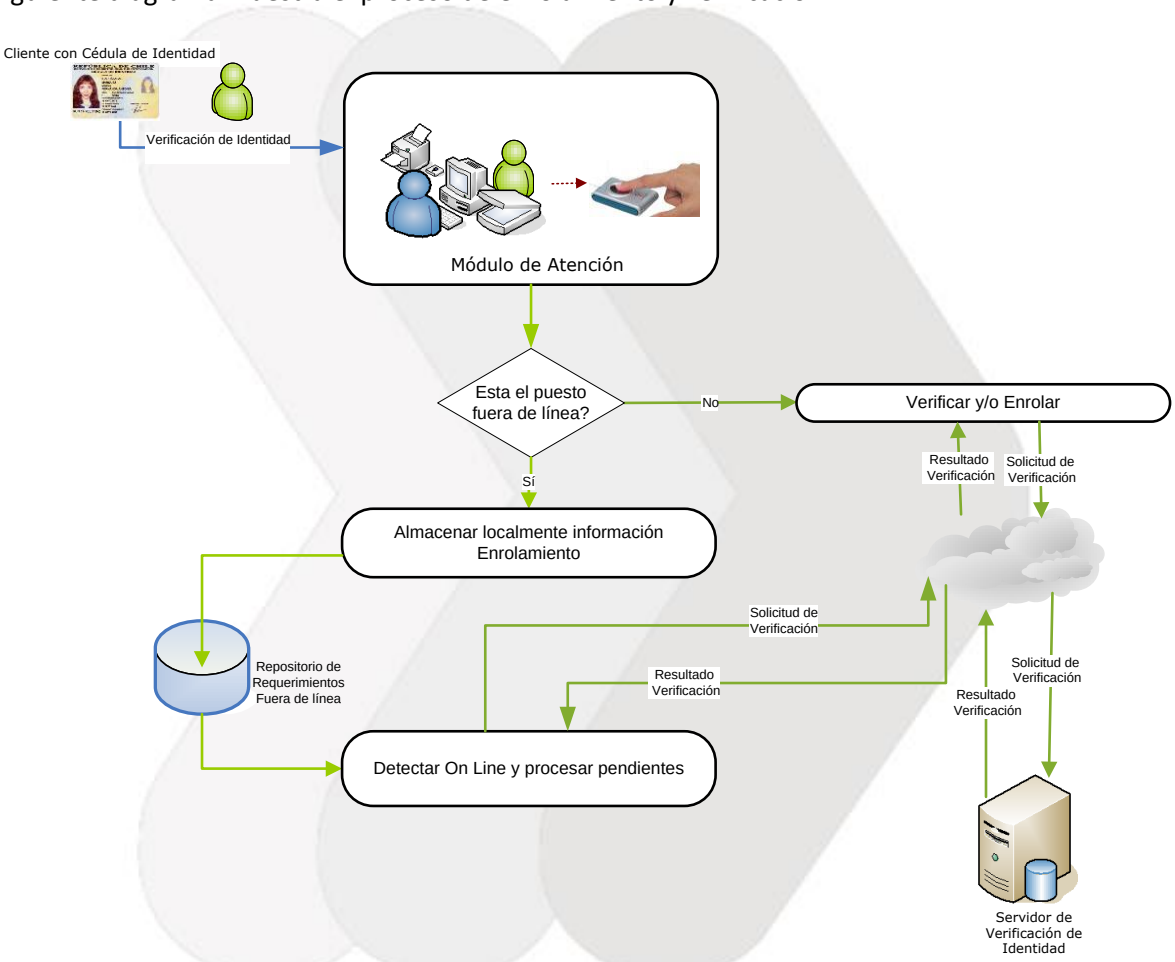
- **Seguridad del Personal:** Acepta, con el objeto de favorecer un uso adecuado de la información y de los sistemas que la apoyan, cuenta con políticas de seguridad de la información vinculadas al recurso humano. Esas políticas, en la medida que se refieran a obligaciones o prohibiciones que afecten al personal de Acepta, deberán encontrarse alineadas, entre otras, con las normas

laborales vigentes, en especial, con los contratos de trabajo y el reglamento interno de orden, higiene y seguridad.

