Modelo de Identificación Digital de América Latina y el Caribe

IdLAC

Documento en permanente evolución elaborado por el Grupo de trabajo de Red Gealc con apoyo del Consorcio Ciudadano Digital Regional (BID, Banco Mundial, CoDevelop y OEA)

1. Contenido

1. Contenido 2
2. Objetivo del documento 3
3. Modelo de Identificación Digital de América Latina y el Caribe (IdLAC) 3
4. Niveles de Seguridad en las Identificaciones Digitales 7
5. Aspectos normativos 12
6. Datos para la Identificación Digital 13
7. Protocolos de Integración 16
8. Controles de Seguridad Transfronterizos 17
9. Términos 18
10. Anexo I – Lineamientos para pruebas de vida y biometría facial 19
    Introducción 19
    Consideraciones básicas 19
    Pruebas de Vida 19
    Comparación Biométrica Facial 20
11. Anexo II – Mapeo entre IdLAC y los principales modelos de referencia (ISO/IEC 29115, eIDAS y NIST SP 800-63-06) 28

2. Objetivo del documento

Este documento define el modelo de identificación digital de América Latina y el Caribe llamado IdLAC. Las definiciones y conceptos desarrollados en este documento han sido definidos y aprobados por todos los países y el mantenimiento y evolución del mismo es responsabilidad de todos los países.

Para implementar el modelo y lograr la interoperabilidad de la identificación digital en toda la región, es necesario que cada país implemente el broker modelo (o un broker que esté alineado al modelo) con el fin que se puedan integrar brokers en forma estandarizada y habilitar los proveedores de identificación de confianza de un país en los otros países.

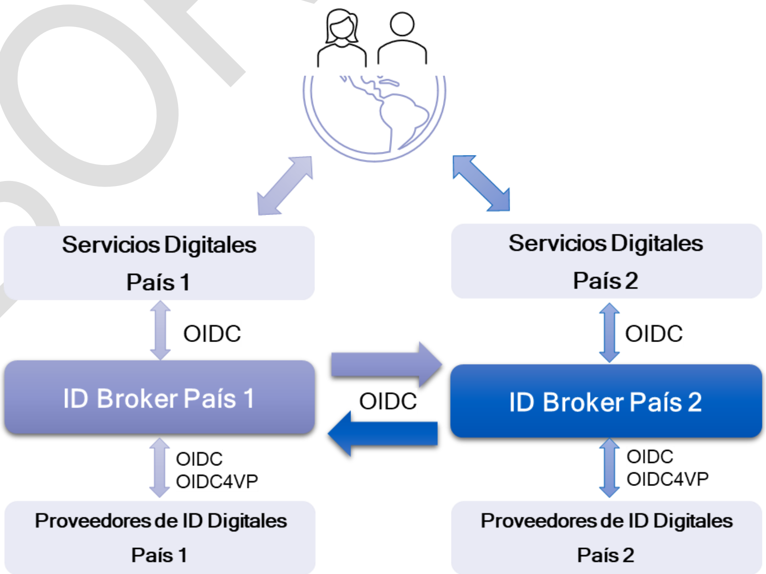
La documentación técnica del broker se encuentra disponible en el documento "Broker Regional - Documentación Técnica" y está alineada a las definiciones acordadas en el presente documento.

3. Modelo de Identificación Digital de América Latina y el Caribe (IdLAC)

El objetivo del modelo es estandarizar la identificación digital para escalar en forma ordenada, simple y segura en la interoperabilidad transfronteriza en toda la región. Este modelo incluye los siguientes temas:

- Niveles de seguridad en las identificaciones digitales.
- Datos para la identificación digital.
- Protocolos utilizados para integrar proveedores de identificación y servicios digitales.
- Controles de Seguridad Transfronterizos.

La siguiente imagen ilustra el modelo planteado donde dos países integran sus identificaciones digitales integrando sus brokers de identificaciones digitales:

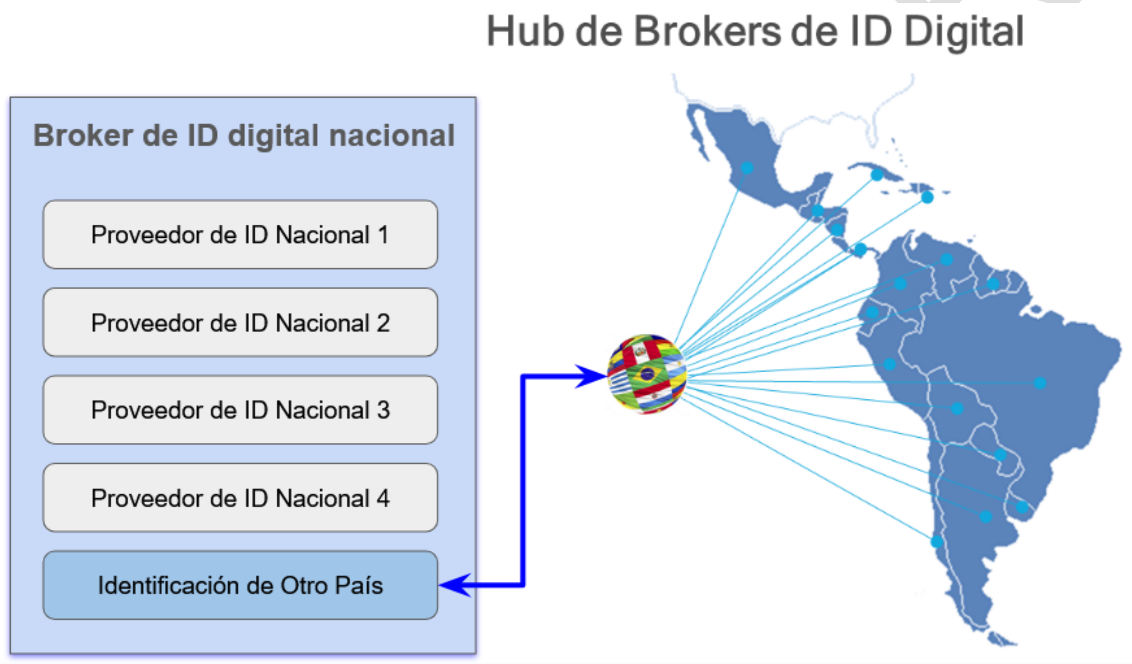


La imagen anterior muestra como mediante la integración entre dos brokers nacionales, los proveedores de identificación digital de un país se habilitan para acceder a los servicios digitales del otro país y viceversa. **El impacto de esto es que un ciudadano de un país puede**

utilizar sus identificaciones digitales nacionales para ingresar en forma simple y confiable a los servicios digitales del otro país.

