Traducido: *Francisco Javier González García*

Tecnología de Identificación Digital

Traducido: *Francisco Javier González García*

Contenido

Traducido: *Francisco Javier González García*

Cifras

Traducido: *Francisco Javier González García*

Acerca de ID4D

La iniciativa Identificación para el Desarrollo (ID4D) del Grupo del Banco Mundial utiliza el conocimiento y la experiencia global en todos los sectores para ayudar a los países a darse cuenta del potencial transformador de los sistemas de identificación digital para alcanzar los Objetivos de Desarrollo Sostenible. Opera en todo el Grupo del Banco Mundial con prácticas y unidades globales que trabajan en desarrollo digital, protección social, salud, inclusión financiera, gobernanza, género, legal, entre otros.

La misión de ID4D es permitir que todas las personas accedan a los servicios y ejerzan sus derechos, aumentando el número de personas que cuentan con una identificación segura, verificable y oficialmente reconocida. ID4D hace que esto suceda a través de sus tres pilares de trabajo:

> Liderazgo de pensamiento y análisis para generar evidencia y llenar los vacíos de conocimiento;
> Plataformas globales y convocatorias para ampliar las buenas prácticas, colaborar y crear conciencia; y
> Compromiso nacional y regional para brindar asistencia financiera y técnica para la implementación de sistemas de identificación digital sólidos, inclusivos y responsables que estén integrados con el registro civil.
> El trabajo de ID4D es posible gracias al apoyo del Grupo del Banco Mundial, la Fundación Bill y Melinda Gates, el Gobierno del Reino Unido, el Gobierno de Australia y la Red Omidyar. Para obtener más información sobre ID4D, visite bancomundial.org/id4d.

Expresiones de gratitud

Este informe se preparó como parte de la iniciativa Identificación para el Desarrollo (ID4D), el esfuerzo intersectorial del Grupo del Banco Mundial para apoyar el progreso hacia los sistemas de identificación utilizando soluciones del siglo XXI. Fue posible gracias al generoso apoyo de Digital Impact Alliance (DIAL) y los socios del Fondo Fiduciario de Donantes Múltiples ID4D (Fundación Bill & Melinda Gates y Omidyar Network).

El equipo de Accenture que contribuyó a este documento como autores o revisores incluye a: Dan Bachenheimer, Dan Baker, Sebabrata Banerjee, Craig Chatfield, Ilkka Hyvonen, Akshay Iyer, Mrinal Jha, Suneeta Kudaravalli, Christine Leong, Sabareesh Madhav, Rahul Malik, Nilanjan Nath, Juhi Saxena, Luca Schiatti y Srijan Singh.

Este informe se benefició enormemente de los aportes de Anita Mittal y las revisiones del personal del Grupo del Banco Mundial, incluidos Seth Ayres, Luda Bujoreanu, Susan David Carevic, Kamya

Traducido: *Francisco Javier González García*

Chandra, Tina George, Jonathan Marskell, Anna Zita Metz y David Satola bajo la supervisión de Vyjayanti. Desai.

Los hallazgos del informe se basan en la investigación, las consultas y las evaluaciones detalladas de las tecnologías de identificación y autenticación a fines de 2017. Como resultado, la información que se presenta aquí representa una instantánea de las tecnologías en el momento en que se escribió el informe y es posible que no refleje desarrollos recientes.

El informe no habría sido posible sin las opiniones y revisiones del Dr. Joseph Atick, ID4Africa & Identity Counsel; Jérôme Buchler, identificación HSB; Dasha Cherepennikova, Identidad mundial única; Sanjay Dharwadker, CMI; Rebecca Distler, Elemento Inc; Alan Gelb, Centro para el Desarrollo Global; Marta Ienco, GSMA; Sanjay Jain, iSprit; Brett McDowell, Alianza FIDO; Mónica Monforte, GSMA; C. Maxine Most, inteligencia de mercado de Acuity; Wameek Noor, DIAL; Adam Perold, Elemento Inc; Kris Ranganath, NEC; Yiannis Theodorou, GSMA; Don Thibeau, El Intercambio Abierto de Identidad; Colin Wallis, Iniciativa Kantara; Anne Wang, Gemalto; Dr. Jim Wayman, Universidad Estatal de San José (Director del Programa de Investigación de Identificación Biométrica); Matt Wilson, GSMA; y Jeff Wishnie, DIAL.

Términos y definiciones clave

Autenticación:El proceso de probar una identidad. Ocurre cuando los sujetos proporcionan las credenciales adecuadas, a menudo como requisito previo para recibir acceso a los recursos.[1]

Biometría:Una característica física medible o un rasgo de comportamiento personal utilizado para reconocer la identidad de un solicitante o verificar su identidad reclamada. Las imágenes faciales, las huellas dactilares y las muestras de escaneo del iris son ejemplos de biometría.[2]

Credencial:Un objeto o estructura de datos que vincula con autoridad una identidad, a través de un identificador o identificadores, y (opcionalmente) atributos adicionales, a al menos un autenticador poseído y controlado por un suscriptor.[3]

Deduplicación:En el contexto de los sistemas de identificación, es una técnica para identificar copias duplicadas de datos de identidad. Los datos biométricos, incluidas las huellas dactilares y los escaneos de iris, se utilizan comúnmente para desduplicar identidades a fin de identificar afirmaciones de identidad falsas o inconsistentes y establecer la singularidad.

Identificación digital:El proceso de validación de los atributos y características de una persona, incluida la singularidad, para establecer su identidad digital.[4]

Identidad digital:La terminología utilizada a lo largo de este documento para referirse a un conjunto de atributos y credenciales capturados y almacenados electrónicamente que pueden identificar de manera única a una persona.[5]

Traducido: *Francisco Javier González García*

Sistema de identificación fundacional:Sistema de identificación creado para la administración pública general y la identificación, incluidos los registros civiles, las cédulas de identidad y los registros nacionales de población. Puede servir como base para una amplia variedad de transacciones públicas y privadas, servicios y credenciales de identidad derivadas. Los ejemplos comunes incluyen identificaciones digitales o registros civiles.

Sistema de identificación funcional:Sistema de identificación creado en respuesta a una demanda de un servicio o transacción en particular. Puede emitir credenciales de identidad tales como identificaciones de votantes, registros de salud y seguros y tarjetas bancarias. Estos pueden ser comúnmente aceptados para propósitos de identificación más amplios, pero no siempre otorgan identidad legal.

Identificación:La determinación de la identidad y el reconocimiento de quién es una persona; la acción o proceso de determinar qué es una cosa; o el reconocimiento de una cosa como siendo lo que es.

Identidad:Un conjunto único de rasgos y características que individualizan a una persona, incluidos los atributos biográficos y biométricos.

Darril (diciembre de 2011).*Identificación, autenticación y autorización*. Obtenga la certificación Get Ahead Obtenido de:http://blogs.getcertifiedgetahead.com/identification-authentication-authorization/

Richard Kissel (mayo de 2013).*Glosario de términos clave de seguridad de la información*. NIST Obtenido de:http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Grassi, P.A., Fenton, J.L., et al. (junio de 2017).*Pautas de identidad digital*. NIST Obtenido de:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Banco Mundial (2016).*Identidad digital: hacia principios compartidos para la cooperación entre los sectores público y privado (inglés)*. Grupo del Banco Mundial. Obtenido de:https://openknowledge.worldbank.org/bitstream/handle/10986/24920/Digital0identi0e0sector0cooperation.pdf?sequence=1&isAllowed=y

Banco Mundial (2016).*Identidad digital: hacia principios compartidos para la cooperación entre los sectores público y privado (inglés)*. Grupo del Banco Mundial. Obtenido de:https://openknowledge.worldbank.org/bitstream/handle/10986/24920/Digital0identi0e0sector0cooperation.pdf?sequence=1&isAllowed=y

Protocolo:Conjunto de reglas y formatos, semánticos (significado) y sintácticos (formato), que permiten a los sistemas de información intercambiar información.[6]

Revocación:El proceso de finalización prematura del período operativo de un certificado o credencial vigente en una fecha y hora específicas.[7]

Usuario:Proceso individual o (del sistema) autorizado para acceder a un sistema de información.[8]

Verificación:Confirmación y establecimiento de un vínculo entre una identidad reclamada y la persona viva real que presenta la evidencia.

Traducido: *Francisco Javier González García*

Richard Kissel (mayo de 2013).*Glosario de términos clave de seguridad de la información.*NIST Obtenido de:http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Richard Kissel (mayo de 2013).*Glosario de términos clave de seguridad de la información.*NIST Obtenido de:http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Richard Kissel (mayo de 2013).*Glosario de términos clave de seguridad de la información.*NIST Obtenido de:http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Grassi, PA, Fenton, JL, et al. (junio de 2017).*Pautas de identidad digital.*NIST Obtenido de:https://pages.nist.gov/800-63-3/sp800-63a.html

abreviaturas

Nivel de garantía del autenticador AAL

IA Inteligencia Artificial

Interfaz de programación de aplicaciones API

BN mil millones

Sistema biométrico BSoC en tarjeta

Documento Nacional de Identidad Informatizado CNIC

Lista de revocación de certificados CRL

Proveedor de servicios de credenciales de CSP

Tecnología de contabilidad distribuida DLT

Ácido desoxirribonucleico de ADN

DNI Documento Nacional de Identidad

Electrocardiografía ECG

eID Identificación Electrónica

Traducido: *Francisco Javier González García*

---

eIDAS Identificación Electrónica, Autenticación y Servicios de Confianza EMS Enterprise Mobility + Security

EMV Europay, MasterCard y Visa

UE Unión Europea

Tasa de falsa aceptación FAR

FIDO Identidad rápida en línea

Tasa de rechazo falso de FRR

FTE Incumplimiento de inscripción

Sistema global GSM para móviles

Asociación móvil del grupo especial GSMA

Protocolo de transferencia de hipertexto HTTP

Nivel de garantía de identidad de IAL

OACI Organización de Aviación Civil Internacional

DNI Identificación

ID4D Identificación para el Desarrollo

Grupo de trabajo de ingeniería de Internet del IETF

Base de datos en memoria de IMDB

IoT Internet de las cosas

ISO Organización Internacional para la Estandarización

KYC Conozca a su cliente

Análisis discriminante lineal LDA

MN millones

MRTD Documento de viaje de lectura mecánica

Zona de lectura mecánica de MRZ

N/A No aplicable

Traducido: *Francisco Javier González García*

Base de datos nacional y autoridad de registro de NADRA

Comunicación de campo cercano NFC

NIR infrarrojo cercano

Instituto Nacional de Estándares y Tecnología del NIST

Autorización abierta de OAuth

Reconocimiento óptico de caracteres OCR

Contraseña de un solo uso de OTP

Análisis de componentes principales de PCA

PII Información de identificación personal PIN Número de identificación personal

Verificación de identidad personal PIV

Infraestructura de clave pública de PKI

Respuesta rápida QR

Memoria RAM de acceso aleatorio

RF radiofrecuencia

Llamada de función remota RFC

Identificación por radiofrecuencia RFID

RSA Rivest-Shamir-Adleman

Software SaaS como servicio

Kit de desarrollo de software SDK de lenguaje de marcado de aserción de seguridad SAML

Módulo de identificación de suscriptor SIM Servicio de mensajes cortos SMS

Módulo de plataforma segura de TPM

Marco de autenticación universal UAF Frecuencia ultra alta UHF

Interfaz de usuario de la interfaz de usuario

Traducido: *Francisco Javier González García*

Bus serie universal USB

USD dólares estadounidenses

1. Introducción

Los sistemas de identificación robustos, inclusivos y responsables pueden aumentar el acceso a las finanzas, la atención médica, la educación y otros servicios y beneficios críticos. Los sistemas de identificación también son clave para mejorar la eficiencia y permitir la innovación de los servicios de los sectores público y privado, como una mayor eficiencia en la provisión de redes de seguridad social y la facilitación del desarrollo de economías digitales. Sin embargo, el Banco Mundial estima que más de 1.100 millones de personas no tienen prueba oficial de su identidad. Las nuevas tecnologías brindan a los países la oportunidad de superar los sistemas basados en papel y establecer rápidamente una sólida infraestructura de identificación. Como resultado, los países están adoptando cada vez más programas de identificación digital (ID) a nivel nacional y aprovechándolos en otros sectores.

Ya sea que un país esté mejorando los sistemas de identificación existentes o implementando nuevos sistemas desde cero, las opciones tecnológicas son fundamentales para el éxito de los sistemas de identificación digital. Están surgiendo una serie de nuevas tecnologías para permitir varios aspectos del ciclo de vida de la identificación. Para algunas de estas tecnologías, no se han realizado estudios a gran escala; para otros, la especulación actual dificulta las evaluaciones objetivas.

Este informe es un primer intento de desarrollar una descripción completa del panorama tecnológico actual para la identificación digital. Su objetivo es servir como marco para comprender la miríada de opciones y consideraciones de tecnología en esta agenda que avanza rápidamente y de ninguna manera pretende brindar asesoramiento sobre tecnologías específicas, particularmente dado que hay una serie de otras consideraciones y contextos de países que necesitan ser considerados. Este informe tampoco recomienda el uso de una determinada tecnología de un proveedor en particular para ninguna aplicación en particular.

Si bien algunas tecnologías son relativamente fáciles de usar y asequibles, otras son costosas o tan complejas que su uso a gran escala presenta desafíos abrumadores. Este informe brinda a los profesionales una descripción general de varias tecnologías y avances que son especialmente relevantes para los sistemas de identificación digital. Destaca los principales beneficios y desafíos asociados con cada tecnología. También proporciona un marco para evaluar cada tecnología según múltiples criterios, incluido el tiempo que ha estado en uso, su facilidad de integración con sistemas heredados y futuros, y su interoperabilidad con otras tecnologías.

Se recuerda a los profesionales y partes interesadas que lean esto que tengan en cuenta que las tecnologías asociadas con los sistemas de identificación están evolucionando rápidamente y que este informe, preparado a principios de 2018, es una instantánea en el tiempo. Por lo tanto, es

Traducido: *Francisco Javier González García*

---

posible que las limitaciones y los desafíos tecnológicos que se destacan hoy en este informe no sean aplicables en los años venideros.

El informe comprende las siguientes secciones:

·**Sección 1 Introducción.**La Introducción establece el contexto y describe los desafíos tecnológicos que los profesionales y las partes interesadas pueden tener que abordar al evaluar o implementar sistemas de identificación digital. La lista de desafíos no es exhaustiva, pero aborda los conocimientos adquiridos a partir de la implementación de sistemas de identificación digital en diferentes países del mundo. La lista de desafíos

Banco Mundial (2017).*Identificación para el Desarrollo*. Obtenido del Banco Mundial:http://www.worldbank.org/en/programs/id4d

Banco Mundial (2015).*Enfoque de Integración de Identificación para el Desarrollo (ID4D)*. Obtenido del Banco Mundial:http://pubdocs.worldbank.org/en/205641443451046211/ID4D-IntegrationApproachStudyComplete.pdf

también se ha enmarcado en el contexto de los países en desarrollo que a menudo tienen poblaciones en rápido crecimiento y presupuestos limitados para sistemas de identificación.

·**Sección 2: Comprender el ciclo de vida de la identidad.**Esta sección agrupa el proceso de identidad en sus pasos principales y explica brevemente los subprocesos en cada paso. También proporciona el marco para una discusión sobre cómo las diferentes tecnologías pueden permitir diferentes etapas del ciclo de vida de la identificación.
·**Sección 3: Introducción al marco de evaluación de tecnología.**Esta sección detalla los parámetros utilizados para evaluar las tecnologías, incluida la madurez, el rendimiento, la escalabilidad, la adopción, la seguridad y la asequibilidad. Cada parámetro tiene múltiples subparámetros, y estos se califican en una escala de 3 puntos de alto, medio o bajo. La sección también enumera las tecnologías evaluadas utilizando este marco y los pasos del ciclo de vida de la identidad que pueden habilitar o afectar.
·**Secciones 4 a 6**: Estos proporcionan una descripción general de cada tecnología examinada a través del marco de evaluación y destacan los desafíos que la tecnología podría resolver, los desafíos que no resuelve y los nuevos desafíos que podría presentar su adopción. A través de estos análisis, los profesionales pueden comprender mejor las consideraciones clave involucradas en la elección de tecnologías de identificación digital.
·**Sección 7: Otras Consideraciones.**Esta sección final describe algunas consideraciones importantes que los profesionales deben tener en cuenta al elegir la tecnología.
El objetivo principal del informe es evaluar las tecnologías relacionadas con el ciclo de vida de la identificación digital. Sin embargo, esto de ninguna manera implica que la tecnología sea la única o la consideración más crítica para los profesionales que buscan maximizar los beneficios de los sistemas de identificación mientras mitigan los riesgos. Los “Principios de identificación para el desarrollo sostenible: hacia la era digital” destacan una variedad de consideraciones críticas. Estos Principios han sido respaldados por más de 20 organizaciones y se enumeran brevemente a continuación para beneficio de los lectores.