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:

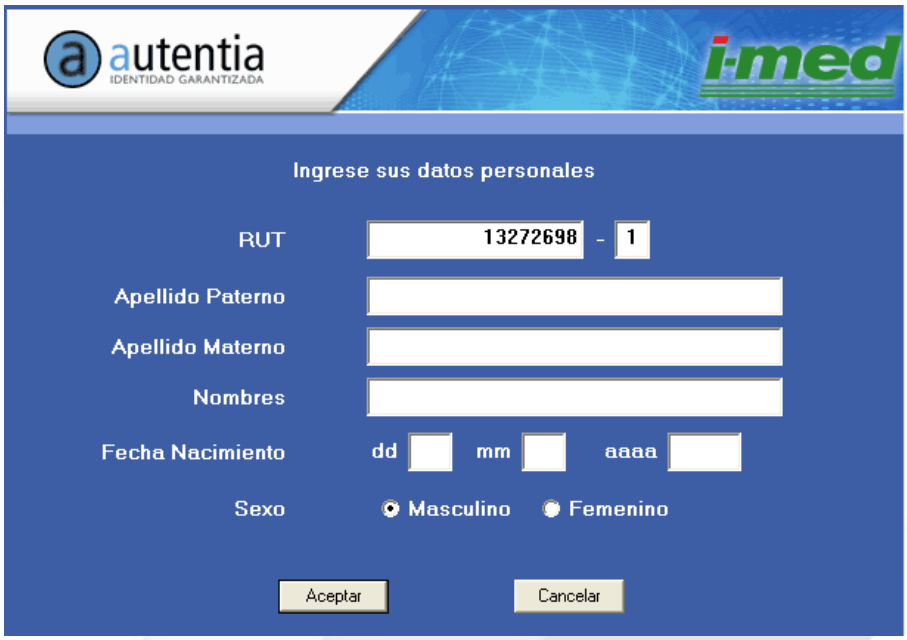
- Completar, por parte del agente, dentro de la pantalla de enrolamiento (activada en este momento):
  - Nombre del titular
  - Fecha de Nacimiento
  - Sexo
  - N° de serie del documento o fecha de vencimiento (de tratarse de un documento de formato antiguo).
  - Mail si corresponde
- Capturar 4 impresiones 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.

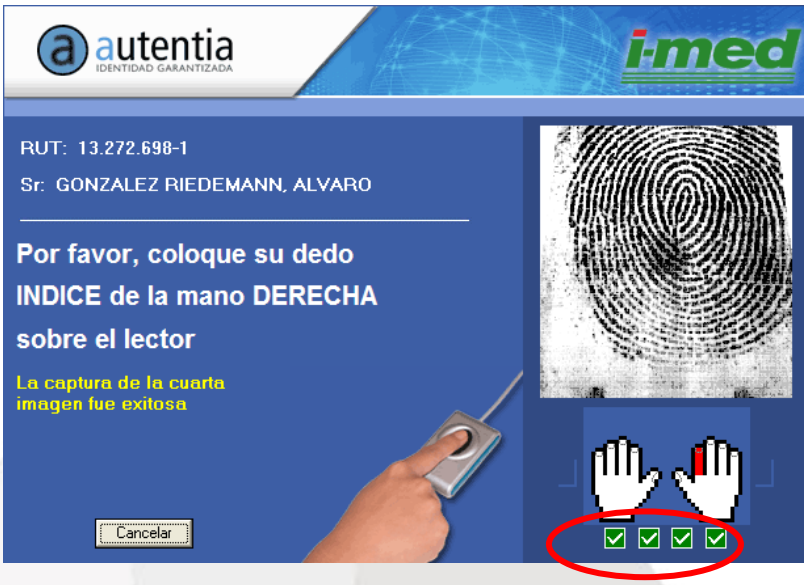
Las siguientes pantallas muestran las etapas del proceso de enrolamiento efectuada por la aplicación biométrica:

- 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:



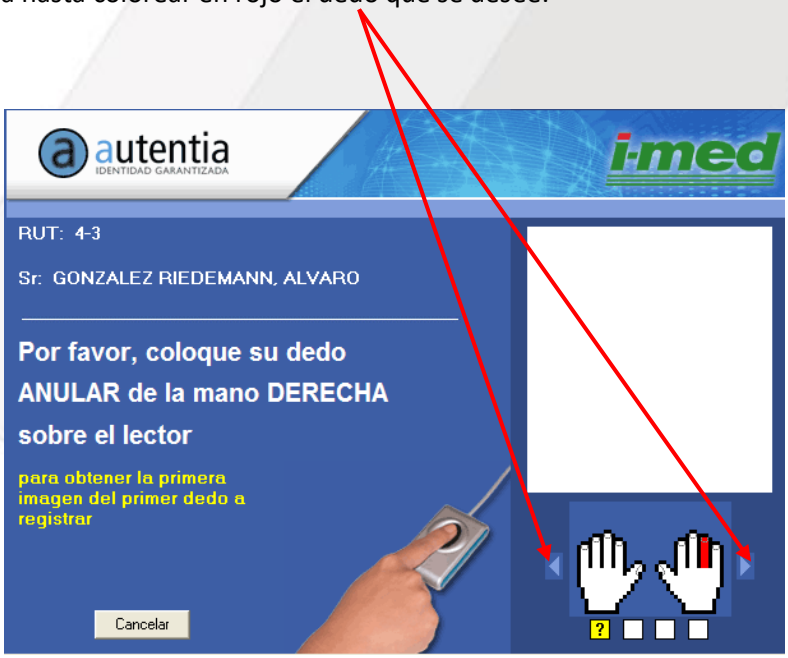
Y también el Nº de serie del documento o fecha de vencimiento (de tratarse de un documento de formato antiguo).