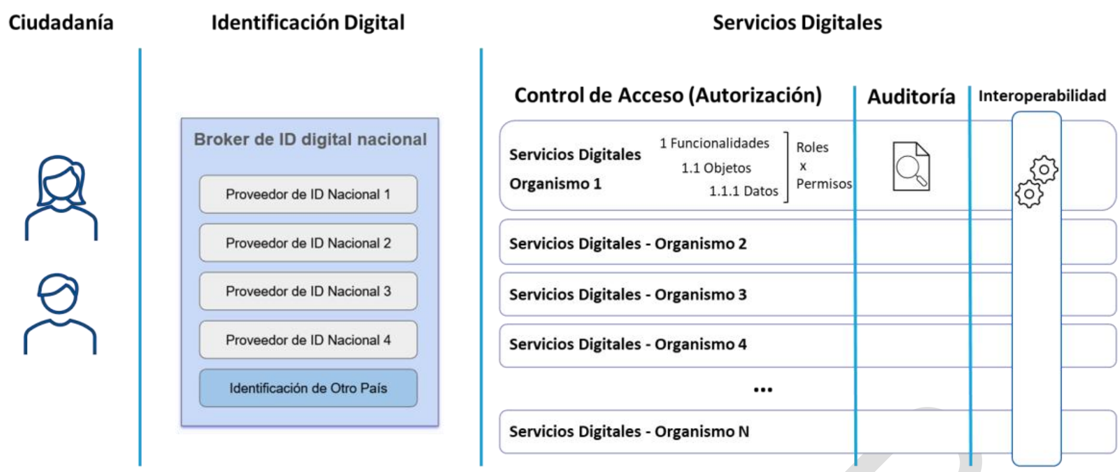
Cada usuario se identifica (autentica) en un proveedor de identificación de su país, las credenciales nunca salen del proveedor. **En identificaciones transfronterizas, los brokers confían en las identificaciones realizadas en los otros países.** Así como a nivel nacional, los servicios digitales integrados al broker confían en las identificaciones realizadas en los proveedores de identificación integrados de su país.

A mediano plazo, en un escenario donde muchos países poseen un ecosistema de identificaciones digitales con varios proveedores habilitados, articulado por un broker nacional, será necesario fortalecer la gobernanza, definir y desarrollar un hub de brokers de modo que cada país integre su broker una sola vez al hub. Este esquema permitiría escalar a toda la región, en forma ordenada, estandarizada y segura. La siguiente imagen muestra esta situación:



La imagen anterior muestra un ejemplo donde un usuario va a ingresar a un servicio digital y se va a identificar mediante el broker de identificaciones digitales nacional. En este caso, si es un usuario del mismo país, puede elegir cualquiera de los 4 proveedores de identificación disponibles y si es un usuario extranjero, a través del hub de borkers accede al broker nacional de su país, utilizan un proveedor de identificación digital confiable de su país y vuelve al servicio original identificado.

A nivel país, en un modelo donde existe un ecosistema nacional de identificaciones digitales articulado por un broker que integra varios proveedores y la posibilidad de utilizar identificaciones digitales confiables de otros países, cada organismo integrado al broker debe resolver la autorización, la auditoría y la interoperabilidad. La siguiente imagen ilustra esta situación:



El esquema anterior refleja relación entre la identificación digital nacional y lo que deben adaptar los organismos integrados en el ecosistema:

1. **Identificación Digital:** Los ciudadanos utilizan una identificación digital nacional para ingresar a los servicios digitales de diferentes organismos. Se identifican como personas físicas o naturales, no hay identificación de empresas (persona jurídica). El broker de identificación digital nacional actúa como Single Sing On en todo su ecosistema, es decir, en todos los servicios u organismos integrados. **La identidad digital de una persona es única y universal y está directamente asociada a su identidad física, los métodos para identificarse pueden ser varios, pueden utilizar diferentes tecnologías y estándares para verificar la identidad de la persona, lo que puede repercutir en diferentes niveles de confianza.** Es importante resaltar el concepto de identidad, los datos que identifican a las personas son siempre los mismos, la forma de a hacerlo puede cambiar según el proveedor.

2. **Autorización:** Los sistemas informáticos en cada organismo, idealmente vistos como un único sistema diseñado bajo una estrategia multicanal, deben desarrollar un sistema de autorización basado en roles y permisos que sea posible de configurar en tres niveles de profundidad:

    a. Funcionalidades: el nivel más amplio, configurando roles y permisos a nivel de cada funcionalidad del sistema.

    b. Objetos: nivel intermedio, los objetos dependen directamente del negocio de la organización (en una historia clínica podría ser un acto médico, en la administración tributaria, una declaración jurada, etc).

    c. Datos: el nivel más granular, se debería poder configurar permisos a roles sobre un dato específico. Esto debería estar alineado al modelo de gobernanza de datos de la organización.

    Las personas ingresan a un organismo con su identificación digital nacional (o extranjera) y el sistema de control de acceso debe habilitar las operaciones (permisos) sobre las funciones, objetos y datos que le fueron asignados en función de la normativa asociada. La identidad no varía en todo el ecosistema, los permisos si, dependiendo del rol de la persona en cada caso. Es importante que el sistema de control de acceso posea reportes y herramientas que alerten y ayuden a los responsables a gestionar los roles y permisos sobre su información en cada caso.

3. **Auditoría:** En un escenario donde muchas personas ingresan a un organismo actuando con diversos roles sobre mucha información, es importante un sistema de auditoría

que registre debidamente todos los movimientos del usuario. Esto es importante por muchas razones, entre otras, para restaurar la integridad de la información si fuese necesario o contar con evidencia confiable ante posibles fraudes o delitos.

4. **Interoperabilidad:** la identificación digital intercambia datos minimalistas suficientes para identificar una persona. Si los diferentes sistemas y organismos necesitan información que no es parte de la identificación de una persona deben resolver esto mediante las diferentes plataformas de interoperabilidad disponibles asegurándose de cumplir con la normativa vigente.

Un sistema de identificación digital nacional con integración transfronteriza, donde las personas poseen una única identidad global, que se puede mapear en forma simple y confiable con su identidad física, favorece sustancialmente la interoperabilidad a nivel regional, otorgando facilidades y confianza para obtener información de una persona y simplificar los servicios digitales. Este escenario favorece el desarrollo de sistemas inteligentes que brindan múltiples servicios en diferentes áreas basados en el uso de información de calidad y potenciado por herramientas de Inteligencia Artificial.

4. Niveles de Seguridad en las Identificaciones Digitales

Se definen tres niveles de seguridad o confianza para las identificaciones digitales del modelo IdLAC:

1. Nivel bajo de confianza
2. Nivel medio de confianza
3. Nivel alto de confianza

Si bien el modelo define tres niveles, cada país podrá utilizar los nombres que desee, el objetivo del modelo es poder homologar en forma clara los niveles de seguridad en la región.