Principios

Traducido: *Francisco Javier González García*

Inclusión

3. Garantizar la cobertura universal para las personas desde el nacimiento hasta la muerte, sin discriminación
4. Eliminar las barreras de acceso y uso y las disparidades en la disponibilidad de información y
   tecnología

Diseño

3. Establecer una identidad robusta, única, segura y precisa
4. Crear una plataforma que sea interoperable y que responda a las necesidades de varios usuarios.
5. Uso de estándares abiertos y garantía de neutralidad tecnológica y de proveedores
6. Proteger la privacidad y el control del usuario a través del diseño del sistema
7. Planificación para la sostenibilidad financiera y operativa sin comprometer la accesibilidad

Gobernancia

8. Salvaguardar la privacidad de los datos, la seguridad y los derechos de los usuarios a través de un marco legal y regulatorio integral

El Banco Mundial (febrero de 2017).*Principios de Identificación para el Desarrollo Sostenible: Hacia la Era Digital.*El Banco Mundial. Obtenido de:http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples.pdf

9. Establecer mandatos institucionales claros y rendición de cuentas

10. Hacer cumplir los marcos legales y de confianza a través de la supervisión independiente y la adjudicación de quejas

Una discusión detallada de estos principios se encuentra en el informe del Banco Mundial titulado Principios de Identificación para el Desarrollo Sostenible: Hacia la Era Digital.

Aunque este informe se centra en las tecnologías, la iniciativa Identificación para el Desarrollo del Banco Mundial está trabajando en los temas enumerados en los Principios. Por ejemplo, dada la importancia de los estándares abiertos e interoperables para una plataforma de identificación digital segura y eficiente para la prestación efectiva de servicios, se está trabajando más en los estándares. Un informe titulado *Normas Técnicas de Identidad Digital*, preparado en 2017.

Además, el surgimiento de nuevas tecnologías digitales y el aumento de una cantidad de actores estatales y no estatales que utilizan esas tecnologías para la recopilación, el almacenamiento y el procesamiento de datos de y sobre las personas plantea una serie de problemas de protección de datos, privacidad, y cuestiones de consentimiento que deben considerarse como parte del diseño e implementación de sistemas de identificación digital. Los Principios anteriores incluyen la protección

de la privacidad del usuario (en el diseño) y la protección de la privacidad, la seguridad y los derechos del usuario de los datos (en el gobierno de un sistema).

Los regímenes de privacidad y protección de datos establecen derechos y obligaciones predecibles con respecto al tratamiento de datos individuales e información de identificación personal (PII) que son una parte importante para establecer confianza en los sistemas digitales, confianza que luego fomenta el uso.Dada la importancia de esta agenda, y para ayudar a los países a identificar brechas en el marco legal y regulatorio para la privacidad, la protección de datos y la inclusión, la iniciativa ID4D está desarrollando la herramienta ID Enabling Environment Assessment (IDEEA) que se implementará en varios países en 2018. .

Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU. (junio de 2017).*Pautas de identidad digital: inscripción y prueba de identidad*. Obtenido de NIST:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

Véase Digital Dividends, The World Development Report 2016, en la página 222 y siguientes, Banco Mundial; disponible en:http://www .worldbank.org/en/publication/wdr2016

2. Comprender el ciclo de vida de la identidad

El ciclo de vida de la identidad, como su nombre lo indica, no es un evento de una sola vez; más bien, es un proceso que comienza cuando una persona solicita una identificación digital y finaliza cuando se elimina el registro y la identificación se invalida debido a la muerte, la solicitud de eliminación por parte del individuo o algún otro evento. Las tecnologías relacionadas con la autorización no están dentro del alcance de este informe y, por lo tanto, no se analizan en las secciones siguientes.

2.1. Registro (Prueba de Identidad)

El aspecto fundamental de la identidad de una persona se establece durante el proceso de registro, cuando un solicitante proporciona evidencia de su identidad a la autoridad emisora de credenciales. (Consulte "Términos y definiciones clave" para obtener la definición de *credencial*.) Si la persona se identifica de manera confiable, la autoridad puede afirmar esa identidad con un cierto nivel de seguridad de identidad. En los países en desarrollo, y en casos como los de personas desplazadas o refugiadas, no es raro que los solicitantes carezcan de documentos fundamentales (nacimiento

Las terminologías utilizadas en este marco se alinean con los estándares NIST y la literatura ID4D existente publicada por el Banco Mundial.

Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU. (junio de 2017).*Pautas de identidad digital: inscripción y prueba de identidad*. Obtenido de NIST:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

certificado, pasaporte, factura de servicios públicos, permiso de conducir). Y en algunas situaciones, incluso si alguna forma de documento de identidad (típicamente, un documento de criador, como un certificado de nacimiento) está disponible, es posible que no sea confiable. En tales situaciones, los sistemas de identificación pueden utilizar un introductor quien tiene la tarea de verificar la identidad y la dirección del solicitante. Una vez que se completa la verificación, el registro biométrico y la eliminación de duplicados vincularán al solicitante con su reclamo de identidad, que luego se utilizará durante las interacciones de identidad posteriores.

Idealmente, un sistema de identificación digital debería integrarse con el registro civil, que es el registro oficial de nacimientos, defunciones y otros eventos vitales, incluidos matrimonios, defunciones, divorcios, nulidades, separaciones, adopciones, legitimaciones y reconocimientos.[19] Lo que esto significa en la práctica es que el registro de una persona en el sistema de identificación digital y su número de identificación único se generan primero mediante el registro de su nacimiento. El sistema de identificación digital es notificado de la muerte de una persona tan pronto como sea posible después del registro de la muerte. Además de promover la cobertura y la sostenibilidad de un sistema de identificación digital, esta integración brinda la oportunidad de producir estadísticas vitales en tiempo real, como sobre población, fertilidad y mortalidad.

El registro puede comenzar con ***Resolución***, el proceso de distinguir de manera única a un individuo en una población o contexto determinado. El primer paso en la resolución es la preinscripción. Aquí, el solicitante proporciona a la autoridad emisora información biográfica, documentos de criador (como certificados de nacimiento, certificados de matrimonio y documentos de la seguridad social) y fotografías. El solicitante puede presentarlos personalmente o proporcionar la información en línea o fuera de línea. A esto le sigue la inscripción, que generalmente se realiza en persona, por lo que la autoridad de registro puede validar y aumentar la información previa a la inscripción según sea necesario.

Se requiere prueba en persona para el nivel más alto de garantía de identidad (IAL3). Cuando la información demográfica y biométrica se valida y registra, la prueba de identidad generalmente continúa con la eliminación de duplicados para garantizar que la persona no se haya registrado con una declaración de identidad diferente. Esto se puede lograr con una búsqueda de identificación (1: N) de toda la base de datos biométrica usando uno o más identificadores biométricos (características fisiológicas y/o de comportamiento que se usan para identificar a un individuo). Este proceso puede ser especialmente desafiante con grandes poblaciones.

El siguiente paso es ***Validación***, donde la autoridad determina la autenticidad, vigencia y exactitud de la información de identidad proporcionada por el solicitante y la relaciona con una persona viva. Esto es seguido por ***Verificación***, el establecimiento de un vínculo entre una identidad reivindicada y el sujeto de la vida real que presenta la prueba. El paso final es ***Verificación de antecedentes/evaluación de riesgos***, evaluando el perfil del usuario contra una lista de vigilancia o un modelo basado en riesgos. Según la Publicación especial 800-63A del Instituto Nacional de Estándares y Tecnología (NIST), la prueba de identidad permite a la autoridad:

Resolver una identidad reclamada en una identidad única dentro del contexto de la población de usuarios a los que sirve el proveedor de servicios de credenciales (CSP).

Traducido: *Francisco Javier González García*

Validar que todas las pruebas proporcionadas sean correctas y genuinas (es decir, no falsificadas ni malversadas).

> “Los documentos de obtentor son documentos que se utilizan para acceder a otras formas de identificación legítima, como una licencia de conducir, con el fin de establecer una identidad falsa”.*Ley del Documento Obtentor y Definición Legal*. Obtenido de:https://definiciones .uslegal.com/b/breeder-document/
>
> Aadhaarcard.net.in (7 de noviembre de 2016).*Solicite la tarjeta Aadhaar sin ningún documento*. Obtenido de:https://uidai.gov.in/component/fsf/?view-faq&catid=36
>
> 19 Departamento de Asuntos Sociales y Económicos de las Naciones Unidas (2014).*Principios y recomendaciones para un sistema de estadísticas vitales, Revisión 3*.Obtenido de:https://unstats.un.org/unsd/demographic/standmeth/principles/M19Rev3en.pdf
>
> Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU. (junio de 2017).*Pautas de identidad digital: inscripción y prueba de identidad*. Obtenido de NIST:https://pages.nist.gov/800-63-3/sp800-63a.html
>
> Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU. (junio de 2017).*Pautas de identidad digital*. Obtenido de NIST:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
>
> Jain, Hong y Pankanti (2000).*Identificación biométrica*.Comunicaciones de la ACM, 43(2), p. 91–98. Obtenido de ACM:https://dl.acm.org/citation.cfm?doid=328236.328110

Validar que la identidad declarada existe en el mundo real.

Verifique que la identidad reclamada esté asociada con la persona real que proporciona la prueba de identidad.

Para los países en desarrollo, pueden surgir múltiples desafíos durante el proceso de registro:

> El hardware y el software utilizados para las actividades de registro deben ser precisos, asequibles y utilizables.
> El sistema debe ser inclusivo y debe incluir a miembros de grupos marginados como los pobres, los ancianos, las mujeres y los niños. Algunas personas pueden tener características biométricas deficientes (como una estructura de crestas de huellas dactilares deficiente) que dificultan la inscripción precisa.
> El alcance del proceso debe estar claramente definido, incluyendo la población cuyos datos serán recolectados, los atributos que serán recolectados y el funcionamiento correspondiente del sistema de registro. Por ejemplo, ¿el registro será solo para residentes de ese país o también para visitantes? ¿La información requerida para el registro incluirá nombre, detalles de nacimiento o huellas dactilares? ¿Cuáles son los niveles de precisión y confianza del proceso de registro? Definir claramente el alcance de la población cuyos datos se recopilarán y los atributos que se recopilarán mitigará cualquier problema futuro relacionado con la privacidad y el consentimiento.

2.2. Emisión (Gestión de Credenciales)

La gestión de credenciales comienza con ***Emisión***, que es el proceso de creación y distribución de credenciales virtuales o físicas como pruebas de identidad descentralizadas, pasaportes electrónicos, tarjetas de identificación digitales y licencias de conducir; y un identificador único (con autenticación biométrica central), como el sistema Aadhaar en India.

Traducido: *Francisco Javier González García*

Los otros pasos son ***Mantenimiento***(la recuperación, actualización y eliminación de credenciales) y ***Revocación*** (la eliminación de los privilegios asignados a las credenciales). La interoperabilidad de estas credenciales para la autenticación es cada vez más importante para la prestación de servicios dentro y entre países, como se puede ver en las regiones de la Unión Europea (UE), la Comunidad de África Oriental (EAC) y África Occidental. En la UE, por ejemplo, la identificación electrónica (eID) y los servicios electrónicos de confianza (eTS) proporcionan el marco de interoperabilidad para las transacciones electrónicas transfronterizas seguras del mercado único digital bajo los servicios electrónicos de identificación, autenticación y confianza (eIDAS).

2.3. Autenticación de identidad

La autenticación es el proceso de verificar una afirmación de identidad contra la información de identidad registrada. Dicha información podría ser un número de identificación personal (PIN), una contraseña, datos biométricos como una huella digital, una fotografía o una combinación de estos. Los desafíos en esta fase incluyen cómo reducir el tiempo de procesamiento, mejorar la precisión de la coincidencia para la autenticación, garantizar una experiencia perfecta para los solicitantes, mitigar los desafíos con la conectividad de la red, contrarrestar el comportamiento fraudulento y encontrar soluciones asequibles de hardware y software.

Confiar en Datacard Corporation.*Gestión del ciclo de vida de las credenciales*. Obtenido de:https://www.entrustdatacard.com/solutions/credential-lifecycle-management

Comisión Europea (25 de febrero de 2015).*Servicios de confianza y eID*. Obtenido de Comisión Europea:https://ec.europa.eu/ digital-single-market/en/policies/trust-services-and-eidentification

Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU. (mayo de 2013).*Glosario de términos clave de seguridad de la información*. Obtenido de NIST:http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

2.4. Autorización

Por lo general, la autorización se lleva a cabo después de que se autentica la declaración de identidad de una persona y define los derechos de acceso (u otorga) que una Parte que confía ha asociado con la identidad alineada con la relación entre la persona y la Parte que confía (por ejemplo, una institución financiera), independientemente de el Proveedor de Identidad (por ejemplo, la Autoridad Nacional de Identificación). En esquemas de autorización más avanzados, las concesiones son contextuales y dinámicas. Debido a que este informe se centra en los proveedores de identidad y el aprovisionamiento de identidades, no en las partes que confían y las autorizaciones que pueden asociar con una identidad, no explorará los diversos procesos y tecnologías de autorización que surgen en el mercado actual.

2.5. Gestión de Identidad (Mantenimiento de Identidad)

La gestión o el mantenimiento de la identidad es el proceso continuo de recuperación, actualización y eliminación de atributos de identidad o campos de datos y políticas que rigen el acceso de los usuarios a la información y los servicios. La recuperación de identidad implica obtener los atributos de identidad de un usuario. Las políticas de seguridad deben usarse para hacer cumplir los privilegios

de acceso para garantizar que solo las personas autorizadas puedan acceder, modificar o eliminar la información de identidad, y para garantizar que las acciones se auditen y no se puedan repudiar. Este enfoque garantiza que los recursos estén disponibles solo para usuarios autorizados de acuerdo con las reglas de acceso definidas por atributos y políticas. Las credenciales pueden desactivarse, revocarse o quedar inactivas como resultado de ciertos eventos, y la información de identidad puede actualizarse o eliminarse. Los desafíos de Identity Management incluyen cómo hacer que el mantenimiento del sistema sea rentable, utilizar el análisis de datos para mejorar el rendimiento del sistema (incluida su eficiencia), garantizar que las bases de datos se actualicen para reflejar los principales eventos de la vida (como el nacimiento y la muerte) y mantener la privacidad y la seguridad. control S.

2.6. Ejemplo del viaje de un usuario a través del ciclo de vida de la identidad

¿Cómo es para los usuarios del sistema de identificación digital viajar a través del ciclo de vida de la identidad? Tomemos el ejemplo de Raquel. Quiere inscribirse en el sistema para poder tener acceso seguro a los servicios de salud proporcionados por el gobierno. A medida que avanza a través de las diferentes etapas del ciclo de vida (consulte la Figura 2), se produce un torbellino de actividad tras bambalinas. Los empleados que trabajan en varias partes del sistema se basan en datos, tecnologías y procesos de back-end para garantizar que Rachel sea quien dice ser y que, de hecho, obtenga las credenciales o el documento de identificación que necesitará para acceder a los servicios.

> Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU. (marzo de 2010).*Un informe sobre el Taller de Gestión de Privilegios (Acceso)*.Obtenido de NIST:http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7657.pdf
>
> El viaje del usuario que se muestra en la Figura 2 se alinea con el viaje descrito en el informe de USAID *Identidad en la Era Digital.*
>
> La Figura 2 no incluye la Autorización como paso. Eso es porque la autorización no es responsabilidad de la fundación.
> sistema de identificación Más bien, es responsabilidad de los diversos sistemas de identificación funcional autorizar a los solicitantes al sistema. Los pasos durante la autorización incluyen elegibilidad (política de acceso), gestión de roles, evaluación de riesgos y minimización de atributos.