  - 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.

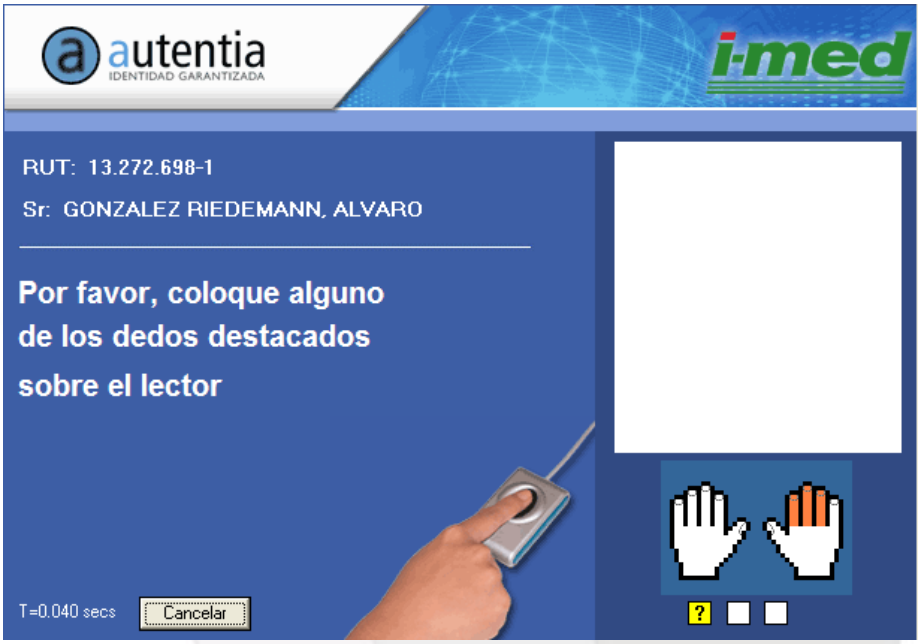
  La solución en este caso es intentar enrolar algún otro dedo, para ello es necesario especificar el dedo que se utilizará en el enrolamiento. Para especificar el dedo a enrolar basta con moverse con la flecha hasta colorear en rojo el dedo que se desee:



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.