El nivel de seguridad (NID) es el mínimo entre dos variables:

1. **Nivel de Registro (RID)**, puede ser bajo (1), medio (2) o alto (3). Un registro 0 es un registro que no fue validado por el usuario, por lo que todavía no puede ser utilizado.
2. **Nivel de Autenticación (AE)**, puede ser bajo (1), medio (2) o alto (3). Todos los proveedores de identificación deben implementar políticas de contraseñas que aseguren que el usuario solamente puede utilizar contraseñas consideradas fuertes.

La siguiente tabla muestra los requerimientos para cada nivel de registro:

Nivel RID	Requerimientos
1 - Bajo	**El usuario creó su registro en línea y lo validó mediante el correo o el teléfono, no hay una validación fehaciente de su identidad.** El sistema realizó algunos chequeos básicos que no incluyen la validación de la identidad de la persona. Los chequeos pueden ser: • Comprobación matemática del número de documento utilizado. • Comprobación de no duplicidad del identificador del usuario (código país - código documento - número de documento) en la base de datos del registro. • Comprobación de no duplicidad del correo ingresado por el usuario. • Comprobación de no duplicidad del número de teléfono ingresado por el usuario. • Comprobación de la existencia de la persona en la base de datos del registro público utilizando uno o más datos proporcionados por el usuario. • Comprobación de inexistencia del usuario en un registro de defunciones público.
2 - Medio	A partir de un usuario básico, el **titular valida su identidad** utilizando alguno de los siguientes medios: • **En forma presencial en un punto de atención habilitado**, utilizando el documento vigente utilizado para crear el registro. El documento de identificación debe ser revisado por un funcionario acreditado y los datos (código país, código documento, número de documento, primer nombre, segundo nombre, primer apellido y segundo apellido) deben coincidir con el registro del usuario. • **En forma remota, utilizando la firma electrónica avanzada,**

	cualificada o certificada de persona física o natural. Ingresando a su registro en forma digital, el usuario debe firmar un acuerdo de adhesión y en caso de que los datos del firmante coincidan exactamente con los del registro (código país, código documento, número de documento, primer nombre, segundo nombre, primer apellido y segundo apellido) y la firma sea válida, se constituye en una prueba de identidad válida. ● **En forma remota, realizando una videollamada con un funcionario acreditado.** Durante la videollamada deben darse las condiciones necesarias de conectividad, claridad en la cámara y en el audio. El funcionario público debe contar con acceso al registro en el organismo público competente de la persona a través de un canal seguro. Durante la videollamada el usuario debe mostrar ante la cámara el documento de identidad utilizado y los datos del documento deben coincidir exactamente con los del registro del usuario (código país, código documento, número de documento, primer nombre, segundo nombre, primer apellido y segundo apellido) en el organismo competente y el registro en el proveedor de identificación. Finalmente, en caso de que todos los pasos anteriores sean satisfactorios, el funcionario deberá tomarle una foto al usuario y la foto deberá ser comparada biométricamente con la foto del registro del usuario en el organismo competente. Si la comparación biométrica es satisfactoria se validará la identidad del usuario. ● **En forma remota automática (imagen del documento, prueba de vida y biometría).** El usuario debe tomar imágenes de su documento físico utilizado para el registro, el documento no puede estar vencido. Los datos obtenidos en la imagen tomada al documento deben coincidir exactamente con los del registro del usuario (código país, código documento, número de documento, primer nombre, segundo nombre, primer apellido y segundo apellido). A continuación, el sistema deberá aplicar una prueba de vida al usuario y luego tomar una fotografía facial al usuario que sea comparada biométricamente con la foto del registro público a través de un canal seguro de interoperabilidad.
3 - Alto	En términos generales: ● El **registro debe tener vencimiento**, por lo que el usuario deberá renovarlo periódicamente. ● El **registro puede ser un certificado digital X.509 y un par de claves de firma electrónica avanzada, cualificada o certificada de persona física o natural** en el contexto de una Infraestructura de Claves Pública reconocida, validada y otorgada por un prestador acreditado. A los métodos para validar la identidad del nivel medio se le agregan los siguientes requisitos: ● **En forma presencial en un punto de atención habilitado**, realizando una validación biométrica de la huella con el registro público o el documento de identidad con chip o una validación biométrica facial con el registro público o el documento de identidad con chip. ● **En forma remota, utilizando la firma electrónica avanzada,**

	cualificada o certificada de persona física o natural. Ingresando al registro con nivel de autenticación alto, previo a su vencimiento, el usuario debe firmar un acuerdo de adhesión y en caso de que los datos del firmante coincidan exactamente con los del registro (código país, código documento, número de documentos, primer nombre, segundo nombre, primer apellido y segundo apellido) y la firma sea válida, se constituye en una prueba de identidad para renovar el registro por un período más. ● **En forma remota, realizando una videollamada** con un funcionario acreditado bajo los mismos requerimientos de nivel medio. Para realizarlo debe ingresar al sistema utilizando su identificación digital de nivel alto antes de su vencimiento. ● **En forma remota automática (imagen del documento, prueba de vida, biometría)**, bajo los mismos requerimientos de nivel medio. Para realizarlo debe ingresar al sistema utilizando su identificación digital de nivel alto antes de su vencimiento. ● **En forma remota automática (imagen del documento, prueba de vida, biometría y presentación del documento electrónico ICAO mediante NFC)**, bajo los mismos requerimientos de nivel medio. Para realizarlo debe ingresar al sistema utilizando su identificación digital de nivel medio o alto.

La siguiente tabla muestra los requerimientos para cada nivel de autenticación:

Nivel AE	Requerimientos
1 - Bajo	El usuario se identifica y valida su identidad utilizando un factor de autenticación (algo que sé, algo que soy o algo que tengo). En caso de utilizar una contraseña (algo que sé), debe ser una contraseña considerada fuerte. En forma opcional el sistema podrá disponer de un segundo factor de autenticación.
2 - Medio	Se habilitan dos tipos de autenticación: **1. Usuario y dos factores de autenticación:** El usuario de autentica utilizando dos factores de autenticación diferentes entre sí (algo que sé, algo que soy o algo que tengo). En caso de utilizar una contraseña debe ser una contraseña fuerte y como segundo factor alguna de las siguientes opciones: ● Código OTP por SMS ● Código OTP por Whatsapp o similar ● Código OTP por correo electrónico ● Código OTP mediante push a una app móvil ● Utilizar pasaportes digitales alineados al estándar ICAO mediante NFC ● Aplicación de autenticación compatible con TOTP previamente configurada ● Aplicación de autenticación que interactúe mediante código QR