3. Introducción al marco de evaluación de la tecnología

3.1. Seis parámetros de evaluación

Traducido: *Francisco Javier González García*

Comprender el ciclo de vida de la identidad ayuda a los implementadores a comprender los diversos procesos y tecnologías involucrados en el aprovisionamiento de las credenciales que permiten la identificación y la autenticación. Algunas tecnologías, como el reconocimiento de huellas dactilares, son bastante maduras y ya han tenido una amplia adopción. Otros están surgiendo e incluyen reconocimiento de huellas dactilares sin contacto, perfilado rápido de ácido desoxirribonucleico (ADN) y blockchain. Estas tecnologías más nuevas aún se encuentran en la etapa de prueba piloto. Con múltiples tecnologías disponibles, un marco de evaluación puede ayudar a los implementadores a compararlas, obteniendo una idea de cómo funcionan las tecnologías, cuáles son sus ventajas y desventajas, y cómo podrían ser más útiles para administrar cada etapa del ciclo de vida de la identidad. Los parámetros de evaluación se presentan a continuación:

Madurez:¿Cuánto tiempo ha estado en uso la tecnología? ¿Qué tan bien se entiende?

·*Longevidad:* Cuánto tiempo ha estado disponible y en uso la tecnología (independientemente de la adopción)
·*Interoperabilidad:* ¿La tecnología está basada en Estándares (preferiblemente abiertos)? ¿Qué tan interoperable es la tecnología con las otras tecnologías en el ecosistema de identidad?
Actuación: ¿Qué tan adecuada es la tecnología para realizar la tarea requerida?
·*Rendimiento:*¿Cuántas solicitudes de servicios de identidad puede procesar la tecnología por unidad de tiempo?
·*Tiempo de respuesta:*¿Qué tan rápido puede responder el sistema a una solicitud individual?
·*Exactitud:*¿Con qué frecuencia la tecnología genera coincidencias falsas o rechazos falsos durante la comparación o con qué frecuencia la tecnología no logra inscribir a un porcentaje específico de la población?
·*Estabilidad:*¿Hasta qué punto la tecnología será resistente al cambio frente a fuerzas externas como la edad, las condiciones ambientales, el ritmo de desarrollo y otros?
Escalabilidad: ¿Se puede escalar el uso de la tecnología según sea necesario?
·*Escalabilidad de datos:*¿Qué tan bien puede adaptarse la tecnología a un aumento o disminución en los volúmenes de
datos que se procesan o el número de personas en el sistema?
·*Simplicidad de los recursos computacionales:*¿Con qué facilidad pueden los arquitectos de sistemas adquirir e instalar el hardware y el software necesarios?
·*Simplicidad de la infraestructura de red:*¿Con qué facilidad pueden los arquitectos de sistemas establecer canales de transferencia de datos, especialmente en dominios con ancho de banda limitado?
Adopción: ¿Hasta qué punto los operadores y usuarios del sistema aceptan la tecnología?
·*Integración:*¿Podemos integrar la tecnología con sistemas heredados y futuros?
·*Facilidad de aprendizaje:* ¿Con qué facilidad pueden los operadores del sistema aprender a usar la tecnología?
·*Sencillez de la interfaz de usuario (UI):* ¿Qué tan complejas son las interfaces de software y hardware de la tecnología?

Traducido: *Francisco Javier González García*

·*Simplicidad de entrenamiento:* ¿Qué tan fácil es capacitar a alguien para usar la tecnología?

·*Aceptación cultural:* ¿Cuáles son los sentimientos y pensamientos de los usuarios sobre la tecnología?

Seguridad: ¿Qué tan segura es la tecnología contra el acceso y uso no autorizado?

·*Resistencia a la elusión:*¿Qué tan bien protegida está la tecnología de piratas informáticos y otros ataques? ·*Resiliencia:*¿Con qué rapidez y eficacia puede la tecnología recuperarse de un ataque o una infracción?

·*Seguridad de transmisión:*¿Qué tan seguro es el canal de intercambio de información?

Asequibilidad:¿Qué tan económica es la tecnología?

·*Asequibilidad del hardware:*¿Qué tan rentable es el hardware dedicado?
·*Asequibilidad del software:*¿Qué tan rentable es el software dedicado?
·*Oportunidades de ingresos:*¿Hasta qué punto podríamos recuperar nuestra inversión en la tecnología a través de acuerdos de interoperabilidad, como tarifas de proveedores de servicios del sector privado por realizar e-KYC (Conozca a su cliente) utilizando la base de datos de identificación única del gobierno?
·*Ahorro de costes de tiempo:*¿Qué tan rentable es la tecnología basada en el tiempo requerido para ser completamente funcional?

3.2. Una escala de tres puntos

El Marco de evaluación de tecnología utiliza una escala de tres puntos de "alto", "medio" y "bajo" para representar las respuestas a cada una de las preguntas anteriores. "Alto" es el puntaje máximo o el mejor resultado para un parámetro en particular, mientras que "bajo" es el peor resultado o el puntaje más bajo para un parámetro.
Algunas de las tecnologías evaluadas a través de este marco son muy nuevas, por lo que la información disponible sobre ellas es escasa. En tales casos, se hicieron predicciones informadas tanto para el puntaje como para la dirección del crecimiento de esta tecnología, basándose en el análisis de la tecnología, las tendencias en identificación y autenticación, y los conocimientos de expertos en la materia.
Antes de profundizar en las calificaciones de las diversas evaluaciones de tecnología, los lectores pueden encontrar útil ver un ejemplo de cómo se ve el resultado del marco de evaluación de tecnología. (Consulte la Figura 3.)
Se utilizó el siguiente proceso para decidir las calificaciones de los elementos internos del círculo:

1. Si todos los subparámetros o elementos externos tienen una calificación alta, entonces el elemento interno respectivo tiene una calificación alta.
2. Por el contrario, si todos los subparámetros tienen una calificación baja, entonces el elemento interno tiene una calificación baja.

3. Para todas las demás combinaciones, la clasificación del elemento interior es Media.
4. Si un determinado subparámetro no es aplicable (N/A) para la calificación, se excluye del proceso de calificación.

3.3. Evaluación de tecnologías utilizadas en identificación y autenticación

La Figura 4 a continuación presenta las tecnologías cubiertas en la evaluación. El informe agrupa las tecnologías en seis amplias categorías.

Figura 4: Tecnologías de identificación y autenticación

Para cada categoría, se consideran las capacidades actuales de la tecnología y la trayectoria de crecimiento futuro. También se destacan algunos lanzamientos aplicables a gran escala y pilotos limitados en los que estas tecnologías se utilizan para respaldar la identificación o la autenticación. Aunque el enfoque de este informe está en las aplicaciones en los programas de identificación digital, también se presentan algunos ejemplos de cómo se utiliza una tecnología en el sector privado.

3.4. Asignación de tecnologías al ciclo de vida de la identidad

Antes de entrar en las evaluaciones detalladas de las tecnologías, la Figura 5 indica qué tecnologías pueden habilitar o afectar un determinado paso en el ciclo de vida de la identidad. Por ejemplo, las tecnologías de captura y comparación de huellas dactilares y vasculares son aplicables en el Registro, la Autenticación y la Gestión de Identidad, pero no en la Emisión. Del mismo modo, blockchain es aplicable solo después de la prueba de identidad. Las siguientes secciones proporcionarán una descripción de cada uno y resaltarán los problemas que una tecnología en particular puede o no puede resolver.

4. Tecnologías de credenciales

Este informe clasifica las credenciales en tres subtecnologías: biometría, tarjetas y dispositivos móviles. Un identificador biométrico se puede utilizar como credencial una vez que se haya registrado con la autoridad emisora. Por ejemplo, después de que un viajero completa el proceso de registro con la Agencia de Servicios Fronterizos de Canadá, sus iris son la única credencial requerida para NEXUS Air. Las tarjetas, las tarjetas inteligentes y los dispositivos móviles se pueden usar para almacenar información de identidad y se pueden usar como evidencia para respaldar un reclamo de identidad.

Traducido: *Francisco Javier González García*

Las credenciales se diseñaron originalmente para dispositivos informáticos tradicionales (como computadoras de escritorio y portátiles) donde la tarjeta de verificación de identidad personal (PIV) se puede usar para la autenticación de identidad a través de lectores integrados. Sin embargo, con el surgimiento de una nueva generación de dispositivos informáticos y móviles, el uso de tarjetas PIV ha demostrado ser un desafío. Los dispositivos móviles carecen de lectores de tarjetas inteligentes integrados. Aquí es donde los desarrollos en biometría y comunicación de campo cercano (NFC) están permitiendo a los usuarios autenticarse utilizando los sensores biométricos integrados de un teléfono y dispositivos móviles y tarjetas habilitadas para NFC.

4.1. Biometría

En las secciones que siguen, se revisan varias modalidades biométricas, que incluyen el iris, las huellas dactilares, el rostro, la voz, el comportamiento, vascular y el ADN. (Consulte la Figura 6.)

En la evaluación, la captura biométrica y la coincidencia se distinguen entre sí. La razón es que las tecnologías están madurando a ritmos diferentes. Y aunque están relacionados, se seleccionan en función de necesidades específicas que pueden no estar relacionadas. Por ejemplo, la facilidad de captura tiene poco que ver con la velocidad de coincidencia. La captura es el proceso de recopilación de datos biométricos del usuario. La coincidencia es el proceso en el que el registro biométrico de la sonda de una persona se compara con el registro almacenado (candidato) cuando un usuario final solicita acceso a cualquier sistema protegido biométricamente (como para la autenticación), o se compara con todos los candidatos durante una deduplicación (es decir, , identificación) búsqueda. Ciertas modalidades también tienen diferentes niveles de madurez y avance tecnológico para la captura y el cotejo. Además, las calificaciones son un promedio de diferentes dispositivos y temas. Los dispositivos pueden variar en términos de costo, velocidad, funciones y otras características, mientras que los sujetos pueden variar según la edad, la profesión y otros factores que facilitan o dificultan el proceso de captura para el grupo demográfico específico.

Aunque las tecnologías de captura y comparación para cada modalidad se han evaluado por separado, en el resumen de evaluación biométrica que se muestra en la Figura 7, las diferentes evaluaciones de captura y comparación se combinan en un gráfico mediante gradientes. El color interior representa la clasificación de la tecnología de captura de la modalidad respectiva y el color exterior representa la clasificación de la tecnología coincidente.

El reconocimiento biométrico utiliza los atributos fisiológicos y de comportamiento únicos de un individuo para identificar y autenticar su identidad. Los atributos fisiológicos incluyen elementos relacionados con la forma o la composición del cuerpo, como las crestas de las huellas dactilares, los patrones del iris y las características faciales. Los ejemplos de atributos de comportamiento incluyen la marcha, la firma, los patrones de pulsación de teclas y el uso del mouse. El tipo de atributo recopilado y emparejado se denomina modalidad. Por ejemplo, la huella dactilar y el iris son modalidades biométricas diferentes.

Al determinar qué modalidades incorporar en un sistema de reconocimiento biométrico, los encargados de tomar decisiones deben considerar los siguientes criterios:

Traducido: *Francisco Javier González García*

·**Exactitud:**tasa de aceptación falsa (FAR) y tasa de rechazo falso (FRR) en condiciones operativas
·**Universalidad:**presencia del rasgo en los miembros de la población relevante—importante porque ciertos rasgos (como las huellas dactilares) pueden ser deficientes o estar dañados en ciertos datos demográficos y pueden conducir a una falla en el registro (FTE) del individuo
·**Estabilidad:**permanencia del rasgo en el tiempo o después de una enfermedad o lesión
·**Coleccionabilidad:**facilidad con la que se pueden adquirir muestras de buena calidad
·**Resistencia a la elusión:**vulnerabilidad de la modalidad al fraude
·**Aceptabilidad:**grado de apertura pública para el uso de la modalidad
·**Usabilidad:**facilidad con la que las personas pueden interactuar con la tecnología utilizada para capturar los datos biométricos
·**Costo:**costos de recolección y comparación de muestras; a saber, costos de hardware y software
Al evaluar qué tan bien los diferentes datos biométricos cumplen con estos criterios de eficacia, los datos biométricos pueden ser
considerado como perteneciente a dos categorías principales:
·**biometría primaria** están asociados con modalidades como el reconocimiento de huellas dactilares, rostro e iris, y tienen FAR y FRR relativamente bajos. Los sistemas de identificación que deben buscar en grandes galerías de muestras biométricas utilizan la biometría primaria porque producen resultados más precisos.
·**biometría blanda** se relacionan con las características de comportamiento de un individuo, como los patrones de pulsación de teclas, la firma y la forma de andar. Las tasas de error suelen ser demasiado altas para las búsquedas de identificación, pero estas modalidades se utilizan para la autenticación continua para verificar la identidad del usuario durante una sesión. A través del análisis de los comportamientos e interacciones de un usuario con un dispositivo, la autenticación continua puede detectar anomalías durante una sesión.
Las siguientes secciones examinarán cada modalidad biométrica con más detalle.

4.1.1. Reconocimiento de huellas dactilares

La presencia y ubicación de características distintivas en la superficie de la punta de un dedo, en lo que se conoce como crestas de fricción, son exclusivas de un individuo. Las crestas de fricción incluyen bifurcaciones y terminaciones de crestas, y la ubicación y dirección de estas características se denominan minucias. Otras características se clasifican como basadas en patrones, donde los patrones se clasifican como islas, deltas, bucles, verticilos y poros. Los algoritmos de coincidencia biométrica derivan y comparan plantillas a partir de imágenes que incluyen algunas o todas estas características de huellas dactilares (minucias y patrones) para identificar y autenticar a las personas.

Según las necesidades comerciales y el nivel de seguridad necesario, la cantidad de huellas dactilares capturadas y comparadas para una persona puede ser de 1 a 10 dedos (o más para anomalías físicas, como polidactilos). Las autoridades pueden usar varios sensores diferentes para capturar huellas dactilares:

Traducido: *Francisco Javier González García*

·**Sensores óptico s**capturar una imagen, esencialmente una fotografía, y usar algoritmos para detectar patrones únicos mediante el análisis de las áreas más claras y más oscuras de la imagen.[30]

29 Naser Zaeri (2011).*Extracción y reconocimiento de huellas dactilares basado en minucias, biometría*. Dr. Jucheng Yang (Ed.). InTech. DOI: 10.5772/17527. Obtenido de:https://www.intechopen.com/books/biometrics/minutiae-based-fingerprint-extraction-and-recognition

30 Robert Triggs (9 de julio de 2016).*Cómo funcionan los escáneres de huellas dactilares: explicación de las variantes óptica, capacitiva y ultrasónica.*Obtenido de Android Authority:https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

·**Sensores capacitivos** usar corriente eléctrica para formar una imagen de la huella dactilar. La capacitancia de los valles de las huellas dactilares difiere de la de las crestas debido a las bolsas de aire en los valles.
·**sensores de deslizamiento** tome lecturas después de que un individuo pase su dedo por una pequeña franja capacitiva. La tecnología “une” varias imágenes individuales para crear una imagen de la yema del dedo.
·**Sensores ultrasónico** use un transmisor para enviar ondas de sonido de alta frecuencia que se absorben o rebotan según el patrón de la huella dactilar. Luego, un receptor analiza este pulso para construir el patrón.
·**Sensores térmicos** lea las diferencias de temperatura en la superficie de contacto entre las crestas y los valles de las huellas dactilares.
·**Sensores multiespectrales** capture múltiples imágenes de la yema del dedo bajo diferentes condiciones de iluminación, como longitud de onda, orientación de la iluminación y polarización.
·**Sensores emisores de luz**, una tecnología emergente, supuestamente funciona bajo la luz solar directa en los dedos secos o húmedos y resiste la abrasión. Los dispositivos son mucho más pequeños y livianos que los escáneres ópticos tradicionales.[31]
·**Sensores ópticos de transistores de película delgada,**Otra tecnología emergente, utiliza píxeles sensibles a la luz y una pantalla gráfica para iluminar la superficie de captura y guiar a los usuarios en la colocación de las yemas de los dedos. La tecnología es más pequeña y liviana que los escáneres de huellas dactilares tradicionales, así como más fácil para que las personas interactúen. Específicamente, puede mostrar elementos gráficos, animaciones o videos en la superficie donde las personas colocan las yemas de los dedos.
La coincidencia de huellas dactilares es el proceso de comparar las plantillas de huellas dactilares de una persona con las plantillas de huellas dactilares almacenadas en el almacén de identidad para que ese usuario verifique una afirmación de identidad o contra todos los usuarios para una búsqueda de identificación. El resultado de la búsqueda de huellas dactilares es una lista de candidatos cuya puntuación de similitud está por encima del umbral definido para la operación. En algunas implementaciones, se proporcionan puntuaciones de similitud para todas las comparaciones; en otros, se proporcionan puntajes solo para los mejores candidatos 'N'.
La evaluación de la coincidencia de huellas dactilares es importante, dadas sus aplicaciones generalizadas. Los avances recientes en la tecnología de coincidencia de huellas dactilares han logrado tasas de precisión muy altas, con tasas de identificación de falsos negativos (FNIR) tan bajas como 1,9 % para la coincidencia de un solo dedo índice y 0,09 % para la

Traducido: *Francisco Javier González García*

---

coincidencia de diez dedos. La precisión de la coincidencia de huellas dactilares mejora con las huellas de más dedos capturados para cada individuo.
El reconocimiento de huellas dactilares se utiliza cada vez más para la autenticación en línea. Esto ya está en práctica en las aplicaciones bancarias. Por ejemplo, los clientes de Bank of America pueden guardar sus huellas dactilares en sus teléfonos y usarlas para acceder a sus cuentas. Esto también puede eliminar la necesidad de contraseñas o PIN.[34]La captura y comparación de huellas dactilares tiene una alta penetración en el mercado, y muchos países utilizan las huellas dactilares como modalidad principal en sus sistemas de identificación digital. Además, capturar y comparar huellas dactilares requiere poca capacitación para los operadores y para las personas a las que se les toman las huellas dactilares.