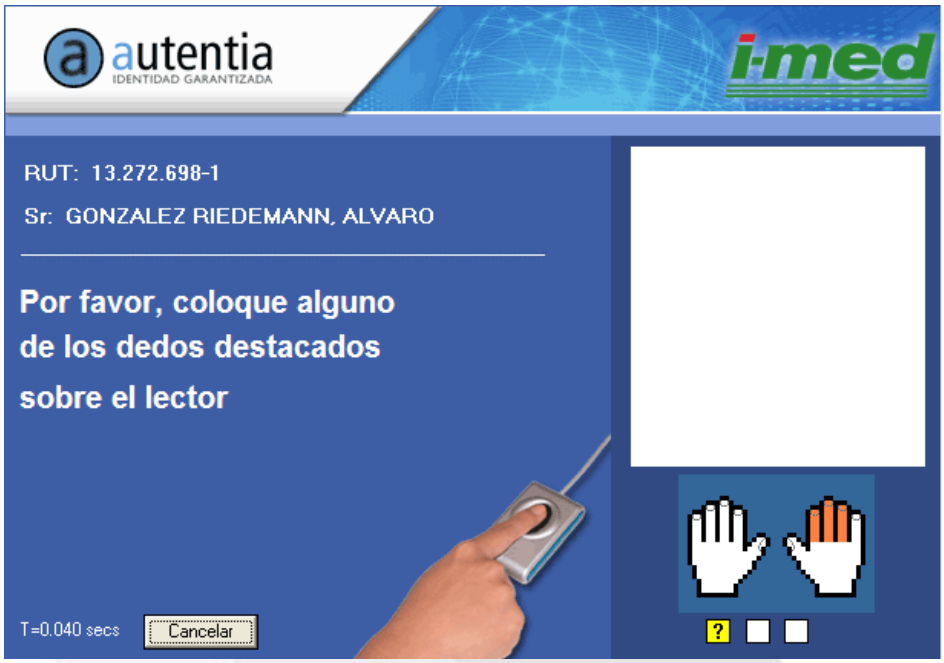
Graduación de la Verificación

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

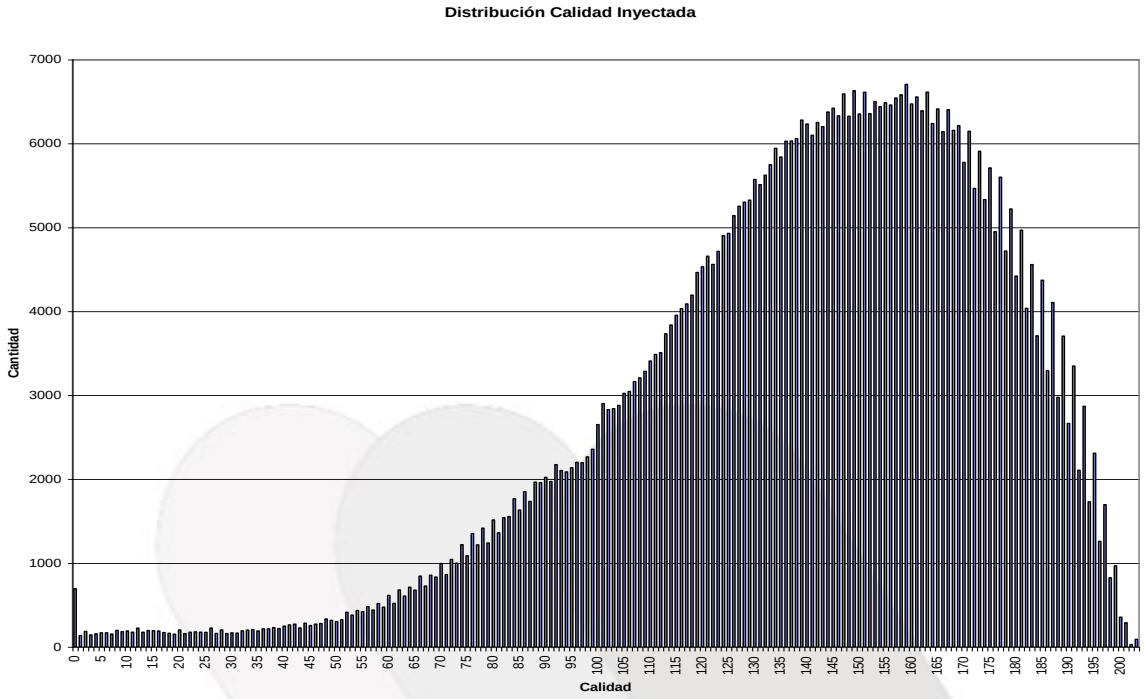
El algoritmo de reconocimiento de la impresión dactilar, utilizado por Acepta, fue desarrollado por los principales investigadores en el campo de la biometría de impresiones dactilares. Este algoritmo incorpora metodologías tradicionales para la identificación de la impresión dactilar, creando un patrón que identifica de manera única de cada usuario.

El funcionamiento de los algoritmos se mide como compensación entre dos cualidades: La tasa de falsa aceptación (FAR), que es la probabilidad de aceptar a alguien que no es y la tasa de falso rechazo (FRR) que es la probabilidad que el sistema rechace a una persona legítima.

El ajuste de los umbrales de FAR y FRR se mueve en dirección opuesta, es decir a una menor FAR se tiene un mayor FRR. El algoritmo utilizado por Acepta, está siendo mejorando continuamente en ambos aspectos.

Este algoritmo proporciona actualmente una FAR de 0.01% y un FRR de 1.4%. Los valores mencionados son dependientes de la calidad de la impresión dactilar del usuario individual.

La prueba grupos masivos ha demostrado que los 80% de todos los usuarios tienen impresiones dactilares con calidad suficiente, que hacen que el algoritmo biométrico siempre indique quien es la persona, sin un falso rechazo.



Del 20% restante, cerca de 15% de usuarios tiene menos información en sus impresiones. En este caso los usuarios tendrán que colocar su dedo sobre el lector de impresión dactilar dos veces para obtener el acceso seguro del sistema. Cerca del 5% de los usuarios tienen impresiones de mala calidad, por tanto, tendrán que intentar una segunda y tercera vez para obtener una lectura exacta.

El motor del reconocimiento de este algoritmo, se ha optimizado para reconocer impresiones de mala calidad, sin embargo, un número muy pequeño de impresiones dactilares, ya sea por el desgaste natural del trabajo manual o por la edad no serán posibles de leer; por lo que el sistema de Acepta permite el registro de uno o más dedos del titular, de manera tal de ampliar las probabilidades de reconocimiento de quien dice ser.

El algoritmo utilizado por Acepta, también elimina las impresiones "latentes" que se dejan en el cristal de exposición de la captura anterior en que fue utilizado. Es esta capacidad que hace claramente superior el algoritmo por Acepta utilizado. El sistema es además enteramente rotación-invariante, lo que significa que el usuario puede poner su dedo en el lector en cualquier ángulo.

4.3 Revocación del dato biométrico

La revocación se realiza en forma presencial en oficinas de Acepta, entregando los antecedentes que comprueben la identidad del suscriptor, mencionando los motivos de la revocación.