	• Biometría: prueba de vida + biometría facial de una foto con la imagen del registro público. • Token físico (token TOTP) que genera un OTP compatible con TOTP previamente configurado. **2. Credenciales Verificables reconocidas y firmadas por un organismo competente.** A través de una Credencial Verificable desde la billetera digital en el teléfono móvil del titular, emitida y firmada por el organismo competente, interactuando mediante el protocolo OIDC4VP. En este caso, se envía la credencial verificable de identificación tal cual fue entregada y firmada por el organismo competente. Si la firma es válida y es la firma electrónica avanzada, cualificada o certificada del organismo habilitado según la lista de confianza del país, el sistema podrá confiar en los datos de identidad de la credencial.
3 - Alto	Se habilitan dos tipos de autenticación: **1. Basados en firma electrónica avanzada, cualificada o certificada de persona física o natural:** • Firma en la nube, utilizando una app móvil para autorizar e ingresar el PIN para permitir utilizar la clave privada en un HSM. • Firma en un dispositivo criptográfico como un token, smart card que podrá interactuar mediante contacto con el dispositivo mediante USB o en forma inalámbrica a través de un chip RFID mediante NFC y un protocolo que cifre el canal inalámbrico como PACE. • A través de una Presentación Verificable que incluye credenciales verificables emitidas y firmadas por organismos competentes. La Presentación Verificable deberá ser firmada con la firma electrónica avanzada, certificada o cualificada del titular (persona física o natural) o de la billetera digital utilizada (siempre y cuando sea válida según la política del país) y enviada al validador mediante el protocolo OIDC4VP. **2. Usuario y dos factores de autenticación considerados fuertes.** El usuario se autentica utilizando dos factores de autenticación diferentes entre sí (algo que sé, o algo que soy o algo que tengo) considerados fuertes. Como primer factor una contraseña fuerte y como segundo factor una de las siguientes opciones: • Aplicación de autenticación compatible con TOTP previamente configurada. • Aplicación de autenticación que interactúe mediante código QR • Biometría: prueba de vida + biometría facial de una foto con la imagen del registro público. • Token físico (token TOTP) que genera un OTP compatible con TOTP previamente configurado. • Utilizar pasaportes digitales alineados al estándar ICAO mediante NFC.

La siguiente tabla muestra un resumen de los niveles de seguridad (NID) en función del nivel de registro (RID) y el nivel de autenticación (AE):

Nivel de Seguridad (NID)		**Autenticación (AE)**			
		0 Pass débil	1 Pass Fuerte	2 Pass fuerte + 2FA	3 Certificado Digital o 2FA fuerte
Registro (RID)	0 No confirmado	-	-	-	-
	1 Correo o teléfono confirmado	-	Bajo	Bajo	-
	2 Identificación Validada	-	Bajo	Medio	-
	3 Validación biométrica y renovación	-	-	-	Alto

5. Aspectos normativos

Consentimiento del usuario

Protección de datos personales

6. Datos para la Identificación Digital

Los datos que se van a utilizar para identificar a cada usuario son los siguientes:

- Identificador:
    - Código de país según la norma ISO 3166-1, código alfa-2 (dos letras, ejemplo: ar, br, ch, py, pa, do, cr, uy, pe, etc).
    - Código de documento.
    - Número de documento.
- Primer nombre (obligatorio).
- Segundo nombre
- Primer apellido (obligatorio).
- Correo electrónico (obligatorio si no ingresa el número de teléfono).
- Número de teléfono celular incluyendo características del país (obligatorio si no ingresa el correo electrónico).
- Nivel de seguridad compuesto de 3 variables (ver estandarización de niveles):
    - RID: registro;
    - AE: autenticación;
    - NID: menor entre RID y AE.

Los datos anteriormente descritos, en la implementación del broker modelo se corresponderá de la siguiente forma:

La siguiente tabla describe el contenido del token JWT proporcionado, incluyendo sus claims estándar y personalizados.

Claim	**Descripción / Valores posibles**	**Obligatoriedad**	**Formato**	**Ejemplo**
sub	Identificador del sujeto global.	SI	código país – código documento – número documento	UY-CI-42907981-
ae	Nivel de autenticación. Los valores posibles son: 0, 1, 2, 3	SI	Integer	0
document_country	Código de país que emitió el documento del usuario según la norma ISO 3166 alfa-2	SI	String	UY

document_id	Número de documento sin incluir barras, separadores o puntos	SI	String	42907981
document_type	Código de documento	SI	String	CI
iss	Issuer (emisor del token)	SI	String	
nid	Nivel de Seguridad: 0, 1, 2 o 3	SI	Integer	1
rid	Nivel de Registro: 0, 1, 2 o 3	SI	Integer	1
given_name	Primer nombre del usuario autenticado	SI	String	Juan
middle_name	Segundo nombre del usuario autenticado	NO	String	Martín
sid	ID de sesión	SI	String	OOtZNDRTPpLR... 2-SA0wg
aud	Propósito de uso del token	SI	String	email
auth_time	Hora de autenticación	SI	Integer	
name	Nombre completo	NO	String	Juan Martín Perez
phone_number	Número de celular (incluyendo código del país)	NO	String	+506-223100
exp	Fecha de expiración del token	SI	Integer	1755611155
iat	Fecha de emisión del token	SI	Integer	1755609355
family_name	Primer apellido del usuario	SI	String	Perez
second_family_name	Segundo apellido del usuario	NO	String	Gómez

jti	JWT ID	SI	String	0b700e02-f1ac-4ccb-addb-3f51197ec0bc
email	Correo electrónico del usuario	SI	String	Juan.gomez@agesic.gub.uy

Ejemplo de token

```
{
  "sub": " UY-CI-42907981-",
  "ae": 3,
  "document": {
    "document_country": "UY",
    "document_id": "42907981",
    "document_type": " CI"
  },
  "iss": "http://localhost:8080",
  "nid": 1,
  "rid": 1,
  "given_name": "Juan",
  "middle_name": "Martín",
  "sid": "OOtZNDRTPpLR5D07bsdQ0Mj3LIqYoj4_LdvE2-SA0wg",
  "aud": "sp-client",
  "auth_time": 1755609343,
  "name": "Juan Martín Pérez Gómez ",
  "phone_number": "+506-223100",
  "exp": 1755611155,
  "iat": 1755609355,
  "family_name": "Perez",
  "second_family_name": "Gómez",
  "jti": "0b700e02-f1ac-4ccb-addb-3f51197ec0bc",
  "email": "juan.gomez@agesic.gub.uy"
}
```

7. Protocolos de Integración

El broker se debe integrar con tres tipos de sistemas (como se muestra en la figura al inicio del documento):