¿Qué problemas puede resolver?

Actuación. La precisión de coincidencia de huellas dactilares es lo suficientemente buena como para justificar su uso a escala nacional. La inclusión es alta; en el programa Aadhaar, por ejemplo, la tasa FTE para la biometría de huellas dactilares fue

Biometría Integrada, LLC. Obtenido de:https://integratedbiometrics.com/technology/

Jenetric GmbH. Obtenido de:http://www.jenetric.com/technology.html

Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU. (diciembre de 2014).*Proveedor de huellas dactilares*
*Evaluación de Tecnología.*Obtenido de NIST:http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf

Danny Thakkar.*Biometría en la banca: para identificación y verificación.* bayométrico. Obtenido de: https://www.bayometric

La tecnología de coincidencia de huellas dactilares también ha avanzado hasta el punto en que algunos algoritmos de coincidencia pueden realizar más de mil millones de coincidencias por segundo. y se están probando escáneres de alta resolución de más de 1000 dpi para biometría infantil.

·**Madurez.**La coincidencia de huellas dactilares es bastante madura y tiene estándares bien establecidos para la interoperabilidad, lo que la hace muy adecuada para aplicaciones interinstitucionales y transfronterizas.
·**Asequibilidad.**La tecnología de comparación de huellas dactilares es rentable, del orden de las tecnologías de comparación biométrica de muchas otras modalidades. Las tecnologías de captura de huellas dactilares van desde menos de $ 100 por un dispositivo de captura producido en masa con un solo dedo hasta miles de dólares por un dispositivo de captura sin contacto de cuatro dedos.

¿Qué problemas no resuelve?

·**Rendimiento (estabilidad).** La captura de huellas dactilares no es universalmente inclusiva, dado que algunas crestas de fricción son ilegibles, están dañadas o desgastadas, especialmente en personas que trabajan con productos químicos cáusticos y en agricultura o trabajo manual, ancianos, bebés y personas con dedos pequeños.

·**Adopción.** Algunas personas aún consideran que los sensores de captura de huellas dactilares basados en contacto son antihigiénicos, y estas percepciones podrían limitar la disposición a utilizar la tecnología. En los casos en que se requiere que los administradores ayuden físicamente a los sujetos durante el proceso de captura, algunos pueden percibirlo como invasivo o inapropiado. Además, algunos todavía asocian la toma de huellas dactilares con el comportamiento delictivo y se oponen. Sin embargo, la tecnología emergente de escáneres sin contacto podría ayudar a aliviar tales preocupaciones.
·**Seguridad.** La tecnología no es inmune a la elusión, lo que genera algunas preocupaciones sobre la seguridad y la privacidad. No obstante, están surgiendo tecnologías para detectar ataques de presentación, tal como se define en la norma ISO 30107.

¿Qué problemas podría crear?

·**Asequibilidad.** Los escáneres de captura de huellas dactilares sin contacto podrían costar mucho más que los escáneres tradicionales.

4.1.2. Reconocimiento de iris

El reconocimiento del iris utiliza las características únicas del iris, que incluyen la porción pigmentada del ojo que separa la pupila oscura en el centro del ojo de la esclerótica blanca alrededor del pigmento. La luz infrarroja cercana (NIR) se usa típicamente para iluminar el iris durante el proceso de captura, resaltando los patrones al disminuir el espectro (variación de color) en el área de interés. La cámara captura una imagen de uno o ambos ojos y luego un algoritmo procesa la imagen, detectando los límites de la esclerótica y la pupila, y segmentándolos en consecuencia. Después de la segmentación, un algoritmo deriva una plantilla (un código de iris) basada en las características del iris.
Las principales ventajas de la tecnología de reconocimiento de iris incluyen la velocidad de coincidencia; alta precisión; y estabilidad de la forma, el color y la textura del iris. La tecnología de coincidencia de iris generalmente emplea modelos matemáticos para el reconocimiento de patrones para comparar las plantillas de iris. El iris es altamente inclusivo, seguro y preciso, con FRR de 0,2 % (las huellas dactilares tienen un 1 %) y FAR de 0,0001 % (las huellas dactilares tienen un 0,00002 %).[37]En términos de tasa de captura, en un proyecto de ACNUR en Malawi, el iris obtuvo una tasa de captura del 98 % para un iris bueno, frente a una tasa de captura del 87 % para cuatro dedos buenos en personas de 4 años o más. Para niños pequeños y bebés de 0 a 3 años.

Basado en una discusión de SME con Sanjay Jain, exgerente jefe de productos de UIDAI.

nnovatrics (10 de agosto de 2017).*El algoritmo de Innovatrics procesa mil millones de coincidencias por segundo.*Obtenido de:http://www.marketwired.com/press-release/innovatrics-algorithm-processes-1-billion-matches-per-second-2229791.htm

Thakkar, D.*Los cinco datos biométricos principales: cara, huellas dactilares, iris, palma de la mano y voz*. bayométrico. Obtenido de:https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/

Traducido: *Francisco Javier González García*

La tasa de captura de un buen iris fue del 14 % frente al 2 % de cuatro buenas huellas dactilares. Por lo tanto, el iris obtuvo una puntuación más alta que las huellas dactilares en términos de facilidad de uso, velocidad y preferencia general.

El reconocimiento de iris se puede usar para la autenticación en aplicaciones en línea, y los esfuerzos de investigación se han centrado en cómo usar esta biometría para la autenticación en aplicaciones bancarias y de comercio electrónico.

¿Qué problemas puede resolver?

·**Actuación.** La coincidencia de Iris es muy adecuada para la eliminación de duplicados de identidad debido a sus tasas de error relativamente bajas para la coincidencia de uno a muchos durante las búsquedas en galerías grandes (más de 1 millón de identidades). En Aadhaar, por ejemplo, las tasas de FTE para escaneos de iris son solo del 0,2% al 0,5%. Además, el iris es más estable que algunas otras modalidades (es decir, la cara y la huella dactilar). Así, los operadores no tienen que reinscribirse con frecuencia en esta modalidad.
·**Escalabilidad.** Las velocidades de coincidencia son altas, con ciertos algoritmos que coinciden a una velocidad de 200 000 plantillas de iris por segundo. Por lo tanto, la tecnología se puede escalar a grandes poblaciones.
¿Qué problemas no resuelve?

.

.

4.1.3.

Adopción. La tecnología de captura del iris puede no ser tan fácil de usar como la toma de huellas dactilares faciales o sin contacto, porque algunos dispositivos de captura del iris requieren un posicionamiento muy específico del sujeto. También existe cierto estigma cultural asociado con el escáner de iris. Pero los escáneres de iris más nuevos están superando estos desafíos al ser mucho más fáciles de operar y requieren menos interacción del operador o del sujeto que los dispositivos más antiguos. La nueva tecnología de iris a distancia también permite capturar el iris a distancias más lejanas del dispositivo, como de 0,8 a 1,2 metros.[44]

Asequibilidad. El hardware y el software de captura de iris suelen costar más que la toma de huellas dactilares. La tecnología de coincidencia de iris, por otro lado, generalmente requiere menos poder de cómputo que la de la toma de huellas dactilares.

Reconocimiento facial

El reconocimiento facial utiliza las características de la cara que no cambian significativamente con la edad o con la cirugía. Estos incluyen el borde de la ceja, los pómulos, los bordes de la boca, la distancia entre los ojos, el ancho de la nariz y la forma de la mandíbula y el mentón.

Traducido: *Francisco Javier González García*

Actualmente, la tecnología de reconocimiento facial se utiliza principalmente en la seguridad (como en los sistemas automatizados de control de fronteras y vigilancia), así como para controlar el acceso físico de las personas a las instalaciones.

38 Gelb, A., Mukherjee, A. y Diofasi, A. (01 de agosto de 2016). *Reconocimiento de iris: mejor que las huellas dactilares y la caída del precio*. Centro para el Desarrollo Global. Obtenido de:https://www.cgdev.org/blog/iris-recognition-better-fingerprints-and-falling-price

Lawal, A. y Chukwu, R.O. (noviembre de 2014).*Aplicación de la tecnología biométrica Iris a la industria bancaria en Nigeria*. International Journal of Soft Computing and Artificial Intelligence Vol-2, Issue-2, pp. 17–22. Obtenido de:http://www.iraj.in/journal/journal_file/journal_pdf/-141544422317-21.pdf

Vangala, R. R. y Sasi, S. (2004).*Autenticación biométrica para transacciones de comercio electrónico.*2004 Taller internacional IEEE sobre técnicas y sistemas de imágenes, IST. págs. 113–116. Obtenido de:https://www.researchgate.net/publication/4125406_Biometric_authentication_for_e-commerce_transaction

NIST.*Desempeño de Algoritmos de Identificación de Iris.*Obtenido de:http://ws680.nist.gov/publication/get_pdf

Basado en una entrevista de SME con Sanjay Jain, ex gerente jefe de productos de UIDAI.

Neurotecnología. Obtenido de:http://www.neurotechnology.com/megamatcher-technical-specifications.html

Morfo.*Iris a distancia: el poder detrás del iris.*Obtenido de:https://www.morpho.com/en/media/iris-distancia-poder-detrás-iris-20140311

Los sistemas y algoritmos de reconocimiento facial se dividen en dos categorías principales: bidimensionales (2D) y tridimensionales (3D). Actualmente, los sistemas 2D superan a los 3D, pero se espera que esto cambie pronto.[45]2D utiliza el análisis de componentes principales (PCA) para mejorar la precisión al reducir la dimensionalidad de los datos (reduciendo la cantidad de variables aleatorias bajo consideración al obtener un conjunto de variables principales), al tiempo que conserva la mayor cantidad posible de la variación presente en el conjunto de datos original . Los operadores pueden lograr mejoras significativas mapeando primero los datos en un subespacio dimensional más bajo.[46]El análisis discriminante lineal (LDA) es otra técnica 2D.

También tiene como objetivo reducir la dimensionalidad y preservar las variaciones de datos. Sin embargo, es más capaz de distinguir la variación de la imagen derivada de factores como la iluminación y la expresión facial. Apple ha incluido el reconocimiento facial que llama Face ID con el último iPhone X. Face ID es una forma de autenticación biométrica que se basa en características únicas de la cara. Utiliza una combinación de un emisor de infrarrojos y un sensor para proyectar 30.000 puntos de luz infrarroja sobre y alrededor de la cara. Luego, la cámara calcula la profundidad y el ángulo de cada punto y construye un mapa de profundidad que luego se usa para hacer coincidir. Esta característica mejora la precisión de coincidencia y hace que los ataques de presentación sean más fáciles de detectar porque la profundidad se usa junto con otras características para determinar si el sujeto es genuino o está siendo manipulado de alguna manera.

A medida que las soluciones de reconocimiento facial se vuelven más frecuentes, también se pueden usar para autenticar a los usuarios en transacciones en línea. Varias instituciones de servicios financieros han realizado recientemente varios ensayos de reconocimiento facial para investigar la eficacia de la tecnología; por ejemplo, en los pagos con tarjeta de crédito. MasterCard incluso realizó una prueba para aprobar compras en línea mediante un escaneo facial.[48]

¿Qué problemas puede resolver?

Traducido: *Francisco Javier González García*

·**Actuación.**Esta tecnología se puede utilizar en sistemas de identificación a gran escala, incluso en casos de identificación interinstitucional y transfronteriza, porque la precisión de la coincidencia de rostros tridimensionales ha mejorado sustancialmente. Hoy en día, las tasas FAR y FRR están a la par con las de los sistemas de reconocimiento de huellas dactilares para la autenticación (coincidencia 1 a 1) La precisión del sistema de reconocimiento facial se ve afectada por la calidad y el tamaño de la galería que se busca y no funciona tan bien como el iris y la huella dactilar en la identificación a gran escala (búsquedas de uno a muchos).

·**Adopción.** La tecnología de captura de reconocimiento facial es relativamente fácil de usar**.**Tomar una fotografía requiere un entrenamiento mínimo para los operadores y poco cambio de comportamiento por parte de los usuarios, aunque la calidad de la imagen merece atención. Con el aumento del uso de tecnologías encubiertas de reconocimiento facial (como las que se utilizan para marketing o seguridad sin el permiso o notificación de los sujetos), las preocupaciones por la privacidad han aumentado.[50]

·**Asequibilidad.** El reconocimiento facial se ha vuelto cada vez más asequible, debido a un aumento en la combinación de la tecnología con los sistemas de cámara de los teléfonos inteligentes. Por lo tanto, podría rivalizar con el éxito del sensor de huellas dactilares basado en teléfonos inteligentes para la autenticación personal. Cuando los sistemas de reconocimiento facial se utilizan para búsquedas de identificación automatizadas (1: N) en grandes bases de datos con fotos de entrada de calidad baja a media (que suele ser el caso), los propietarios del sistema pueden esperar costos operativos más altos debido a una tasa más alta de adjudicaciones manuales.

Scheenstra, A., Ruifrok, A. y Veltkamp, R.C. (2005). *Una encuesta de métodos de reconocimiento facial 3D*.En Lecture Notes in Computer Science, págs. 891–899. Obtenido de:http://www.cs.uu.nl/groups/MG/multimedia/publications/art/avbpa05.pdf

Bebis G. (2016). Biometría. Notas de lectura. Obtenido de:https://www.cse.unr.edu/~bebis/CS790Q/Lect/FR_PCA_LDA.ppt

G. Jetsiktat, S. Panthuwadeethorn y S. Phimoltares (2015).*Mejora de la autenticación de usuario del pago con tarjeta de crédito en línea*
utilizando la comparación de imágenes faciales con el descriptor de histograma MPEG7-edge.Conferencia Internacional de Informática Inteligente 2015
and Biomedical Sciences (ICIIBMS), Okinawa, págs. 67–74. Obtenido de IEEE:http://ieeexplore.ieee.org/document/7439481/

José Pagliery (01 de julio de 2015).*MasterCard aprobará compras escaneando tu cara*. CNN. Obtenido de:http://dinero.cnn
.com/2015/07/01/technology/mastercard-facial-scan/index.html

SME Aporte del Dr. Joseph Atick, presidente ejecutivo, ID4 Africa & Identity Counsel.

(03 de octubre de 2017).*La privacidad está amenazada por la revolución del reconocimiento facial*. Tiempos financieros. Obtenido de:https://www
.ft.com/content/4707f246-a760-11e7-93c5-648314d2c72c

¿Qué problemas no resuelve?

·**Actuación.**Aunque el rendimiento del software de reconocimiento facial ha mejorado significativamente, solo ofrece un rendimiento satisfactorio en escenarios controlados. El rendimiento se degrada con el envejecimiento, la mala iluminación y las variaciones en las poses de los sujetos. Además, existe la oportunidad de una mayor estandarización.

Traducido: *Francisco Javier González García*

·**Seguridad.**La tecnología no es inmune a la elusión. Por ejemplo, usando una técnica llamada morphing, las personas pueden crear una identificación con foto que contenga una representación gráfica de varias caras, lo que permite que varias personas compartan sus credenciales.. Este riesgo empeora en entornos no supervisados.

¿Qué problemas podría crear?