En el caso de no ser presencial, el cliente debe enviar un correo indicando la solicitud de revocación, señalando los motivos y una copia de cédula de identidad por ambos lados con su firma manuscrita ante notario. Para mayor detalle ver 3.4.

4.4 Renovación de datos biométricos

La renovación de un dato biométrico implica necesariamente la captura en vivo de una nueva muestra de dicho dato biométrico. El dato biométrico previamente capturado no es factible de ser actualizado así mismo.

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

Los sistemas de Acepta, como Entidad de Certificación, se encuentran alojados en sites con los más altos estándares de seguridad. Todos los sitios cuentan con niveles de protección y solidez de la construcción adecuado y con vigilancia durante las 24 horas al día, los 7 días a la semana.

Los sitios cuentan con diversos perímetros de seguridad, diferentes requerimientos de seguridad y autorizaciones. Entre los equipos que protegen los perímetros de seguridad se encuentran sistemas de control de acceso físico, sistemas de video vigilancia y de grabación, de detección de intrusiones entre otros.

Los sitios además cuentan con un sistema central de vigilancia mediante circuito cerrado de televisión, distribuidas en lugares estratégicos del piso, las que permanentemente están grabando las actividades y registrando los accesos de personas a lugares que requieren acceso restringido. Los centros de control son monitoreados por guardias de seguridad las 24 horas del día, todos los días de la semana, lo que permite llevar un registro y control total de acceso.

Se ha reforzado el control del ingreso a áreas de alta seguridad, como es el área de servidores, a través de la instalación de puertas reforzadas que permanecen constantemente cerradas y que sólo pueden ser abiertas por personas previamente autorizadas por la Gerencia de los Datacenters, bajo la estrecha supervisión de Guardias de Seguridad.

Los controles definidos en los 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, encontrándose los sitios certificados o en proceso de obtención de dicha certificación.

5.2.2 Sistema de Energía Eléctrica

El suministro eléctrico para los sitos está garantizado a través de grupos electrógenos dimensionado para proporcionar energía eléctrica a todas las instalaciones de cada sitio, ante fallas de los proveedores de energía. Todos los sistemas de suministro eléctrico están reforzados por una serie de UPS's instaladas en cascada, tiempo más que suficiente para activar los generadores respectivos y asegurar la continuidad del servicio. También se cuenta con tableros eléctricos redundantes de modo de asegurar el funcionamiento antes fallas de la distribución de los equipos.

Los sitios en sus instalaciones disponen de sistemas de alimentación ininterrumpida con una potencia suficiente para mantener autónomamente la red eléctrica durante los períodos de apagado controlado del sistema y para proteger a los equipos frente a fluctuaciones eléctricas que los pudieran dañar. Los sitios cuentan con todos los resguardos necesarios para mantener una continuidad de energía suficiente y su operación por largos periodos de tiempo.

5.2.3 Sistema de Control Ambiental

Los sitios cuentan con un suministro continuo de climatización (aire acondicionado, humedad, polvo en suspensión) en modalidad 24x7x365, garantizando el buen funcionamiento de los equipos. Las especificaciones son:

- Temperatura: 21°C+/-3°C.
- Humedad relativa: 45%+/-10%.
- Polvo en suspensión: 75 Microgramos por m3, como máximo.

Para cumplir esta función los sitios cuentan con equipos de climatización precisa que detectan y controlan la humedad relativa del ambiente, lo que permite mantener ambientes óptimos de temperatura y humedad, en las distintas salas. Todos cuentan además con un sistema redundante de climatización dimensionado para asegurar una temperatura estable y continua a las salas de equipamiento y a las áreas de operación. En caso de fallas del sistema de aire acondicionado, éste cuenta con un sistema de respaldo que garantiza la continuidad del servicio.

5.2.4 Sistema de Extinción y Control de Incendios

Dado los riesgos de incendio a que pueden estar sujetos los sitios, es que todos ellos cuentan con el suministro e instalación de un sistema de protección contra incendios sobre la base de detección temprana que se realiza bajo vía un sistema de aspiración de partículas del ambiente y de extinción automática con FM-200, aprobación UL, e instalado bajo norma NFPA.

5.2.5 Telecomunicaciones

Tomando en cuenta la importancia que tiene la infraestructura de comunicaciones para el negocio de Acepta, es que se ha diseñado para cada servicio una plataforma robusta, segura y escalable, utilizando como base para ello los servicios WAN, estos servicios provistos por los principales carriers del país, que acceden a los distintos sitios, nos aseguran, redes confiables y con tecnología de última generación.

El objetivo principal de este diseño es cumplir con los niveles de servicio comprometidos por Acepta, por lo que se contempla respaldos en todos los puntos críticos. Adicionalmente, cabe destacar que las redes de transporte del carrier están diseñadas para entregar una alta disponibilidad, con una arquitectura redundante interna, lo cual permite garantizar el servicio de conectividad sobre su red.