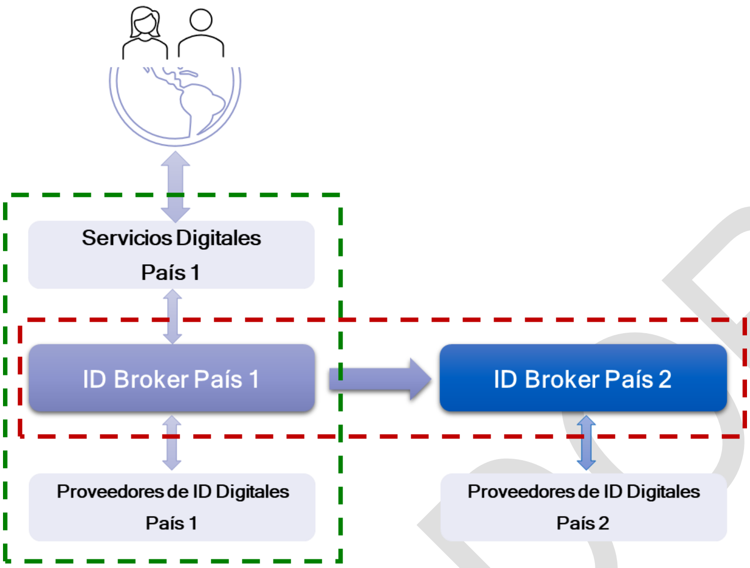
- **Servicios digitales** (SPs, Service Providers): para integrar a los servicios digitales del país se utilizará **OIDC (OpenID Connect)** según lo especificado en OpenID Foundation (https://openid.net/).
- **Proveedores de Identificaciones digitales** (IDPs, Identity Providers): para integrar a los proveedores de identificación habilitados por el país se podrán utilizar dos protocolos:
  - **OIDC (OpenID Connect)** según lo especificado en OpenID Foundation (https://openid.net/)
  - **OIDC4VP (OpenID Connect for Verifiable Presentations)** según lo especificado en OpenID Foundations (https://openid.net/sg/openid4vc/) para habilitar el uso de credenciales verificables para identificarse digitalmente en todo el ecosistema del broker.
- **Brokers de otros países** (identificación digital transfronteriza): para la integración transfronteriza se utilizará **OIDC (OpenID Connect)** según lo especificado en OpenID Foundation (https://openid.net/).

Adicionalmente el broker deberá cumplir con los siguientes requerimientos:

- El bróker asegurará el inicio de sesión unificado **(SSO – Single Sign-On)** a partir de la autenticación en cada proveedor de identificación.
- La estrategia de identificación digital de cada país, apoyada por el marco normativo definido, podrá habilitar la integración de servicios digitales privados, así como la integración de proveedores de identificación privados al broker nacional.
- Los servicios digitales integrados delegarán la autenticación de sus usuarios a través del bróker a los diferentes IdPs integrados y deberán desarrollar sistemas de autorización y auditoría específicos para su negocio, asumiendo que a sus servicios ingresarán personas físicas o naturales con un identificador universal, tal como se define en este modelo.
- Tanto los SPs como IdPs pueden ser sistemas web o aplicaciones móviles.

8. Controles de Seguridad Transfronterizos

A partir de la figura del capítulo 2, el ecosistema de identificación digital articulado por el broker de un país puede ser abordado desde dos puntos de vista: El ecosistema nacional y el regional. La siguiente imagen muestra esta situación:



En el ecosistema nacional (recuadro verde) pueden darse dos escenarios:

- Generalmente estos modelos federados no cargan ninguna decisión sobre el broker. Esto significa que una persona se identifica digitalmente en un proveedor integrado y vuelve al servicio digital original. En este flujo, el broker simplemente traspasa toda la información al servicio digital, entre otros: datos de la identidad de la persona y nivel de seguridad (nid, rid y ae). El servicio digital, a partir de la identidad de la persona y el nivel de seguridad de su identificación, utilizando el sistema de autorización, toma decisiones habilitando o no operaciones a determinadas funcionalidades, objetos y/o datos. En este escenario, el broker no toma ningún tipo de decisión.
- Una variante es, para servicios que solamente habiliten identificaciones intermedias o altas, el broker podría contar con una funcionalidad para deshabilitar los proveedores de identificación que no cumplan con estos requerimientos. De modo que, si un usuario accede al broker para identificarse en uno de estos servicios, el broker le presente los proveedores que cumplen con estas condiciones, evitando que la persona utilice un nivel de seguridad que luego el servicio no le permita realizar acciones.

A nivel regional (recuadro rojo), con el fin de fortalecer la identificación digital regional, reducir riesgos y motivar a las personas a utilizar identificaciones fuertes en confianza, el broker podría permitir solamente identificaciones altas cuando un usuario viene desde otro broker.

Ambos controles pueden ser parametrizables de modo que cada país defina cómo lo quiere implementar en su ecosistema nacional.

9. Términos

En proceso de realizar: un mapeo de términos clave para el modelo.

10. Anexo I – Lineamientos para pruebas de vida y biometría facial

Introducción

Con la amplia penetración de celulares inteligentes, el uso de la biometría facial se consolidó como una herramienta práctica y segura (bajo determinados lineamientos) para validar identidades en forma remota y cómoda para los usuarios.

Este apartado define en alto nivel algunas consideraciones relevantes que se deben cumplir para que se puedan utilizar herramientas biométricas para validar identidades.

Consideraciones básicas

A continuación, se definen una serie de requerimientos que se deben cumplir en todos los casos en lo que se utilice biometría facial:

1. Siempre antes de tomar la imagen para realizar la comparación biométrica se debe aplicar una prueba de vida con el fin de asegurar que la imagen que se está tomando es a una persona viva.
2. La comparación biométrica de la imagen tomada a la persona debe realizarse contra el registro público a través de una conexión segura entre el sistema de identificación digital y el del registro público. En algunos casos se podrá escanear un documento presentado por el usuario, es decir, utilizar la cámara del dispositivo para obtener la imagen de un documento y simplificar el ingreso de datos u obtener una foto facial de la persona. La comparación que se pueda realizar a la foto obtenida desde la carga de un documento no sustituya la comparación biométrica que debe realizarse entre la foto obtenida de la persona y el registro público.

Las consideraciones básicas deben cumplirse en todos los casos, a continuación, se presentan lineamientos para la prueba de vida y luego para la comparación biométrica facial.

Pruebas de Vida

Comparación Biométrica Facial

La biometría se puede definir como un conjunto de métodos o técnicas usadas para identificar un individuo a través de sus registros biológicos, tanto de naturaleza sean física o de comportamiento. En este apartado, nos referiremos siempre a la biometría facial como el método capaz de identificar o verificar a un sujeto a través de una imagen, vídeo o cualquier elemento audiovisual de su rostro. Esto se realiza generalmente mediante la comparación de vectores de imagen identificados previo almacenaje. Además, como se trata de validar la identidad de un individuo conocido, **solamente se considera la identificación 1:1**, es decir, comparar una fotografía facial de la persona, tomada en el momento, con su fotografía facial en el registro público.