·**Adopción.** Si los sistemas de reconocimiento facial se optimizan para el reconocimiento de la mayoría de los grupos étnicos en una sociedad multiétnica, pueden cometer más errores al evaluar los rostros de las personas que son miembros de grupos minoritarios. Esto podría empeorar la exclusión y marginación de tales individuos.

·**Adopción (aceptación cultural).** El reconocimiento facial podría usarse para vigilar a las personas de un país sin su consentimiento. Estos sistemas recopilan información de numerosas cámaras de circuito cerrado de televisión (CCTV) y realizan reconocimiento facial en tiempo real para identificar a los delincuentes u otras personas de interés. Países como China y Rusia ya han desplegado tales sistemas en pilotos a gran escala.

·**Adopción (bloqueo de proveedores).** Es necesaria una mayor estandarización. Esto es especialmente cierto en la definición de plantillas faciales para eliminar posibles bloqueos de proveedores y reducir los requisitos de almacenamiento, ya que la mayoría de los implementadores deben almacenar imágenes que a menudo requieren más espacio de almacenamiento que las plantillas comprimidas de la Organización Internacional de Normalización (ISO) de huellas dactilares.

4.1.4. Reconocimiento de voz

La tecnología de reconocimiento de voz interpreta los patrones de voz para reconocer a las personas en función de su voz. En estos sistemas, las muestras de voz recopiladas se convierten en un espectrógrafo, una representación visual de las propiedades acústicas de un sonido. Este espectrógrafo se utiliza luego con fines de verificación o identificación.

La voz es una modalidad biométrica tanto fisiológica como conductual. De hecho, las propiedades acústicas del habla de un individuo están determinadas por características anatómicas como la forma de la boca de la persona y la longitud y calidad de las cuerdas vocales (fisiológicas), junto con sus entonaciones únicas al hablar. Usando más de 100 factores físicos y de comportamiento (incluyendo pronunciación, énfasis, velocidad del habla, acento, tracto vocal y conductos bucales y nasales), las tecnologías de reconocimiento de voz pueden crear una firma de voz única de un individuo.

El uso de esta modalidad comienza con el registro de voz, el proceso de capturar la muestra de voz de un individuo por primera vez, evaluar su calidad y crear y almacenar el modelo resultante.

M. Hassaballah y S. Aly (30 de julio de 2015).*Reconocimiento facial: desafíos, logros y direcciones futuras.*IET Computer Vision, vol. 9, núm. 4, págs. 614–626. Obtenido de:http://ieeexplore.ieee.org/document/7172641/

Garvey, et al. (2016).*La alineación perpetua: el reconocimiento facial de la policía no regulada en Estados Unidos.*Centro de derecho de Georgetown sobre privacidad y tecnología

Chin, J. y Lin, L. (26 de junio de 2017).*El estado de vigilancia que todo lo ve de China está leyendo las caras de sus ciudadanos.*Wall Street Journal. Obtenido de:https://www.wsj.com/articles/the-all-seeing-surveillance-state-feared-in-the-west-is-a-reality-in-china-14984930

Traducido: *Francisco Javier González García*

Gianluca Mezzofiore (28 de septiembre de 2017).*La red CCTV de reconocimiento facial de Moscú es el mayor ejemplo de sociedad de la vigilancia hasta el momento.*Mashable. Obtenido de:http://mashable.com/2017/09/28/moscow-facial-recognition-cctv-network-big-brother/#GzhBgoBDd8qy

Aporte de PYME de Jérôme Buchler, Gerente de Desarrollo de Negocios Internacionales en HSB identificación.

Verificación de voz y identificación potencial, es el proceso de comparar una muestra de sonda (prueba) con la muestra registrada para autenticar a un individuo.

Hay dos tipos de sistemas de coincidencia de voz: verificación de locutor e identificación de locutor. Los sistemas de verificación de hablantes verifican si la muestra de voz presentada por una persona coincide con la muestra de voz almacenada en la base de datos. Este es un proceso de coincidencia 1:1. Los sistemas de identificación de hablantes intentan hacer coincidir una muestra de voz dada con las muestras en una base de datos para identificar al hablante. Este es un proceso de coincidencia 1:N.

Predominan dos tipos de sistemas de verificación del hablante: dependientes del texto, que requieren que el hablante diga exactamente la contraseña inscrita o dada, e independientes del texto, donde la identidad del hablante se puede verificar sin restricciones en el contenido del discurso. Si bien la independencia del texto es más conveniente porque las personas pueden hablar libremente con el sistema, requiere una capacitación más extensa del algoritmo y la prueba de las expresiones de los hablantes para brindar la máxima precisión.[56]

Muchos bancos ahora utilizan el reconocimiento de voz como una biométrica de autenticación, especialmente al brindar servicios bancarios a los clientes por teléfono. También se están realizando investigaciones sobre el uso del reconocimiento de voz en aplicaciones de comercio electrónico.[59,60]

¿Qué problemas puede resolver?

·**Adopción** El reconocimiento de voz se adopta fácilmente porque la gente está familiarizada con él y es fácil de usar. Tampoco plantea preocupaciones sobre la higiene o la idoneidad cultural, ya que el proceso de captura de voz no requiere contacto físico entre las personas y un dispositivo, ni la intervención física de los operadores. La voz también se puede utilizar para autenticar usuarios de forma remota. Por ejemplo, se puede utilizar en centros de llamadas para autenticar la identidad de un cliente.
·**Asequibilidad.** Configurar un sistema de identificación basado en la voz es rentable porque requiere poco hardware de captura más allá de un simple micrófono para grabar voces, y la tecnología de coincidencia asociada está a la par con otras modalidades.
¿Qué problemas no resuelve?
·**Actuación.** El proceso de captura de voz requiere grabar unos 10 segundos de una conversación normal cuando se utiliza el reconocimiento de voz independiente del texto. La captura para el registro requiere unos 30 segundos de voz. En ambos casos, la calidad de la grabación afecta la precisión de la coincidencia. Además, cualquier ruido de fondo extenso, junto con los esquemas de compresión que degradan la calidad de la muestra, aumenta las tasas de error. Otros factores, como el envejecimiento y la enfermedad, junto con la calidad del micrófono o del canal, la amplitud de la señal y la duración de la muestra, también

Traducido: *Francisco Javier González García*

---

pueden erosionar la calidad de la muestra. La coincidencia de voz generalmente tiene tasas de error más altas en comparación con el reconocimiento de rostro, huella digital e iris.
·**Escalabilidad.** En comparación con los sistemas de huellas dactilares e iris, que pueden realizar millones de coincidencias por segundo, los sistemas comunes de reconocimiento de voz pueden procesar solo un millón de registros por día.

Zhengyou Zhang (20 de agosto de 2006).*Verificación del hablante: dependiente del texto frente a independiente del texto.*Microsoft Recuperado de:https://www.microsoft.com/en-us/research/project/speaker-verification-text-dependent-vs-text-independent/

Kevin Peachey (01 de agosto de 2016).*Los bancos recurren al reconocimiento de voz*. BBC. Obtenido de:http://www.bbc.com/news/ business-36939709

Banco ICICI (25 de mayo de 2015).*ICICI Bank presenta el reconocimiento de voz para la autenticación biométrica.*Banco ICICI Obtenido de:https://www.icicibank.com/aboutus/article.page?identifier=news-icici-bank-introduces-voice-recognition-for-biometric-authent ication-20152505124050634

Shaji, N.A., Murali, S., et al. (noviembre de 2016).*Una encuesta sobre autenticación biométrica para transacciones en línea.*Revista internacional de ingeniería y ciencias de la computación, volumen 5, número 11, págs. 19241–19243. Obtenido de:https://www.ijecs.in/issue/v5-i11/93%20ijecs.pdf

W. Yang, Y. Wu y G. Chen (2011).*Aplicación de Reconocimiento de Voz para la Seguridad del Comercio Electrónico Móvil*. Tercera Conferencia de Asia-Pacífico sobre Circuitos, Comunicaciones y Sistemas (PACCS), Wuhan, págs. 1–4. Obtenido de:http://ieeexplore.ieee.org/document/5990286/

¿Qué problemas podría crear?

·4.1.5.

Seguridad. Dado que la coincidencia de voz se puede realizar de forma remota, estos sistemas podrían eludirse utilizando una muestra de voz de un individuo. Además, debido a que el ruido de fondo y otros factores pueden impedir la precisión del reconocimiento de voz, esta modalidad solo se puede usar en entornos donde el nivel de seguridad necesario para una declaración de identidad es bajo. La elusión se puede mitigar a través del reconocimiento de voz dependiente del texto, que incluye una frase de contraseña dinámica.

Reconocimiento de comportamiento

La biometría del comportamiento utiliza patrones de comportamiento humano para autenticar a un individuo y, por lo general, se combina con una o más modalidades fisiológicas en un sistema multimodal. La biometría del comportamiento incluye la dinámica de la firma (como la velocidad y la presión con la que una persona firma su nombre), la forma de andar, la dinámica de pulsación de teclas, el uso del mouse y las interacciones con la pantalla táctil. Los dispositivos como los teléfonos inteligentes se pueden configurar para capturar pasivamente datos de comportamiento a través de la pantalla táctil, el acelerómetro y el giroscopio. Cada vez más, las organizaciones utilizan la huella de las redes sociales (también llamada metadatos) para prevenir y rastrear el robo de identidad y el fraude, y para respaldar la autenticación continua de un usuario durante una sesión.

La biometría del comportamiento se está implementando actualmente en la banca en línea, el comercio electrónico, los pagos y los mercados de autenticación de alta seguridad. Ahora se está desarrollando tecnología para identificar a los usuarios en función de comportamientos como

Traducido: *Francisco Javier González García*

---

movimientos del cursor, patrones de clic, velocidad de escritura, patrones de deslizamiento y ubicación geográfica. El análisis de comportamiento junto con el aprendizaje automático ahora también se está utilizando para brindar garantía de identidad.

¿Qué problemas puede resolver?

·**Actuación.** Los operadores pueden utilizar la biometría del comportamiento para la autenticación continua en tiempo real junto con los mecanismos de autenticación heredados, como la entrada de contraseña. Para la coincidencia de comportamiento, se recopilan numerosos puntos de datos y los operadores pueden usar cualquier combinación de ellos para identificar a un individuo.

·**Adopción.** En la verificación de firma dinámica (un tipo de registro de reconocimiento de comportamiento), los resultados son independientes del idioma nativo del usuario. Esto hace que la tecnología sea más aceptable social y legalmente, lo que aumenta la probabilidad de adopción.

¿Qué problemas no resuelve?

·**Madurez.** La tecnología de reconocimiento de comportamiento aún no se ha estudiado por completo, y aún se están desarrollando estándares para la recopilación e intercambio de datos. Por lo tanto, la tecnología puede no ser adecuada para su uso como sistema independiente para la identificación digital.

·**Actuación.** La precisión de la verificación de firma dinámica no es lo suficientemente alta como para usarla como una modalidad independiente para los sistemas de identificación digital. Aunque se tienen en cuenta varios parámetros (como la presión de la punta del lápiz, el número de trazos y el ángulo del lápiz), dicha verificación solo tiene una precisión del 97,47 %.[64]Al igual que con el uso de un biométrico como el dedo o el iris para bloquear un teléfono inteligente, un patrón de bloqueo que es biométrico de comportamiento es menos seguro.

Asociación Internacional de Biometría + Identidad.*Biometría del Comportamiento.*IBIA. Obtenido de:https://www.ibia.org/download/datasets/3839/Behavioral%20Biometrics%20white%20paper.pdf

Alton, L. (23 de agosto de 2015).*La ciberseguridad de próxima generación tiene que ver con el reconocimiento del comportamiento.*TechCrunch. Obtenido de:https://techcrunch.com/2015/08/23/next-gen-cybersecurity-is-all-about-behavior-recognition/

Oeltjen, J. (06 de noviembre de 2017).*Autenticación y aprendizaje automático: llevar el reconocimiento de comportamiento a un nuevo nivel.*RSA Seguridad LLC. Obtenido de:https://www.csoonline.com/article/3209917/identity-management/article.html

Schmidt, T., Riffo, V. y Mery, D. (2011).*Reconocimiento dinámico de firmas basado en Fisher Discriminant.*Progreso en reconocimiento de patrones, análisis de imágenes, visión artificial y aplicaciones, págs. 433–442. Obtenido de:https://link.springer.com/chapter/10.1007/978-3-642-25085-9_51

·**Escalabilidad.** La tecnología no es altamente escalable porque los metadatos asociados con el reconocimiento de comportamiento generalmente se capturan y analizan en una ubicación centralizada durante un período de tiempo. Por el contrario, otros sistemas se inscriben solo una vez y se autentican localmente contra el patrón inscrito inmediatamente. Además, capacitar a un operador en el uso de sistemas biométricos de comportamiento suele llevar días o semanas. Finalmente, la autenticación de comportamiento no se puede realizar localmente en los dispositivos y

debe conectarse a un servidor de back-end, a diferencia de otras modalidades como la huella digital y la cara.

¿Qué problemas podría crear?

·**Adopción.** La tecnología podría generar inquietudes sobre la privacidad y la vigilancia, ya que los datos de fondo necesarios para la autenticación del comportamiento se capturan continuamente y, en algunos casos, sin el conocimiento o el permiso de las personas.

4.1.6. Reconocimiento Vascular

Cada persona tiene un patrón distinto de venas. El reconocimiento de patrones vasculares (venas) utiliza este rasgo biométrico fisiológico para el reconocimiento de identidad, como el dorso de la mano, en la palma o en los dedos. La luz NIR se utiliza para iluminar las venas justo debajo de la piel, que se muestran oscuras y distintas sobre un fondo más claro de arterias. Luego, un sensor lee la imagen para capturar o hacer coincidir el patrón de la vena. La vena de la palma se utilizó como ejemplo para la evaluación presentada en esta sección.

Algunas empresas ofrecen tecnologías de reconocimiento vascular para la autenticación y la tecnología se está adoptando gradualmente para la identificación. Un ejemplo notable es el Centro Médico Langone de la Universidad de Nueva York, que utiliza un sistema de comparación de venas para identificar a los pacientes y obtener sus registros médicos anteriores de la base de datos. Este sistema ha resultado útil para identificar incluso a pacientes inconscientes y poco comunicativos.sesenta y cincoEl sector de servicios financieros de Japón también ha implementado la tecnología para verificar a los clientes en los canales minoristas. Este enfoque ha reducido la dependencia de los proveedores de servicios financieros de tarjetas o documentos portátiles, que con frecuencia se han perdido en la nación insular debido a los terremotos.

El reconocimiento vascular se ha utilizado desde la década de 1980, pero no ha logrado una alta penetración en el mercado. Una razón potencial para esto podría ser la falta de estudios a gran escala de esta modalidad.

¿Qué problemas puede resolver?

·**Actuación.**Algunos sistemas de correspondencia vascular pueden acomodar transacciones de hasta 100.000[67]individuos Los sistemas también tienden a ser precisos, informando FRR de solo 0,01 % y FAR de usuarios no autorizados de 0,00008 %.[68]
·**Adopción.**Las tecnologías de captura vascular más nuevas se adaptan a una mayor variabilidad en el posicionamiento de la mano. La mayor facilidad de uso mejora la probabilidad de adopción.
·**Seguridad.**La tecnología de captura vascular sin contacto ofrece una mayor seguridad que los escáneres de huellas dactilares de contacto tradicionales. Eso es porque sin contactoel

Traducido: *Francisco Javier González García*

---

escaneo vascular no deja huellas latentes durante el proceso de captura, lo que reduce la posibilidad de que alguien engañe al sistema. Además, a diferencia de la cara, el iris y las huellas dactilares, la captura remota de patrones vasculares es imposible sin el conocimiento del sujeto.

65 Plasencia, A. (25 July 2011). *El hospital escanea las manos de los pacientes para obtener información médica*. NBC. Obtenido de:https://www.nbcnewyork.com/news/local/Hospital-Scans-Patient-Hands-to-Pull-Medical-Info-126142628.html

Shimbun, A. (14 de septiembre de 2016).*Banco japonés permitirá a los clientes usar datos biométricos de venas de la palma de la mano en lugar de tarjetas*. Encuentre biometría. Obtenido de:https://findbiometrics.com/japanese-bank-palm-vein-biometrics-30142/

PV1000-Vena de la palma.Indiamart.com. Obtenido de:https://www.indiamart.com/proddetail/pv1000-palm-vein-9918273197.html

Fujitsu.*Solución de autenticación de venas de palma PalmSecure*®.Obtenido de:https://www.fujitsu.com/us/Images/palmsecure_ hoja de datos.pdf

¿Qué problemas no resuelve?