5.2.6 Seguridad Lógica Data Center

Los sitios cuentan los siguientes aspectos de seguridad lógica:

- Múltiple tecnología de firewall
- Sistema de detección de intrusos
- Sistemas de análisis de seguridad activos

5.3 Controles de procedimientos

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

5.3.1 Papeles de confianza

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

- Administrador de Sistemas: A cargo de
  - La instalación y configuración de sistemas operativos, de productos de software y del mantenimiento y actualización de los productos y programas instalados. Cuentan con capacidad para configurar y mantener los sistemas, pero sin acceso a los datos.
  - Activar los servicios.
  - Establecer y documentar los procedimientos de monitorización de los sistemas y de los servicios que prestan.
  - Son responsables de la correcta ejecución de la Política de Copias, y en particular, de mantener la información suficiente que permita restaurar eficientemente cualquiera de los sistemas.
  - Debe mantener el inventario de servidores y equipamiento que compone el núcleo de la plataforma de certificación.
- Administrador de Seguridad
  - Debe cumplir y hacer cumplir las políticas de seguridad de Acepta, y debe encargarse de cualquier aspecto relativo a la seguridad de la PSC de Acepta, desde seguridad física hasta la seguridad de las aplicaciones, pasando por seguridad de la red. Esta función estará soportada a través de una oficina de seguridad técnica, además del oficial de seguridad.
- Operador de Unidad de Registro:
  - Responsable de realizar el registro presencial ante la solicitud de un enrolamiento, preocupándose de la verificación de identidad del solicitante.
- Responsable de formación, soporte y comunicación
  - Se encarga del mantenimiento de contenidos de la web de Acepta.
  - Se encarga de definir el plan de formación para usuarios finales, para agentes de Call Center y para personal implicado directamente en la operación y administración de la plataforma de certificación de la PSC de Acepta.
  - Debe revisar mensualmente los ficheros de incidencias y respuestas de Call Center, y revisar los registros de los agentes de Call Center.
  - El Responsable de formación, soporte y comunicación contará con la colaboración de las áreas de RRHH, Marketing o Post venta de estimarse necesario.

- Responsable de Seguridad
    - Se asigna esta tarea al Comité de Seguridad de la Información de Acepta, asumiendo la responsabilidad general en cuanto a la actualización e implantación de las políticas y procedimientos de seguridad que han sido aprobadas.
    - Gestionará que los sitios donde se encuentran los sistemas de Acepta, cumplan con gestionar los sistemas de protección perimetral y la correcta gestión de los sistemas de detección de intrusiones (IDS) y de las herramientas asociadas a éstos.
    - Es el responsable de resolver o hacer que se resuelvan las incidencias de seguridad producidas, de eliminar vulnerabilidades detectadas, y otras tareas relacionadas.
    - Es responsable de autorizar movimientos de material fuera de las instalaciones de la PSC
    - Debe encargarse de efectuar la selección y determinar la contratación de terceros especialistas que puedan colaborar en la mejora de la seguridad de la PSC de Acepta
- Auditor
    - Encargado de realizar auditorías internas. En definitiva, debe comprobar todos los aspectos recogidos en la política de seguridad, políticas de copias, prácticas de certificación, políticas de certificación, etc. tanto en el núcleo de sistemas de la PSC de Acepta y su personal como en los puntos de Registro. Para esta labor se hará uso de Auditores internos como también la contratación de una auditoría externa anual.
- Responsable de Documentación
    - Se encargará de mantener el repositorio de documentación y los archivos de documentación en papel.
    - Controlará que cada área lleve a cabo la actualización de documentos cuando se requiera.
    - Se encargará de mantener actualizado el fichero de índice de documentos y será el único habilitado para almacenar, borrar o modificar documentos en el repositorio de documentación.

5.4 Controles de seguridad del personal

5.4.1 Requerimientos de antecedentes y experiencia

Acepta requiere que todo el personal asociado a la PSC cuente con una calificación y experiencia acorde a la prestación de servicios de certificación, de acuerdo a la Ley 19.799 sobre documentos electrónicos firma electrónica, certificación de dicha firma, marca de tiempo y biometría

5.4.2 Comprobación de antecedentes

Mediante CV y entrevistas realizadas al momento de la vinculación.

5.4.3 Requerimientos de formación y reentrenamiento

Como parte de las recomendaciones en que Acepta ha trabajado, se considera para el personal asociado a la PSC, cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual de Acepta para la PSC. Este plan incluirá labores de reentrenamiento de existir cambios tecnológicos, en las políticas o prácticas de certificación o cualquier documento que se considere relevante de ser informado.

5.4.4 Frecuencia de rotación de tareas

No aplica.

5.4.5 Sanciones

Acepta informa y entrega a cada empleado el Reglamento Interno de Orden, Higiene y Seguridad de la empresa, en el cual se establecen las obligaciones de los trabajadores y las sanciones aplicables en caso de incumplimiento de las mismas, atendidas las responsabilidades o funciones de éstos.