Estos registros en su conjunto determinan el "ser" de un individuo, por tanto, pueden ser utilizados para la identificación. Para ello necesitamos cumplir con las siguientes características:

Principios de los registros Biométricos:

- **Universales:** Se pueden encontrar en todas las personas (excepto en aquellas con daños o faltantes).
- **Únicos:** Deben ser capaces de distinguir entre individuos dentro de los inscriptos.
- **Permanentes**: deben ser estables e invariables en el tiempo, con respecto a la coincidencia teniendo en cuenta las variaciones causadas por el ciclo de vida humano.
- **Medibles:** El sistema debe poder adquirirlos y digitalizarlos fácilmente.
- **Desempeño de manera efectiva:** Los sistemas a implementar Biometría deben ser precisos, rápidos y robustos, de modo que los cálculos matemáticos de comparación puedan ser ejecutados velozmente y de manera correcta.
- **Aceptables:** La biometría debe ser implementada de modo que los usuarios no la consideren perjudicial o intrusiva, satisfacer las normas y expectativas sociales y ser capaces de ser utilizados por un gran porcentaje de la población.
- **Seguros:** Los registros biométricos deben ser considerados como un dato de alto riesgo, ya que, en caso de vulnerabilidades en ellos, se puede generar la impersonalización llevando a una suplantación de identidad mediante el acceso no autorizado, usando varios artefactos y técnicas de sustitución de características.

La cara está comúnmente disponible y se adquiere fácilmente mediante captura próxima o remota. Pero estos están sujetos a desafíos particulares y restricciones técnicas que pueden resultar en Imágenes faciales de mala calidad. Tales imágenes afectan significativamente la probabilidad de detección correcta (o a la inversa el número de falsas aceptaciones generadas por el sistema). La calidad tanto de la foto de inscripción (la fotografía disponible en el registro civil) como de la foto tomada con una cámara puede tiene un impacto. Se pueden encontrar recomendaciones al respecto en la publicación "Formato de Datos para el Intercambio de Huella Dactilar, Facial & Otra información biométrica y Dispositivo de identificación móvil Recomendación de mejores prácticas" de NIST[1]. Los atributos de calidad específicos incluyen: iluminación, pose, posición de la cámara, expresión, cubiertas para la cabeza, anteojos, barbas, resolución (píxeles entre los ojos) y edad.

[1] Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information, Mobile ID Device Best Practice Recommendation, NIST: https://www.nist.gov/system/files/documents/itl/ansi/Approved-Std-20070427-2.pdf

Algunas de las vulnerabilidades comunes para la biometría facial son:

- **Fraude por semejanza:** un documento de identidad utilizado por alguien que se parece al genuino, sujeto pretendido. Esto permite que la persona en una lista de vigilancia afirme que no es el objetivo correcto si se detecta.
- **Máscaras**: están disponibles máscaras de látex avanzadas que son difíciles de detectar observación casual.
- **Maquillaje:** Cuando el deseo es evitar la detección, el uso correcto del maquillaje puede oscurecer rasgos faciales mientras se ven naturales para un observador humano.
- **Anteojos:** los anteojos oscuros o de montura gruesa pueden oscurecer una parte importante de los rasgos faciales. utilizado para el reconocimiento.
- **Comportamiento**: Si los objetivos sospechan que están siendo observados, el uso de un teléfono móvil y mirar hacia el suelo puede dificultar la obtención de una imagen de calidad.
- **Morphing:** Muestras biométricas (por ejemplo, imágenes de rostros) de dos o más donantes que se fusionan para permitir la verificación exitosa de cualquiera de los sujetos donantes contra la identidad "fusionada".

El uso de datos biométricos requiere del abordaje de varios temas importantes a nivel de cada país, que no son parte del alcance de este apartado:

- Gobernanza
- Privacidad
- Seguridad de datos, tanto en reposo como en tránsito
- Acceso al sistema
- Comprensión y gestión de cualquier diferencial algorítmico
- Gestión continua del rendimiento
- Auditabilidad
- Pruebas de rendimiento y eficacia

Requerimientos generales para la comparación biométrica facial:

- **Política de retención o eliminación de datos:** Debe estar alineada a la regulación vigente de protección de datos personales del país.
- **Procesamiento de datos:** Una organización responsable del procesamiento de datos debe designar un controlador de datos que será responsable de gestionar todas las actividades de procesamiento de datos, incluida la recopilación, el almacenamiento, el uso y borrado de los datos. El controlador de datos conserva la responsabilidad incluso si la función de procesamiento de datos se subcontrata a otras partes. Cualquier proveedor u operador externo debe estar sujeto a contratos que requieran un nivel muy alto nivel de seguridad y debe involucrar auditorías externas por parte de la agencia contratante y sanciones por incumplimiento de los requisitos de seguridad y privacidad del contrato.
- **Compartir datos:** Debe alinearse a la regulación vigente de protección de datos personales, que entiende como un dato guardado para un uso determinado y exclusivo explícito en un acuerdo de uso, contrato o política de términos y condiciones.
- **Coincidencia de datos**: el uso de algoritmos informáticos para determinar si la consulta plantilla coincide con la(s) plantilla(s) de la base de datos seleccionada(s). Las plantillas de consulta normalmente no son conservadas si se han comparado con una plantilla de referencia en la base de datos.

- **Salida**: la 'coincidencia' o 'no coincidencia' resultante respaldará la función del sistema general, por ejemplo, si el componente biométrico está diseñado para verificar una afirmación de identidad de aquellos en la base de datos con acceso legítimo a un edificio seguro, entonces una 'coincidencia' permitiría la entrada, basado en la verificación con la plantilla de identidades afirmadas, pero una 'no coincidencia' negaría entrada.
- **Persistencia de datos**: el sistema de identificación digital no deberá preservar las dos imágenes utilizadas para la comparación biométrica. Si podrá preservar ambos vectores y los hashes de ambos vectores, así como el grado de acierto y el algoritmo utilizado, como evidencia del resultado de la comparación biométrica.

Variables técnicas para tener en cuenta:

- **Tasa de aceptación real (TAR)**: la medida de la capacidad del sistema para hacer coincidir correctamente los atributos biométricos de identidad de la misma persona.
- **Tasa de falsa aceptación (FAR)**: la falsa aceptación se produce cuando la plantilla biométrica de consulta de una persona es emparejada por error por el sistema con la plantilla biométrica de otra persona en la base de datos. La FAR es el número de aceptaciones falsas como proporción del número total de consultas biométricas que deberían haber sido rechazadas, es decir, el número de no coincidencias generadas y presentados como coincidencias por el sistema como una proporción de verdaderas no coincidencias.
- **Tasa de rechazo verdadero (TRR)**: la medida del número de ocasiones en que la identidad biométrica atributo de una persona no coincide correctamente con los atributos de identidad biométrica de otros en la base de datos, es decir, la frecuencia de no coincidencias correctas.
- **Tasa de rechazo falso (FRR)**: el rechazo falso ocurre cuando la plantilla biométrica de consulta no está coinciden con la plantilla de base de datos correcta, aunque sean de la misma persona. el FRR es el número de falsos rechazos como proporción del número total de consultas biométricas que debería haber sido aceptado, es decir, el número de coincidencias generadas y presentadas como no coincidencias por el sistema como una proporción de coincidencias genuinas.