·**Asequibilidad.**La tecnología de captura vascular es más costosa que las tecnologías utilizadas para la toma de huellas dactilares y cuesta entre 400 y 500 dólares estadounidenses.[69]

¿Qué problemas podría crear?

·**Madurez.**Ninguna organización independiente líder (como NIST) ha probado aún el rendimiento de la tecnología biométrica vascular en identificación y autenticación a gran escala. Por lo tanto, la tecnología no se comprende bien y la falta de comprensión podría plantear desafíos relacionados con la integración y la interoperabilidad cuando se implemente.

ENFOQUE: PRIVACIDAD

Los datos biométricos son una forma de PII. El Instituto de Biometría, un foro internacional independiente e imparcial para compartir conocimientos e información sobre biometría, ha publicado las siguientes pautas para el manejo de información biométrica:[70]

1. ***Todos los miembros del personal y los gerentes de una organización que utiliza datos biométricos deben comprometerse a proteger la privacidad de los sujetos, demostrar respeto por la privacidad y controlar sistemáticamente el uso de datos biométricos y otros datos personales.***
2. ***Siempre que sea posible, las organizaciones deben respetar el derecho de una persona a dar su consentimiento informado para que se recopilen sus datos biométricos. Para dar el consentimiento informado, el sujeto debe comprender:***

O *Por qué y cuándo se recopila la información biométrica* O*quien lo colecciona*

O *Quién más tendrá acceso a él*

Traducido: *Francisco Javier González García*

O *Cómo se protegerá, almacenará, transmitirá y accederá* O*Cuáles son los límites de tiempo para su uso y almacenamiento*

O *Cómo se eliminará o eliminará de la base de datos de identidad*

3. ***Los datos biométricos deben protegerse mediante evaluaciones de impacto en la privacidad, auditorías de privacidad, políticas de privacidad claras y procedimientos y controles técnicos para evitar el acceso no autorizado, la pérdida accidental o el uso indebido de datos personales.***
4. ***Las organizaciones deben tener como objetivo garantizar que a ninguna persona se le niegue el servicio o el acceso a los beneficios debido a su incapacidad o falta de voluntad para proporcionar datos biométricos o utilizar un sistema biométrico. Siempre que sea posible, se debe ofrecer una alternativa, y el diseño del sistema debe incluir procesos alternativos para aquellos que no pueden acceder al sistema, lo que incluye brindar la oportunidad de acceder al sistema en una fecha posterior.***
5. ***Todas las personas/interesados deben ser informados de las circunstancias en las que los datos pueden compartirse con otras partes, ya sea con fines de aplicación de la ley, investigaciones de fraude u otros fines relacionados con la ley o el comercio.***
6. ***Las organizaciones deben establecer sistemas de quejas y consultas que incluyan vías transparentes de reparación y un enfoque comprensivo que acepte la posibilidad de fallas técnicas o de procedimiento en su sistema biométrico.***

*Escáner Fujitsu PalmSecure con carcasa.*Fulcrum Biometrics, LLC. Obtenido de:https://www.fulcrumbiometrics.com/Instituto de Biometría (mayo de 2017).*Pautas de privacidad: una guía de mejores prácticas para biometría y pautas de privacidad.*Instituto de Biometría. Obtenido de:https://www.biometricsinstitute.org/privacy-charter

4.1.7. Perfilado rápido de ADN y coincidencia de ADN

El ADN es el código genético que es exclusivo de cada organismo y se ha utilizado tradicionalmente en las pruebas de paternidad y aplicación de la ley. El ADN también se puede utilizar para establecer parentesco.

La tecnología funciona midiendo secuencias repetidas a corto plazo en el ADN.La medición de la longitud de estas secuencias proporciona un atributo de alta precisión que identifica de forma única al individuo entre toda la población humana.

Antes de la introducción de la tecnología de secuenciación rápida de ADN, el procesamiento de ADN debía realizarse en laboratorios con técnicos capacitados e instrumentos de laboratorio especializados. La generación del análisis final tomó varios días. La tecnología Rapid DNA ha reducido el tiempo de procesamiento a unos 90 minutos. El análisis rápido de ADN implica la creación de un perfil de ADN a partir de una muestra de referencia extraída de la boca o el interior de la mejilla de una persona de forma totalmente automatizada. Además, los dispositivos requeridos se

Traducido: *Francisco Javier González García*

---

han miniaturizado y hecho portátiles, fortaleciendo el caso para el uso del ADN como modalidad de identificación.

El perfil de ADN genera una representación visual del ADN que presenta columnas de bandas paralelas de color oscuro y es equivalente a una huella dactilar levantada de una superficie lisa. Para identificar al propietario de una muestra de ADN, la "huella digital" o perfil de ADN debe coincidir, ya sea con el ADN de un individuo conocido (1:1) o con un perfil de ADN almacenado en una base de datos (1:N).[71]Tanto como el 99,9% del ADN de dos personas será idéntico. El 0,1% de las secuencias del código de ADN que varían de persona a persona es lo que hace que cada individuo sea único. La clave para la coincidencia de ADN es saber dónde buscar en los miles de millones de letras del código genético para encontrar los marcadores genéticos que identificarán las similitudes o diferencias importantes entre las personas. Para hacer coincidir, el ADN se aísla de las células y se hacen millones de copias, utilizando un método llamado reacción en cadena de la polimerasa (PCR). La PCR utiliza una enzima natural para copiar repetidamente un tramo específico de ADN. Tener mucho ADN con el que trabajar facilita el análisis del código genético. Luego, las moléculas de ADN se dividen en ubicaciones particulares para separarlas en secciones conocidas, y el código en esos puntos específicos se analiza para crear una huella digital de ADN. Luego se comparan las huellas dactilares de las dos muestras diferentes para ver si coinciden.[72]

¿Qué problemas puede resolver?

·**Actuación.**Debido a que el ADN contiene patrones de material genético que están presentes en todos los seres humanos y son únicos en casi todos los individuos (excepto en los gemelos idénticos), se puede usar para identificar de manera única a una persona, incluso en poblaciones muy grandes.
·**Seguridad.**Los sistemas de comparación basados en el ADN son muy resistentes a la elusión. Aunque los científicos han demostrado que es posible fabricar pruebas de ADN, hacerlo requiere un proceso sofisticado y, por lo tanto, está fuera del alcance de los delincuentes comunes, según algunos expertos.[73]

¿Qué problemas no resuelve?

·**Actuación.**El desarrollo de un identificador único basado en el ADN lleva un tiempo, unos 90 minutos, incluso en una máquina Rapid DNA. Por lo tanto, la tecnología tiene un uso limitado en un sistema de identificación digital.

·**Asequibilidad.**El hardware para desarrollar rápidamente un perfil de ADN es caro (alrededor de US$250.000), y perfilar cada muestra cuesta aproximadamente US$350. Sin embargo, los costos están bajando, con algunos Rapid

harris, w.*Cómo funciona la evidencia de ADN.* Como funcionan las cosas. Obtenido de:https://science.howstuffworks.com/life/genetic/dna-evidence4.htm

¿Cómo funciona la prueba de ADN?(01 de febrero de 2013). BBC. Obtenido de:http://www.bbc.co.uk/science/0/20205874

Traducido: *Francisco Javier González García*

Pollack, A. (17 de agosto de 2009).*La evidencia de ADN se puede fabricar, muestran los científicos.*New York Times. Obtenido de:http://www.nytimes.com/2009/08/18/science/18dna.html

Butkus, B. (04 de octubre de 2012).*Sistemas rápidos de pruebas forenses de ADN de IntegenX, NetBio/GE Healthcare Hit Market.*Genoma Web LLC. Obtenido de:https://www.genomeweb.com/pcrsample-prep/rapid-dna-forensic-testing-systems-integenx-netbioge-healthcare-hit-market

Los sistemas de ADN están disponibles por solo US$150.000 y los costos de procesamiento de muestras se reducen a solo US$150. Una vez que se perfilan las muestras de ADN (por ejemplo, a través de secuenciadores de ADN rápidos), la coincidencia de ADN es relativamente simple. Requiere una capacidad informática y de almacenamiento mínima, lo que resulta en costos de comparación mucho más bajos que otros sistemas de comparación biométrica.

¿Qué problemas podría crear?

.

4.1.8

Adopción. El uso de ADN para la identificación podría conducir a una mayor discriminación contra las personas que buscan acceder a los servicios, porque los proveedores pueden identificar la raza, el género, el historial médico y las relaciones familiares de los usuarios en función del ADN. Las preocupaciones resultantes sobre los aspectos éticos y la privacidad podrían desalentar la adopción de la tecnología. De hecho, una gran controversia en torno al uso del ADN es que permite que las agencias gubernamentales aprendan mucho más sobre un individuo que solo su identidad.

Tendencias clave en biometría

Si bien las tecnologías subyacentes de captura y reconocimiento continúan evolucionando para el reconocimiento de huellas dactilares, rostro e iris, no se anticipan interrupciones tecnológicas importantes. Por ejemplo, los sensores se han vuelto más precisos y pueden leer datos desde distancias más largas, como a través de huellas dactilares sin contacto y escáneres de iris a distancia. La tecnología de coincidencia de huellas dactilares ha avanzado hasta el punto en que algunos algoritmos de coincidencia pueden realizar más de mil millones de coincidencias por segundo. Se están probando escáneres de alta resolución (más de 1000 ppp) para la biometría infantil, y los algoritmos biométricos faciales están avanzando para adaptarse mejor a los rostros fuera del eje, de menor resolución y mal iluminados. En todas estas modalidades, los sensores están evolucionando de manera que sea más difícil engañar a un sistema de reconocimiento biométrico.

Los expertos esperan ver hasta 600 millones de dispositivos con autenticación biométrica para 2021.[75]Para 2020, se pronostica que estarán en uso 50 mil millones de dispositivos de Internet de las cosas (IoT), y se implementarán 500 millones de sensores biométricos para IoT para 2018.[76]De hecho, IoT será un facilitador importante para combinar análisis y evaluación continua para generar un nivel adecuado de garantía, en tiempo real, de que una persona es quien dice ser.

Mientras tanto, los sistemas biométricos multimodales que utilizan una combinación de modalidades de iris, huellas dactilares y rostro probablemente serán los más prometedores para identificar y

autenticar a un individuo. Al prestar atención a la calidad de las fotografías según lo prescrito en los estándares asociados y las mejores prácticas de la ISO y la Organización de Aviación Civil Internacional (OACI), la tecnología de autenticación facial ahora es casi tan precisa como la huella digital para la autenticación. Sin embargo, este no siempre es el caso en los países en desarrollo donde los datos heredados son de muy mala calidad y las pautas de inscripción se aplican de manera deficiente.

Para algunas aplicaciones, los gobiernos u organizaciones utilizarán el reconocimiento de comportamiento como un medio de autenticación continua para garantizar que una persona autenticada al comienzo de la sesión siga siendo la misma durante toda la sesión. Algunas de las primeras implementaciones de autenticación continua hasta la fecha han sido en la industria bancaria europea. Para lograr la autenticación continua, los operadores del sistema podrían utilizar la biometría multimodal, así como parámetros de comportamiento como la geolocalización, los patrones de trabajo y desplazamiento, y el reconocimiento pasivo de voz y rostro.

75 Smith, S. (29 de noviembre de 2016).*El reconocimiento facial y de voz se utilizará en más de 600 millones de dispositivos móviles para 2021*.Investigación de enebro. Obtenido de:https://www.juniperresearch.com/press/press-releases/ voice-and-facial-recognition-to-be-used-in-over-60

76 Badugu, N. (17 de mayo de 2017).*Biometría en la seguridad del Internet de las cosas (IoT)*.IoT UNO. Obtenido de:https://www.iotone.com/guide/biometrics-in-internet-of-things-iot-security/g712

77 Fuente: Kris Ranganath de NEC.

78 Violín, B. (14 de marzo de 2017).*Autenticación continua: por qué está llamando la atención y qué necesita saber.*IDG Communications, Inc. Obtenido de:https://www.csoonline.com/article/3179107/security/continuous-authentication-why-it-s-Getting-attention-and-what-you-need-to-know.html

ENFOQUE: BIOMÉTRICA INFANTIL

Un sistema de identificación digital efectivo es inclusivo. Pero todas las poblaciones contienen grupos para quienes la captura de información biométrica es difícil o incluso imposible, lo que dificulta el registro de miembros en el sistema. La toma de huellas dactilares de los bebés es un ejemplo de ello. La estructura de cresta disponible limitada, debido a los dedos pequeños, y la aversión al proceso de captura dificultan que los dispositivos capturen imágenes con suficiente detalle y calidad para extraer plantillas utilizables de la muestra.

Sin embargo, están surgiendo tecnologías efectivas de captura y comparación biométrica infantil que aumentan las esperanzas de superar este desafío de inclusión. Considere los programas de vacunación. En los países en desarrollo, se gastan miles de millones de dólares cada año para vacunar a los niños, pero solo se administra alrededor del 50% de las vacunas posibles debido a registros de vacunación poco confiables. Un sistema biométrico que incluya a los niños podría permitir a los médicos relacionar a los niños con sus calendarios de vacunación, que generalmente comienzan un mes después del nacimiento de un bebé. Este enfoque también podría mejorar la provisión de servicios de bienestar (como los beneficios de bienestar materno infantil) y rastrear a los bebés que abandonan estos servicios públicos.

Limitaciones actuales

Traducido: *Francisco Javier González García*

Si bien la tecnología biométrica infantil se está probando en varios países, las soluciones para la inscripción de bebés en los sistemas de identificación digital aún están evolucionando. Además, las tecnologías para modalidades biométricas, como las huellas dactilares y las formas de las orejas y los pies, presentan desafíos en lo que respecta a la biometría infantil. Esto se debe a que estos identificadores biométricos cambian sustancialmente a medida que crece el niño. Los investigadores han estudiado el envejecimiento de las plantillas hasta cierto punto (aplicando algorítmicamente el proceso de envejecimiento a las plantillas para simular el envejecimiento), pero esta técnica aún no ha demostrado su eficacia. La modalidad del iris tampoco es factible para los recién nacidos, que no pueden mirar directamente a un dispositivo de escaneo. Además, el iris patrón por lo general, no se estabiliza hasta después de que el niño haya alcanzado la edad de dos años.

También es caro y plantea preocupaciones éticas sobre su uso con fines distintos de la aplicación de la ley.[80]

Algunos países, incluidos India, Perú, Indonesia, Malasia y Tailandia, están inscribiendo a niños en sus sistemas de identificación sin información biométrica. En su lugar, capturan información demográfica y asocian a los niños con sus parientes adultos más cercanos. En estos casos, la información biométrica se captura y procesa una vez que se estabilizan las modalidades, que suele ser después de los cinco años. La información sobre un niño se puede actualizar y actualizar, incluida la adición de detalles biométricos del iris y las huellas dactilares. En el estado indio de Haryana, por ejemplo, los niños se registran en Aadhaar con los datos biométricos de uno de sus padres, junto con el número de Aadhaar de ese adulto. Los datos biométricos del niño deben cargarse cuando el niño tenga cinco años. Mientras tanto, el documento nacional de identidad para niños de Perú utiliza la información biométrica de los bebés (como huellas y una foto) en combinación con las huellas dactilares de los padres.

Un camino a seguir

Para superar los desafíos inherentes a la biometría infantil, los expertos están trabajando para desarrollar y probar dispositivos de captura biométrica diseñados específicamente para bebés. Por ejemplo, los investigadores están probando el uso de modalidades adicionales como la geometría del pie y la forma de la oreja para mejorar la precisión de coincidencia. Fondo para el Bien Mundial y

LaMonica, M. (04 de septiembre de 2014).*La toma de huellas dactilares de los bebés ayuda a realizar un seguimiento de las vacunas en los países en desarrollo.*Revisión de tecnología del MIT. Obtenido de:https://www.technologyreview.com/s/530481/fingerprinting-infants-helps-track-vaccinations-in-developing-countries/

Debates sobre SME de Secure Insights.

Sural, A. (30 de abril de 2015).*Los bebés en Haryana tendrán tarjetas Aadhaar.*Tiempos de India. Obtenido de:https://timesofindia.indiatimes.com/good-governance/haryana/Babies-in-Haryana-will-have-Aadhaar-cards/articleshow/47111358.cms

Debates de One World Identity SME.