5.4.6 Requerimientos de contratación

Todo trabajador de la PSC asume obligaciones de confidencialidad, las que están descritas en su contrato de trabajo.

5.4.7 Documentación entregada al personal

El personal de la PSC tendrá a su disposición el siguiente material:

- Declaración de Prácticas de Certificación
- Políticas de certificación
- Política de privacidad
- Política de Seguridad de la Información
- Organigrama y funciones del personal

Adicionalmente, se facilitará el acceso a la documentación técnica necesaria para llevar a cabo sus funciones.

5.4.8 Control de cumplimiento

De acuerdo al Plan de seguridad se mide el control de cumplimiento de las actividades programadas de manera anual.

5.4.9 Finalización de contratos

El oficial de seguridad con el apoyo del área de sistemas y RRHH, procederá a:

- Suprimir los privilegios de acceso del individuo a las instalaciones de la organización
- Suprimir los privilegios de acceso del individuo a los Sistemas de Información de la organización
- Supresión de acceso a toda información, a excepción de la considerada PÚBLICA
- Informar al resto de la organización claramente de la marcha de individuo y de su pérdida de privilegios.
- Informar a los proveedores y entidades externas a Acepta la marcha de individuo y de que ya no representa a la PSC de Acepta.
- Verificar la devolución del material proporcionado por la Acepta. Por ejemplo:
    - Equipo computacional
    - Llaves mobiliario oficinas
    - Teléfono móvil
    - etc.

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

Acepta implementa una infraestructura y sistema de certificación de tal modo que permita monitorear continuamente las operaciones realizadas; y poder detectar cualquier situación errónea, así como cualquier intento de uso o ingreso no-autorizado al sistema. Dicho monitoreo se realiza continuamente por personal autorizado.

Adicionalmente, se cuenta con una serie de herramientas de prevención y detección de posibles intentos de penetración indebida a los sistemas de certificación y datos o funciones del back-end del sistema. Dichos registros son revisados al menos mensualmente.

5.5.3 Periodo de Retención para el log de auditoría

Todos los registros correspondientes al registro de eventos con el fin de auditoría se mantienen de tal forma que se permita una adecuada consulta y revisión de tales registros por personal autorizado. Por tanto, varios de dichos registros se mantienen on-line, realizándose respaldos increméntales diariamente, así como respaldos completos con una base mensual.

Cada mes se obtiene un respaldo completo el cual es custodiado de manera segura. Para ello, Acepta cuenta con servicios de custodia electrónica de documentos, los cuales se retienen por un período no inferior a 10 años.

5.5.4 Protección del log de auditoría

Toda la información pertinente a auditorías de seguridad se mantiene de manera segura y no es accesible por cualquier persona o proceso computacional, salvo por aquellos estrictamente autorizados.

5.5.5 Procedimientos de respaldo del log de auditoría

Los respaldos de la información de auditoría se realizan acorde a un detallado programa de respaldos aplicable por igual al resto de los datos generados en las operaciones del PSC. Dicho programa contempla respaldos incrementales diarios y respaldos completos una vez al mes.

5.5.6 Evaluaciones de vulnerabilidad

Con el propósito de mantener un ambiente seguro y confiable, Acepta y sus PSC acreditadas tienen un accionar sistemático y pro-activo respecto a la detección y evaluación de posibles vulnerabilidades que puedan atentar contra dicha seguridad.

Para ello, se mantienen aplicaciones específicas de monitoreo permanente de las operaciones del sistema. Además, se efectúa una adecuada capacitación de todo el personal, sobre sus responsabilidades y conductas respecto a la conservación de un ambiente seguro.

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

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

5.6.3 Sistema de colección de archivos

Los documentos electrónicos se mantienen en custodia electrónica cerrada para su conservación segura. Cada archivo estará firmado digitalmente.

5.6.4 Procedimientos para obtener y verificar información de archivos

La consulta de los documentos electrónicos dejados en custodia electrónica en Acepta, se hace mediante el uso debidamente autorizados, para garantizar la confidencialidad de la información y autorización requerida.

La verificación de la autenticidad de los documentos electrónicos está dada por la verificación de la firma digital.

5.7. Cambio de datos biométricos

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

Los motivos para efectuar un re-enrolamiento normalmente se deben a cambios de la biometría en vivo a ser capturada, ya sea por accidente o desgaste a efecto del tiempo.

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

En caso de sospecha de haber sido alterados uno de estos recursos, de responsabilidad de Acepta, se detendrá el funcionamiento de los servicios de Acepta hasta el restablecimiento de un entorno seguro, con la incorporación de nuevos componentes. De forma paralela se realizará una auditoría para identificar la causa de la alteración y asegurar la no repetición de la misma.