Ante la implementación y uso de registros biométricos faciales se debe tener en cuenta:

- **Detector de vida (prueba de vida):** La implementación de tecnología que permita detectar gestos y movimientos que prueben que detrás de una cámara hay un sujeto presente (previamente detallado en este apartado).
- **Cancelación de biometría**: Un atributo no puede cambiar más allá de un registro de poca calidad. El cambio de registros biométricos se recomienda sea ante supervisión humana.
- **Combinación de registros:** Ejemplo Biometría + Pasaporte como un registro combinado.
- **Base de datos de defraudadores faciales:** Registros que intenten cambiar o probar diferentes combinaciones de los mismos de modo frenético deberían ser bloqueados y guardados.

Tabla de niveles de seguridad para la adquisición de caras para perfil digital del NIST[2,3]:

Perfil de adquisición del sujeto	Nivel SAP
Perfil de adquisición desconocido [2015n>] u otra fuente no mencionada en esta tabla [<2015n]	0
Imagen facial de vigilancia	1
Imagen de la licencia de conducir (AAMVA)	10
Imagen facial frontal completa ANSI (*ANSI 385*)	11
Imagen facial del token ANSI (*ANSI 385*)	12
Imagen facial frontal completa ISO (I*SO/IEC 19794-5*)	13
Imagen facial ISO Token (*ISO/IEC 19794-5*)	14
Imagen facial PIV (*NIST SP 800-76*)	15
Mugshot heredado	20
Aplicación de mejores prácticas – Nivel 30	30
Práctica recomendada de MOBILE ID - Nivel 32	32
Aplicación de mejores prácticas – Nivel 40	40
Prácticas recomendadas de Mobile ID - Nivel 42	42
Aplicación de mejores prácticas – Nivel 50	50
Aplicación de mejores prácticas – Nivel 51	51
Prácticas recomendadas de Mobile ID - Nivel 52	52

Requerimientos para adquisición de imágenes a través de dispositivos móviles según NIST[4]:

Table 13 Mobile device face SAP levels

Captura	Comentarios	Niveles		
		32	42	52
Resolución de imagen	Resoluciones bajas disminuirán precisión	≥ 480 x 600	≥ 786 x 1024	≥ 2400 x 3200
Aparato con sensor de captura		Exploración progresiva (sin entrelazado)	Exploración progresiva (sin entrelazado)	Exploración progresiva (sin entrelazado)

[2] *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information ANSI/NIST-ITL 1-2011 NIST Special Publication 500-290 Edition 3:* **https://doi.org/10.6028/NIST.SP.500-290e3**
[3] Publicación: https://www.nist.gov/publications/data-format-interchange-fingerprint-facial-other-biometric-information-ansinist-itl-1-1
[4] *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information ANSI/NIST-ITL 1-2011 NIST Special Publication 500-290 Edition 3:* **https://doi.org/10.6028/NIST.SP.500-290e3**

Espectro de Color de dispositivo de captura		Mínimo de espacio de color RGB de 24 bits o un mínimo de espacio de color monocromo de 8 bits	Mínimo de espacio de color RGB de 24 bits o un mínimo de espacio de color monocromo de 8 bits	Mínimo de espacio de color RGB de 36 bits o un mínimo de espacio de color monocromo de 12 bits
Captura	**Comentarios**	**Niveles**		
		32	**42**	**52**
Controles de dispositivo de captura		Ganancia automática y obturador automático, opcional: bucle de control para el parámetro de la cámara (velocidad de obturación / intensidad del flash) basado en el área de la cara a bordo	Ganancia automática y obturador automático, opcional: bucle de control para el parámetro de la cámara (velocidad de obturación / intensidad del flash) basado en el área de la cara a bordo (requiere detección continua de la cara)	Ganancia automática y obturador automático, opcional: bucle de control para el parámetro de la cámara (velocidad de obturación / intensidad del flash) basado en el área de la cara a bordo (requiere detección continua de la cara)
Distancia de captura en cm	Las distancias cortas reducen la precisión	60-200 cm (~ 2 – 6 pies), se prefiere la distancia más larga	60-200 cm (~ 2 – 6 pies), se prefiere la distancia más larga	60-200 cm (~ 2 – 6 pies), se prefiere la distancia más larga
Tipo de iluminador: función opcional		Xenon flash o LED / fill-in flash	Xenon flash o LED / fill-in flash	Xenon flash o LED / fill-in flash
Luz ambiente	Nivel mínimo de luz al que se requiere el flash	4 lux	4 lux	4 lux
Rango de longitud de onda		Luz visible 380-780 nm	Luz visible. 380-780 nm	Luz visible 380-780 nm
Tiempo de exposición	Capacidad para congelar el movimiento	≤ 1/100s (10 ms)	≤ 1/100s (10 ms)	≤ 1/100s (10 ms)
Distancia entre los centros oculares	Una resolución más baja puede reducir la precisión	≥ 90 pixeles	≥ 150 pixeles	≥ 300 pixeles
Fotos por segundo	Para posicionamiento (vista en vivo)	≥ 12 fps	≥ 12 fps	≥ 12 fps

Tabla de captura de datos biométricos faciales de "*Mobile ID Device Best Practice Recommendation Version 2.1*" (se destacan los lineamientos adicionales a la tabla anterior), NIST[5]:

Table 6 Mobile ID Still-Frame Photographic Requirements

Factor	Comentarios
Distancia de captura en cm	60-200 cm (~ 2 – 6 pies), se prefiere la distancia más larga
Rango de longitud de onda	Luz visible. 380-780 nanometros

Mobile Device Face Subject Acquisition Profile (SAP)levels (se resalta en negrita la información que no se encuentra en la tabla anterior)

Captura	Comentarios	Niveles		
		32	42	52
Espectro de colores en dispositivo de captura		Mínimo de espacio de color RGB de 24 bits o un mínimo de espacio de color monocromo de 12 bits	Mínimo de espacio de color RGB de 24 bits o un mínimo de espacio de color monocromo de 12 bits	Mínimo de espacio de color RGB de 36 bits o un mínimo de espacio de color monocromo de 12 bits
Resolución	Resoluciones bajas reducen precisión	≥ 480 x 600	≥ 786 x 1024	≥ 2400 x 3200
Controles del dispositivo de captura		Ganancia automática y obturador automático, opcional: bucle de control para el parámetro de la cámara (velocidad de obturación / intensidad del flash) basado en el área de la cara a bordo	Ganancia automática y obturador automático, opcional: bucle de control para el parámetro de la cámara (velocidad de obturación / intensidad del flash) basado en el área de la cara a bordo (requiere detección continua de la cara)	Ganancia automática y obturador automático, opcional: bucle de control para el parámetro de la cámara (velocidad de obturación / intensidad del flash) basado en el área de la cara a bordo (requiere detección continua de la cara)
Composición de la foto	Pose de la persona	'Cabeza' o 'Cabeza y hombros'	Al menos una imagen frontal completa de 'Cabeza y hombros'	Al menos una imagen frontal completa de 'Cabeza y hombros'
Proporción Horizontal-Vertical		4:5	3:4	3:4