Traducido: *Francisco Javier González García*

Element Inc. está utilizando la cámara común en los teléfonos inteligentes para obtener imágenes de una variedad de modalidades infantiles, incluidas las palmas de las manos, los pies y las orejas, y actualmente está realizando pruebas longitudinales en Bangladesh y Camboya. Utilizando inteligencia artificial (IA) y algoritmos de aprendizaje profundo, apunte a desarrollar una solución no táctil para la biometría infantil que pueda implementarse en dispositivos móviles comunes y ejecutarse en áreas de baja conectividad.[83]

Además, NEC y el Dr. Anil Jain, profesor de la Universidad Estatal de Michigan, han desarrollado un escáner de huellas dactilares para bebés de alta resolución que utiliza algoritmos de aprendizaje automático. En un piloto realizado en India, el escáner se utilizó para capturar imágenes de huellas dactilares de más de 300 niños, 100 de los cuales eran bebés. El escáner entregó una precisión del 99 % para niños mayores de seis meses, pero solo una precisión del 80 % para bebés de cuatro semanas. Como parte del mismo piloto, el reconocimiento de huellas dactilares también se está probando con bebés en Benin con el fin de rastrear los registros de vacunación. Sin embargo, dado que las huellas dactilares cambian con el tiempo, los niños deben volver a inscribirse con más frecuencia que los adultos.

Se espera que las tecnologías de reconocimiento biométrico infantil entren en la corriente principal gracias a los avances tecnológicos que mejoran la precisión y reducen los costos. La captura y el uso de la biometría de los niños es un problema emergente. Además de los desafíos técnicos, existen importantes consideraciones éticas que requieren un examen más detenido, sobre las cuales UNICEF ha iniciado recientemente una investigación.

4.2. Tarjetas

Las tarjetas en varios formatos se pueden leer mediante dispositivos de entrada de datos especializados o lectores de tarjetas que utilizan tecnologías que pueden capturar e interpretar códigos de barras o texto a través del reconocimiento óptico de caracteres (OCR), lectores de bandas magnéticas, lectores de tarjetas inteligentes con y sin contacto y otros RFID lectores En las secciones que siguen, se presentan las evaluaciones para cinco formas de tarjetas.

Figura 8: Tarjetas

83*Global Good Fund y Element Inc. para desarrollar tecnología de identificación biométrica para bebés y niños.*(31 de octubre de 2017). Una Identidad Mundial. Obtenido de:https://oneworldidentity.com/element-inc-global-good-fund-create-biometric-health-id-system-infants-children/

4.2.1. Tarjeta no electrónica

Traducido: *Francisco Javier González García*

Tarjeta no electrónica

Las tarjetas de identificación no electrónicas pueden ser tarjetas de plástico, generalmente hechas de PVC o policarbonato, que representan información demográfica básica, como nombre, dirección, fecha de nacimiento, número de identificación digital, fotografía, imagen de firma y nombres de familiares cercanos. Una tarjeta de identificación no electrónica se puede usar como una prueba de identidad con fotografía donde se usan características de seguridad visual para detectar fraudes. Alternativamente, la tarjeta se puede usar para validar un reclamo de identidad usando el número de identificación único para hacer referencia a un registro en una base de datos central. En Sudáfrica, por ejemplo, se lee un número de identidad nacional de la tarjeta de identificación nacional y se envía una huella digital al Sistema Nacional de Identificación de Asuntos Internos (HANIS) para su autenticación.[84]

Los códigos de barras (incluidos 1D: Code 39, Codabar; 2D: PDF417, QR) se utilizan en tarjetas no electrónicas para automatizar el proceso de captura de datos y reducir los errores de perforación.

Con casos de uso limitados para la validación en el lugar, las tarjetas no electrónicas no son completamente a prueba de suplantación de identidad, a menos que estén vinculadas a una base de datos central. Además, sin capacidad de procesamiento o almacenamiento en la propia tarjeta, la tecnología tiene una escalabilidad limitada para las operaciones locales.

¿Qué problemas puede resolver?

·**Madurez.**Las tarjetas no electrónicas se han utilizado durante mucho tiempo y son una de las formas más sencillas de autenticar a las personas. Los códigos de barras o códigos de respuesta rápida (QR) facilitan su integración con otras tecnologías y, por lo tanto, fomentan un alto nivel de interoperabilidad.

*NEC AFIS creó la base de datos de identificación de huellas dactilares civiles más grande del mundo para HANIS.*COMITÉ EJECUTIVO NACIONAL. Obtenido de:http://www .nec.com/en/case/sa/pdf/catalogue.pdf

·**Asequibilidad.**Las tarjetas no electrónicas son muy asequibles a menos que tengan características de alta seguridad. Su facilidad de implementación también genera ahorros de tiempo y costos. Estas tarjetas no requieren ninguna instalación de software específico o incrustación para funcionar, aunque se necesitan lectores de códigos de barras o QR en algunos casos específicos.

·**Adopción.**Al ser principalmente una tarjeta de visualización de información individual, las tarjetas no electrónicas son fáciles de usar y fomentan la adopción inmediata. En la mayoría de los países, muchas personas ya saben cómo funcionan estas tarjetas y cómo usarlas.

¿Qué problemas no resuelve?

·**Seguridad.**Las funciones de seguridad de las tarjetas se limitan a elementos ópticos y mecánicos que no son tan robustos o escalables como las funciones de seguridad electrónica. Las tarjetas perdidas pueden ser utilizadas por cualquier persona que las lleve, a menos que haya una validación biométrica física paralela presente.

·**Escalabilidad.**Las tarjetas no electrónicas no proporcionan un medio eficaz para la autenticación biométrica local. Si bien una plantilla biométrica podría codificarse como un código de barras en la tarjeta para admitir dicho uso local, dichas plantillas se consideran insuficientemente seguras porque no están encriptadas o insuficientemente escalables porque cualquier plantilla encriptada requiere claves que deben distribuirse y protegerse. ***¿Qué problemas podría crear?***

·**Seguridad.**Los dos problemas principales con la tecnología tienen que ver con la seguridad y la escalabilidad. Mientras que una tarjeta inteligente tiene un criptoprocesador y almacenamiento local, una tarjeta no electrónica debe basarse en datos impresos limitados por el tamaño de la tarjeta y la tecnología de código de barras utilizada. Aunque los datos con código de barras se pueden cifrar, sería un esquema de cifrado estático porque no hay un motor criptográfico. Es posible que no se logren los casos de uso que impliquen la implementación de la validación local mediante factores biométricos. Además, las amenazas a la seguridad son mayores con tarjetas no electrónicas, especialmente porque la validación multifactor no es implementable.

4.2.2. Tarjetas no inteligentes RFID

La identificación por radiofrecuencia (RFID) utiliza energía electromagnética para leer la información almacenada en las etiquetas RFID. Según la aplicación, las etiquetas RFID se seleccionan en función de una serie de parámetros, incluida la distancia de lectura; cantidad y velocidad de los datos a transferir; seguridad, tamaño de los documentos y costo. Para muchas aplicaciones de identificación, se prefieren las etiquetas RFID pasivas, en las que la energía electromagnética que se transmite para leer la etiqueta RFID también se usa para alimentarla. Las etiquetas RFID activas se utilizan normalmente para aplicaciones de control de inventario (cadena de suministro) y funcionan con la energía derivada de una fuente interna, normalmente una batería. Además de las etiquetas, un sistema RFID básico incluye lectores y antenas que se utilizan para interrogar las etiquetas.

Esta descripción de RFID pasiva se aplica tanto a las tarjetas inteligentes sin contacto como a las tarjetas RFID no inteligentes. La RFID que no es una tarjeta inteligente utiliza una etiqueta RFID integrada que contiene un microchip con capacidad de computación limitada, memoria limitada y una antena. Las tarjetas RFID pasivas pueden operar a varias distancias según la tecnología seleccionada para la aplicación específica. Este informe se centra en tres tecnologías RFID pasivas que se han adoptado para la autenticación:

1. Proximidad (ISO 14443, alta frecuencia); rango de lectura nominal de 10 centímetros (cubierto en la sección 2.2.4)
2. Vecindad (ISO 15693, alta frecuencia); rango de lectura nominal de 1 metro
3. Largo alcance (ISO 180006-C, frecuencia ultra alta); rango de lectura nominal de 10 metros

Esta sección del informe se centra en las tarjetas no inteligentes RFID, que tienen utilidad en ciertas aplicaciones pero no han visto el mismo nivel de adopción que las tarjetas inteligentes RFID, que se utilizan en aplicaciones electrónicas legibles por máquina.

documentos de viaje (MRTD). Un excelente ejemplo de una aplicación de RFID que no es una tarjeta inteligente es la frontera terrestre de EE. UU., donde se usa RFID de largo alcance para identificar a

los viajeros cuando se acercan a la frontera en vehículos. Las etiquetas RFID de ultra alta frecuencia (UHF) están integradas en las tarjetas de identificación Trusted Traveler (SENTRI y NEXUS). Dichas tarjetas pueden ser utilizadas por estadounidenses, residentes permanentes legales y ciudadanos mexicanos que se hayan inscrito y que crucen la frontera sur en un vehículo inscrito (SENTRI) o crucen la frontera norte (NEXUS) en un vehículo. También pueden ser utilizados por ciudadanos estadounidenses en posesión de un pasaporte estadounidense para viajar a Canadá, México, las Bermudas y el Caribe por un modo que no sea aéreo. El chip RFID almacena solo un número de identificación único para acceder a la información del titular de la tarjeta en una base de datos segura de Aduanas y Protección Fronteriza.[86]

Por diseño, las etiquetas RFID pasivas brindan información cuando las interroga un lector, y la información se limita a un identificador único y otra información de la etiqueta (por lo general, sin PII). Para evitar el acceso no deseado a la tarjeta, se recomienda que las RFID sin contacto se almacenen en una funda de bloqueo de RF similar a las que se proporcionan con los pasaportes estadounidenses y las tarjetas NEXUS y SENTRI.

¿Qué problemas puede resolver?

·**Actuación.**Las tarjetas RFID de largo alcance se pueden leer a distancias de unos 10 metros y se pueden leer en una sucesión rápida. Estas cualidades los hacen útiles para identificar a los viajeros en vehículos cuando se acercan a las fronteras. Además, la RFID de tarjeta no inteligente tiene una ventaja sobre la tecnología de código de barras en el sentido de que no requiere que el documento de identificación esté en la línea de visión del lector de tarjetas, lo que acelera la captura de datos.
·**Seguridad.**Los RFID de largo alcance contienen un número de serie que permite a los usuarios autorizados acceder a la información asociada desde un depósito de datos seguro. No hay PII que requiera seguridad en la tarjeta.
·**Asequibilidad.**La implementación de la tecnología básica de tarjetas RFID requiere una inversión relativamente pequeña, aunque la tecnología es más costosa que la tecnología de código de barras similar.
¿Qué problemas no resuelve?
·**Seguridad.**Cuando las etiquetas RFID no están en sus fundas protegidas, las personas autorizadas y no autorizadas pueden leerlas. Esto genera preocupaciones sobre la privacidad y el posible seguimiento encubierto de cualquier persona que tenga una etiqueta expuesta en su persona.
·**Asequibilidad.**Las etiquetas y los escáneres son más caros que las pegatinas de códigos de barras y los lectores de códigos de barras, una preocupación potencial en los países en desarrollo.
·**Escalabilidad.**La tecnología RFID pasiva carece de la capacidad para almacenar grandes cantidades de datos y carece de potencia de procesamiento, dos capacidades necesarias para soportar operaciones de identificación avanzadas.
¿Qué problemas podría crear?

·**Seguridad.**Si bien las etiquetas RFID han avanzado en complejidad, potencia y flexibilidad, aún son vulnerables a los lectores de RFID no autorizados, que podrían leer la información de la etiqueta y

usarla con fines nefastos. Además, las personas ni siquiera sabrían que sus datos se han visto comprometidos de esta manera. Esto es similar a que alguien asocie el número de placa de un vehículo con un individuo y lo rastree en función de ese número. Los usuarios deben tener cuidado al retirar la RFID de su funda protectora para minimizar las lecturas subrepticias.

*Tarjeta de entrada global.*Aduanas y Protección de Fronteras de EE.UU. Obtenido de:https://www.cbp.gov/travel/trusted-traveler-programs/global-entry/card

86 Nogueira, M. y Greis, N. (diciembre de 2009).*Usos de la tecnología RFID en documentos de identificación de EE. UU. Instituto de Soluciones de Seguridad Nacional.*Obtenido de:https://www.kenan-flagler.unc.edu/~/media/Files/kenaninstitute/CLDS/IHSSResearchBrief_RFID.pdf

4.2.3. Tarjetas inteligentes de contacto

Una tarjeta inteligente de contacto es una credencial física con un microchip integrado y una unidad de procesamiento que está diseñada para operar cuando está en contacto físico con un lector de tarjetas. El microchip incluye un procesador, memoria y un controlador criptográfico que proporciona velocidades de procesamiento más altas y mejor seguridad que las tarjetas de memoria diseñadas para almacenar más datos. Estas tarjetas siguen el protocolo ISO 7816 y han tenido una amplia adopción en muchos países, incluidos Arabia Saudita, Pakistán, Kuwait y Sudáfrica. Los gobiernos los utilizan para permitir que las personas accedan de forma segura a múltiples servicios. En Pakistán, por ejemplo, la Tarjeta Nacional de Identidad Computarizada (CNIC) emitida por la Autoridad Nacional de Registro y Base de Datos (NADRA) se ha integrado con hasta 336 servicios. Las personas deben usar la tarjeta para votar, abrir una cuenta bancaria, solicitar un pasaporte o licencia de conducir, comprar boletos de avión o tren y completar muchos procesos más.

Las tarjetas inteligentes de contacto también pueden actuar como una tarjeta de pago o de crédito. MasterCard y NADRA, por ejemplo, están optimizando CNIC para pagos electrónicos.[88,89]

¿Qué problemas puede resolver?

·**Seguridad.**Las tarjetas inteligentes de contacto permiten a las personas ejecutar transacciones en línea y fuera de línea de manera segura según su conveniencia. La validez de los usuarios se puede confirmar fuera de línea a nivel local, eliminando la necesidad de transferir datos a través de una red y evitando así las vulnerabilidades de red asociadas. Además, la comunicación se puede hacer más segura utilizando las capacidades incorporadas de hash, firma digital y cifrado de las tarjetas.
·**Escalabilidad.**La tecnología puede almacenar suficientes datos de identidad y realizar cálculos criptográficos, por lo que se presta para su uso en muchos servicios diferentes. A medida que la tecnología ha evolucionado, las tarjetas han podido almacenar y transmitir volúmenes de datos cada vez mayores con mayor velocidad y potencia informática.
·**Adopción (integración).**La capacidad de agregar otras aplicaciones a la tarjeta es otra ventaja importante. Dependiendo de la cantidad de memoria disponible, las tarjetas inteligentes pueden servir como credenciales de múltiples aplicaciones que se utilizan para muchos propósitos, incluido el acceso físico a las instalaciones y el seguimiento del tiempo que pasan y la asistencia a una instalación. Por lo tanto, las tarjetas inteligentes ofrecen una

gran flexibilidad.

¿Qué problemas no resuelve?

·**Escalabilidad.**Las tarjetas inteligentes de contacto requieren un lector que los operadores pueden tener que adquirir e instalar si su dispositivo informático aún no tiene uno.

·**Actuación.**Las tarjetas inteligentes deben estar en contacto con el lector y la información se recupera a una velocidad relativamente baja. Una foto en una tarjeta inteligente, por ejemplo, puede tardar varios segundos en leerse.

·**Asequibilidad.**Aunque las tarjetas inteligentes con contacto requieren una inversión inicial menor que las tarjetas inteligentes sin contacto, los costos generales aún pueden ser altos.

·**Seguridad.**La tecnología es moderadamente vulnerable a la elusión. Esto se debe a que la autenticación de las personas se basa en un PIN (y un PIN se puede observar o adivinar). Alternativamente, la autenticación puede basarse en datos biométricos. La referencia biométrica se recupera de la tarjeta inteligente y se compara con una biométrica en vivo capturada en un sensor externo, lo que permite la presentación o el intermediario

Aarti R. (30 de julio de 2009).*Tipos de Tarjetas Inteligentes.*Zumbido. Obtenido de:https://www.buzzle.com/articles/types-of-smart-cards.html

88 Reportero del personal (19 de enero de 2017).*Mastercard y NADRA firman acuerdo sobre facilidad de pago electrónico CNIC.*Amanecer. Obtenido de:https://www.dawn.com/news/1309369

*Documento Nacional de Identidad informatizado.*Obtenido de:https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Computerised_National_Identity_Card.html

L

ataques Se deben consultar las listas de revocación de certificados (CRL) para determinar si una tarjeta inteligente de contacto sigue siendo válida. Esto requiere conectividad en tiempo real o conectividad a intervalos para descargar localmente las últimas CRL.