En el caso de verse afectados los datos biométricos capturados, se notificará del hecho a los titulares de los mismos y se procederá a re-enrolar dichos datos nuevamente.

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

En caso de desastre natural que afecte a las instalaciones del sitio principal de Acepta y sus servicios, se procederá a activar el Plan de Continuidad del Servicio y recuperación de desastres.

5.9 Cese de una PSC

En el evento que Acepta vaya a descontinuar sus operaciones como prestador de servicios de certificación, deberá comunicar tal situación a los titulares de certificados o datos biométricos, en la siguiente forma:

a) Si el cese es voluntario, con una antelación de a lo menos dos meses y señalando al titular que de no existir objeción a la transferencia de los certificados y/o datos biométricos a otro prestador de servicios de certificación, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de los mismos. En este caso, si el prestador es acreditado, se traspasará los certificados y datos biométricos, necesariamente, a un certificador acreditado.

b) Si el cese no es voluntario, la cancelación de la acreditación se comunicará inmediatamente a los titulares. En caso que el prestador de servicios de certificación esté en situación de traspasar los certificados a otro prestador acreditado, se informará tal situación en la forma y plazo señalado en la letra a).

Si el titular del certificado se opone a la transferencia, el certificado y/o datos biométricos capturados quedarán sin efecto sin más trámite, que deberá estar acreditado si aquel lo fuera, o a una empresa especializada en la custodia de datos electrónicos, por el tiempo faltante para completar los 6 años desde la emisión de cada certificado y/o captura del dato biométrico. Esta situación deberá verse reflejada en el registro público de prestadores acreditados de servicios de certificación, el que deberá contener el número de la resolución que concede la acreditación, el nombre o razón social del

certificador, la dirección social, el nombre de su Representante Legal, el número de su teléfono, su sitio de dominio electrónico y correo electrónico así como la compañía de seguros con que ha contratado la póliza de seguros.

En caso que el cese en la prestación del servicio sea por voluntad del Acepta, deberá solicitar a la Entidad Acreditadora, con al menos un mes de anticipación, la cancelación de su inscripción en el registro público mencionado en párrafo anterior, comunicándole el destino que dará a los datos de los certificados y/o datos biométricos, especificando, en su caso, los que va a transferir y a quién, cuando proceda. El cese de la actividad será registrado como nota de cancelación de la inscripción de la acreditación por la Entidad Acreditadora en el registro público mencionado.

En cualquiera de estos casos, las relaciones entre la PSC y los usuarios seguirán rigiéndose por lo señalado en estas CPSB mientras no se ponga en conocimiento de los usuarios un nuevo documento por escrito que venga a sustituir este documento.

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 4.2.1 de estas CPSB.

6.2.2 Verificación de identidad

De acuerdo a 4.2.2 de estas CPSB.

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

Acepta durante el proceso de captura verifica automáticamente la calidad de la imagen, evaluando si es factible con dicha imagen generar el número suficiente de puntos característicos, que permitan realizar los enrolamientos y futuras verificaciones de identidad bajo las actuales tasas de Falso Rechazo y Falsa Aceptación declaradas

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

Protocolo AES (Advance Encryption Standar), el cual es usado en el canal entre el cliente y el servidor, así como para encriptar campos no clave de las tablas de la Base de Datos. Es una encriptación simétrica. Adicionalmente es posible el firmar electrónicamente los datos de enrolamiento capturado, por parte de la PSC 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

Acepta, en lo referente al dominio de la PSC, hace uso de procedimientos de pruebas y paso a producción de cualquier cambio que afecta al software de los servicios de la PSC. Estos cambios están regulados por un procedimiento de control de cambio administrado por el área de desarrollo de Acepta. Asimismo, la aplicación del procedimiento para el almacenamiento seguro del hardware

criptográfico y los materiales de activación se materializa después de la ceremonia de generación de claves. Del mismo modo se realizan pruebas de captura y verificación de identidad en caso de afectarse los módulos biométricos utilizados por Acepta.

6.6 Controles de seguridad de red

Acepta limita el acceso de sus redes al personal debidamente autorizado. En particular:

- Se implementan controles para proteger la red interna de acceso por terceras partes
- Los datos sensibles son cifrados al momento ser intercambiado a través de redes no seguras. Se garantiza que los componentes locales de red están ubicados en entornos seguros

6.7 Controles de seguridad de los módulos criptográficos y biométricos

Acepta utiliza módulos criptográficos y biométrico con hardware y software disponibles comercialmente, los cuales son desarrollados por terceros.

Los módulos criptográficos utilizados cuentan con un nivel de certificación de seguridad suficiente para la funcionalidad y seguridad que se exige.

Los módulos biométricos cuentan con estándares de la industria en su fabricación.

7 Administración de las CPBS

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

7.1 Procedimientos para Modificar las CPBS

Las prácticas 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 CPBS

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