[5] Captura de datos biométricos faciales, NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-280v2.1.pdf

Captura	Comentarios	Niveles		
		32	42	52
Algoritmo de Compresión		JPEG. Relación de compresión máxima 15:1 para la región de interés que comprende la piel expuesta de la cara, desde la corona hasta la barbilla de oreja a oreja. La porción no facial de la imagen puede comprimirse hasta una ración de 120:1. La mejor práctica es aplicar compresión sin pérdidas a la imagen frontal con las orejas visibles.	JPEG 2K. Relación de compresión máxima 15:1 para la región de interés que comprende la piel expuesta de la cara, desde la corona hasta la barbilla de oreja a oreja. La porción no facial de la imagen puede comprimirse hasta una ración de 120:1. La mejor práctica es aplicar compresión sin pérdidas a la imagen frontal con las orejas visibles.	JPEG 2K. Relación de compresión máxima 15:1 para la región de interés que comprende la piel expuesta de la cara, desde la corona hasta la barbilla y de oreja a oreja. La porción no facial de la imagen puede comprimirse hasta una ración de 120:1. La mejor práctica es aplicar compresión sin pérdidas a la imagen frontal con las orejas visibles.
Distancia entre los centros oculares	Menor distancia reduce precisión	≥ 90 pixeles	≥ 150 pixeles	≥ 300 pixeles

Resoluciones

Esta categoría es aplicable a FAP, PAP y TAP. La resolución de las imágenes deberá ser 500 píxeles por pulgada (ppi) o 1000 ppi. Se permite una pequeña variación alrededor de estos dos valores Para dispositivos con certificación PIV, se permite un nivel de tolerancia del 2 % para dispositivos de 500 ppp. Para los dispositivos certificados del Apéndice F, se permite una desviación máxima del 1% de 500 o 1000 pp.

Algoritmo de compresión

Si se comprimen, las imágenes de crestas de fricción capturadas a 500 ppp deben usar Wavelet Scalar Algoritmo de cuantificación (WSQ) para la compresión antes de la transmisión y/o el almacenamiento. Se deben usar platinas de 3,2" x 1,5" o más grandes, WSQ versión 3.1 o superior. Versiones anteriores de WSQ no se adaptan a imágenes más grandes y puede fallar en el manejo adecuado de datos alrededor del borde del área de captura.

Las especificaciones de WSQ están contenidas en *WSQ Gray-scale* Especificación de compresión de imágenes de huellas dactilares, octubre de 2010. Imágenes de crestas de fricción capturado a 1000 ppi utilizará el Grupo Conjunto de Expertos Fotográficos (JPEG) 2000 algoritmo de compresión previo a la transmisión y/o almacenamiento. esto debe estar en de acuerdo con el formato JP2 como se describe en ISO 15444-1.

La publicación especial NIST 500- 289, la guía de compresión para imágenes *Friction Ridge* de 1000 ppp15 proporciona orientación sobre cómo realizar estas compresiones. Algunos sistemas pueden aceptar y procesar sólo imágenes de 500 ppp. Por lo tanto, si un dispositivo móvil captura imágenes a 1000 ppi, la imagen es posible que deba convertirse a 500 ppp antes de la transmisión. Esta conversión será realizada de acuerdo con la guía en "Examen de estrategias de reducción de muestreo para conversión de imágenes de huellas dactilares de 1000 ppp a 500 ppp, *NISTIR 7839*

Índice de compresión

Si una imagen se comprime en exceso, pierde características destacadas que pueden ser útiles para pareo. NIST realizó estudios sobre compresión de imágenes 17 que analizaron los niveles de compresión. Para imágenes pequeñas (más pequeñas que 1,6" x 1,5"), se especifica una compresión de 10:1 a 500 ppp. Para platinas más grandes que capturan a 500 ppp, se especifica una proporción de 15:1. Sin embargo, a 1000 ppp, todos los tamaños de platos deben usar una proporción de 10:1.

11. Anexo II – Mapeo entre IdLAC y los principales modelos de referencia (ISO/IEC 29115, eIDAS y NIST SP 800-63-06)

PENDIENTE

ISO/IEC 29115, Marco de Aseguramiento de Autenticación de Entidades: norma internacional que establece cuatro niveles de aseguramiento para la autenticación (*International Organization for Standardization*, 2013, revisada en 2020, https://www.iso.org/es/contents/data/standard/04/51/45138.html).

eIDAs, Identificación Electrónica y Servicios de Confianza: marco normativo de la Unión Europea donde la identificación digital está enmarcada dentro de un grupo de servicios de confianza con fuerte foco en la interoperabilidad. European Digital Identity Framework (mayo de 2024): https://www.european-digital-identity-regulation.com/

Directrices del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST): pautas y recomendaciones emitidos por el NIST de la serie SP 800-63-4 agosto de 2025: https://pages.nist.gov/800-63-4/

ISO/IEC 29115	eIDAS	NIST SP 800-63-3
Nivel 1 – IAL1: Baja o confianza nula sobre la identidad. Métodos de autenticación sencillos como nombre de usuario/contraseña. **Nivel 2 – IAL2:** Poca confianza sobre la identidad basado en documentos oficiales y controles básicos. Dos factores de autenticación (contraseña fuerte y OTP o app). **Nivel 3 – IAL3:** Alta confianza sobre la identidad, verificación basada en documentos oficiales y biometría fuerte. Métodos de autenticación multifactorial (contraseña + token físico, criptografía o FIDO2). **Nivel 4 – IAL4:** Muy alta confianza sobre la identidad, verificada presencialmente con múltiples elementos. Métodos de autenticación multifactorial robustos con dispositivos criptográficos (hardware) con controles cruzados con fuentes fiables.	**Nivel 1 _ Bajo:** Mínima confianza sobre la identidad. Datos autodeclarados con verificaciones simples. Autenticación simple (usuario / contraseña) con segundo factor opcional. **Nivel 2 - Sustancial:** Confianza elevada, verificación mediante documentos oficiales y/o biometría. Al menos un segundo factor de autenticación. Procedimientos formales de revocación, auditorías, monitoreo, etc. **Nivel 3 - Alto:** Confianza muy alta, verificación presencial o biométrica con pruebas de vida. Autenticación con chips criptográficos según FIDO2.	Verificación de la ID: **IAL1:** Autodeclarada, no hay verificación de la identidad. **IAL2:** Remota o presencial en base a documentos oficiales y controles automáticos con biometría. **IAL3:** Verificación presencial con controles físicos y biometría fuerte. Autenticación: **AAL1**: Factor único. **AAL2:** Dos factores de autenticación distintos y fuertes. **AAL3:** Autenticación con hardware criptográfico, protección y múltiples factores.