¿Qué problemas podría crear?

·**Seguridad.**Si la tarjeta está asegurada con un PIN de cuatro dígitos, por ejemplo, los infractores podrían acceder a la información protegida con relativa facilidad si la tarjeta no se bloqueara después de varios intentos fallidos.

4.2.4. Tarjetas o documentos inteligentes sin contacto

Una tarjeta inteligente sin contacto (ISO 14443) es una credencial física con un microchip integrado similar al de una tarjeta inteligente de contacto como se describe anteriormente. Proporciona capacidades de procesamiento similares, pero con la adición de un transceptor de radiofrecuencia (RF) y una antena diseñada para operar cuando se encuentra cerca de un lector de tarjetas. La tarjeta se alimenta de la energía electromagnética que emana del lector.

Las tarjetas inteligentes sin contacto tienen las mismas dimensiones físicas que las tarjetas inteligentes con contacto y, por lo general, comparten las mismas opciones de procesador. Sin

embargo, las tasas de transmisión de datos sin contacto tienden a ser más lentas que las de la transmisión de datos con contacto.

Estas tarjetas también pueden tomar la forma de documentos, incluidos los pasaportes electrónicos. La tecnología es valiosa para aplicaciones que requieren protección de información personal y comunicación segura con el dispositivo sin contacto. La inteligencia en el chip permite que los sistemas cumplan con las pautas de privacidad y seguridad.

¿Qué problemas puede resolver?

·**Seguridad.**Una contraseña para la identificación de personas hace que la tecnología sea moderadamente resistente a la elusión. Y utilizando un chip de circuito integrado, la criptografía protege la información sobre el titular de la tarjeta y los programas para las múltiples aplicaciones almacenadas en la tarjeta.
·**Adopción (integración).**Decenas de millones de tarjetas inteligentes sin contacto en forma de eMRTD están en uso en todo el mundo y no se espera que estas cifras disminuyan en el futuro cercano. La tecnología puede almacenar suficientes datos de identidad y realizar cálculos criptográficos, por lo que se presta para su uso en muchos servicios diferentes. A medida que la tecnología ha ido evolucionando, las tarjetas han podido almacenar y transmitir cada vez más datos con mayor velocidad y potencia de cómputo.
¿Qué problemas no resuelve?
·**Actuación.**Aunque las velocidades de lectura han aumentado a lo largo de los años, sigue siendo un factor de activación. Por ejemplo, alrededor de un tercio del tiempo promedio que se tarda en atravesar un e-Gate se dedica a leer un pasaporte electrónico (alrededor de 5 segundos).
·**Escalabilidad.**La escalabilidad de la red es media porque la tecnología se basa en una red para verificaciones de CRL en tiempo real o descargas intermitentes a un caché local, por ejemplo.
·**Asequibilidad.**Una tarjeta suele costar entre US$2 y US$10, lo que puede ponerla fuera del alcance de las personas de bajos ingresos, a menudo las mismas personas que más necesitan una identificación para acceder a los servicios.

90 “Un ataque en el que el atacante se mantiene entre dos partes, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación está siendo controlada por el atacante” Tanmay Patange.*Cómo defenderse del ataque MITM o Man-in-the-middle.*El Club de las Ventanas. Obtenido de:http://www.thewindowsclub.com/man-in-the-middle-attack

*Organización de Aviación Civil Internacional (2015).*Documentos de viaje de lectura mecánica. OACI, 7ª edición. Obtenido de:https://www.icao.int/publications/Documents/9303_p4_cons_en.pdf

¿Qué problemas podría crear?

·**Seguridad.**Las tarjetas inteligentes sin contacto, al igual que las tarjetas inteligentes con contacto, pueden usar PIN que se pueden observar o adivinar. Además, al igual que en el caso de las tarjetas RFID no inteligentes, se aplica una estrategia de mitigación y vulnerabilidad de rastreo RFID similar en el caso de las tarjetas inteligentes sin contacto.

Traducido: *Francisco Javier González García*

4.2.5. Sistema Biométrico en Tarjeta (BSoC)

La tecnología de sistema biométrico en tarjeta (BSoC) combina el sensor biométrico y el comparador en una tarjeta inteligente, normalmente una tarjeta del tamaño de una tarjeta de crédito de conformidad con la norma ISO 7810. Por lo tanto, mejora las soluciones de emparejamiento en tarjeta, que contienen solo el emparejador. El sensor captura la muestra biométrica y, a continuación, el procesador extrae las características biométricas de la imagen y las compara con el conjunto de características registradas para su verificación. BSoC nunca transfiere ninguna muestra o datos a un terminal externo.

Mastercard y VISA han presentado recientemente su tarjeta biométrica de próxima generación que combina tecnología de chip con biometría. Los clientes ahora pueden establecer fácilmente su identidad para compras en la tienda a través de sus huellas dactilares en máquinas Europay, Mastercard y VISA (EMV) y pueden pagar a través del móvil.

¿Qué problemas puede resolver?

·**Seguridad.**La autenticación biométrica se realiza cuando el titular legítimo de la tarjeta está presente, lo que mejora la seguridad. La tecnología también es altamente resistente a la elusión. La transmisión de datos es segura porque solo se transmite el resultado de la autenticación, no la PII.
·**Escalabilidad.** Debido a que la tarjeta realiza la comparación localmente, la información de huellas dactilares no necesita transmitirse a un servidor central, lo que mejora la escalabilidad de la tecnología.
·**Asequibilidad.**Aunque los BSoC son más caros que las tarjetas inteligentes estándar, eliminan la necesidad de costosos lectores de huellas dactilares externos.
·**Actuación.**La precisión de la autenticación es moderada debido al tamaño del sensor, pero la velocidad de coincidencia es alta porque el proceso se realiza localmente.
¿Qué problemas no resuelve?
·**Madurez.**La tecnología ofrece una interoperabilidad moderada porque los estándares de intercambio no se han desarrollado ni definido por completo.
·**Asequibilidad.**Dado el costo de estas tarjetas, las agencias que estén considerando usar esta tecnología deben realizar análisis de costo-beneficio para evaluar las ventajas y desventajas de adoptar esta solución.
·**Actuación.**El sensor puede sufrir un desgaste excesivo si no se maneja correctamente, lo que podría disminuir la capacidad del dispositivo para realizar autenticaciones biométricas precisas.
¿Qué problemas podría crear?
·**Adopción.**La experiencia de usar estas tarjetas será cuestionable para aquellos con huellas dactilares deficientes, aquellos que no usan la tecnología para familiarizarse lo suficiente con ella y aquellos que manejan mal la tarjeta, especialmente el sensor.

4.2.6. Tendencias clave en tarjetas

Traducido: *Francisco Javier González García*

Se espera que las tarjetas de identificación digitales en circulación global aumenten de 1750 millones en 2013 a 3300 millones en 2021. De esto, 103 países emitirán un total de 3200 millones de tarjetas inteligentes de identificación nacional.[92]

A principios de 2017, el 82% de todos los países que emiten tarjetas de identificación oficiales han implementado programas que dependen de tarjetas inteligentes o tarjetas de plástico y biometría.[93]

Otras innovaciones en tarjetas incluyen NFC, comunicación inalámbrica que permite el intercambio de datos entre dispositivos que están separados por unos pocos centímetros. Los dispositivos habilitados para NFC, junto con las aplicaciones de identificación electrónica móviles, permiten la autenticación móvil en el sistema de tarjetas de identificación de Alemania. La tecnología de baliza Bluetooth de bajo consumo es una innovación en el dominio de las características de las tarjetas opcionales. La baliza puede encontrar la ubicación de un dispositivo inteligente y usar transmisores para enviar información pertinente a dispositivos habilitados para Bluetooth.

Muchos países ahora están implementando tarjetas con seguridad biométrica incorporada para sus respectivos programas nacionales de identificación. El gobierno de Maldivas lanzó recientemente una identificación nacional basada en una tarjeta inteligente biométrica llamada "Tarjeta de pasaporte" para sus ciudadanos en colaboración con Mastercard. Contiene una combinación única de chip de interfaz dual para lectura de tarjetas sin contacto y con contacto. Esta tarjeta funciona como pasaporte, licencia de conducir e identificación nacional del titular de la tarjeta, y el gobierno puede usarla para brindar servicios de salud y electrónicos. También funciona como una tarjeta de pago para realizar pagos.[94]La tarjeta contiene 10 huellas dactilares para una verificación segura.

Las tarjetas inteligentes sin contacto están siendo adoptadas cada vez más por muchos programas de identidad nacional, como la tarjeta de identidad alemana y MyKad, la tarjeta de identidad emitida por el gobierno de Malasia a sus ciudadanos. MyKad es una tarjeta inteligente multipropósito sin contacto emitida por el Gobierno de Malasia que funciona como tarjeta de identificación, licencia de conducir, pasaporte, tarjeta de tránsito y documento de salud. La tarjeta almacena la información de la huella dactilar del titular de la tarjeta a la que puede acceder un lector para verificar a la persona.

La tarjeta de identidad alemana es una tarjeta inteligente sin contacto emitida a los ciudadanos de Alemania. La tarjeta inteligente sin contacto se basa en tecnología RFID y se puede leer desde una distancia de solo 4 centímetros. Además, el chip está protegido por un PIN que evita que los datos se divulguen a menos que se ingrese el PIN correcto. La comunicación entre la tarjeta y el lector también está encriptada. Este documento de identidad también se puede utilizar como documento de viaje válido entre países de la Unión Europea.[95]

En el futuro, es probable que las tarjetas biométricas tengan un sensor biométrico integrado en lugar de simplemente almacenar una plantilla biométrica. El sensor integrado en un modelo de tarjeta reemplazará la necesidad de PIN y contraseñas y funcionará solo después de que el titular de la tarjeta lo active utilizando su información biométrica. Si bien la huella dactilar sigue siendo la principal biométrica utilizada en dichas tarjetas, existe la posibilidad de utilizar otras métricas, como la electrocardiografía (ECG).[97]

Informe mundial de la industria nacional de identificación electrónica: edición de 2017 por Acuity Market Intelligence.

Traducido: *Francisco Javier González García*

Informe mundial de la industria nacional de identificación electrónica: edición de 2017 por Acuity Market Intelligence,

94 Mastercard (26 de octubre de 2017).*Mastercard y Bank of Maldives presentan Passport Card en asociación con Inmigración de Maldivas.*Tarjeta MasterCard. Obtenido de:https://newsroom.mastercard.com/asia-pacific/press-releases/mastercard-y-bank-of-maldives-presentan-pasaporte-tarjeta-en-asociación-con-maldivas-inmigración/

95 Ryan Kline (01 de febrero de 2011).*Alemania implementa identificación nacional sin contacto*.SecureIDNews.com. Obtenido de:https://www.secureidnews.com/news-item/germany-deploys-contactless-national-id/

96 Alan Goode (15 de diciembre de 2016).*Tendencias biométricas para 2017*.Veridiumid.com. Obtenido de:https://www.veridiumid.com/blog/tendencias-biometricas-para-2017/

97 Tseng, K.-K., Huang, H.-N., Zeng, F. y Tu, S.-Y. (2015).*Tarjeta de sensor de ECG con algoritmos RBP en evolución para verificación humana*.Sensors (Basilea, Suiza), 15(8), 20730–20751. Obtenido de:https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4570445/

4.3.Tecnologías de apoyo para tarjetas

Las tecnologías de soporte para las tarjetas incluyen códigos de barras, bandas magnéticas, características de seguridad física y texto legible por máquina (consulte la Figura 10). La Figura 11 muestra las evaluaciones para cada uno de estos.

Figura 10: Tecnologías de soporte para tarjetas

Las tecnologías de soporte para tarjetas como las descritas en las secciones anteriores podrían complementarse con otras características descritas en esta sección. Estas características pueden aumentar la velocidad de lectura de tarjetas físicas, proporcionar medios alternativos para leer la información contenida en las tarjetas o hacer que estas tarjetas sean más seguras.

4.3.1. códigos de barras

Los códigos de barras son símbolos legibles por máquina que se utilizan para codificar información sobre un producto. Comprenden un patrón de líneas con diferentes anchos (códigos de barras 1D) o rectángulos, puntos, hexágonos y otros patrones geométricos en dos dimensiones (códigos de barras 2D). Son leídos por escáneres ópticos especiales. Hoy en día, las personas pueden usar sus dispositivos móviles para escanear códigos de barras y encontrar información de interés, como características y precios de los productos que están considerando comprar. La tecnología es madura y se usa ampliamente en tarjetas de identificación nacionales, incluso en Argentina, Costa Rica y Bosnia y Herzegovina (por nombrar algunos).

Los gobiernos están comenzando a utilizar códigos de barras que se generan automáticamente de acuerdo con la información ingresada por un individuo, en la fase de preinscripción del ciclo de vida de la identidad. Las personas completan un formulario en línea, que genera un código de barras que captura la información del formulario.

Traducido: *Francisco Javier González García*

En Egipto se utilizaron tarjetas de votante con código de barras que contenían datos biométricos para autenticar a las personas durante las últimas elecciones. Los datos biométricos se pueden almacenar en las tarjetas de votante en forma de código de barras 2D o en un chip integrado. Se escanea la credencial de votante y se capturan las huellas dactilares o el iris del votante y se comparan con los datos biométricos de referencia almacenados en la credencial de votante o en una base de datos local. Los datos codificados en el código de barras 2D de la tarjeta incluyen una firma criptográfica utilizada para validar la integridad y autenticidad del código de barras.

¿Qué problemas puede resolver?

·**Actuación.**La tecnología de código de barras tiene un alto rendimiento y precisión en comparación con la entrada manual (con una tasa de error de solo 1 de cada 36 millones de caracteres escaneados). Por lo tanto, se presta al procesamiento de datos de gran volumen para aplicaciones de identificación.
·**Madurez.**Los códigos de barras se han utilizado durante décadas y han demostrado su eficacia para la captura de datos de bajo volumen con línea de visión.
·**Asequibilidad.**Los costos de hardware y software para esta tecnología son relativamente bajos, por lo que vale la pena considerarlos para los sistemas de identificación.
·**Adopción.**La tecnología es fácil de integrar con los sistemas existentes.***¿Qué problemas no resuelve?***
·**Actuación.**El código de barras debe estar en la línea de visión del dispositivo de lectura. La precisión del escaneo de códigos de barras puede verse comprometida por factores como inconsistencias en la impresión, desgaste del código de barras, contrastes de color inadecuados entre los elementos claros y oscuros del código de barras y posicionamiento incorrecto del lector de códigos de barras.
·**Escalabilidad.**La cantidad de datos que se pueden codificar en un código de barras está limitada incluso con esquemas de codificación de alta densidad. Por ejemplo, la codificación QR en modo byte está limitada a 2953 bytes.

4.3.2. Rayas Magnéticas

Una banda magnética, o Magstripe, consta de diminutas partículas de hierro esparcidas sobre una película similar al plástico. y magnetizado en una determinada orientación. Un escáner magnético lee la banda y traduce los impulsos electrónicos en datos. La tecnología es muy madura y tiene una alta penetración en el mercado. Es ampliamente utilizado en tarjetas de crédito y débito y se utiliza en algunas tarjetas de identidad para diversas necesidades. En los Estados Unidos, el

*Protección de datos y confidencialidad para garantizar procesos fiables en la organización de elecciones democráticas.*Zetes. Obtenido de:http://peopleid.zetes.com/en/solution/elections

¿Cómo funciona una banda magnética en el reverso de una tarjeta de crédito?(14 de abril de 2008). HowStuffWorks.com. Obtenido de:http://money.howstuffworks.com/personal-finance/debt-management/magnetic-stripe-credit-card.htm

Traducido: *Francisco Javier González García*

La tarjeta de verificación de identidad personal (PIV) incluye una banda magnética opcional compatible con ISO 7811 para codificar un número de credencial de tarjeta inteligente de agencia federal (FASC-N).[100]

¿Qué problemas puede resolver?

·**Adopción.**La tecnología de banda magnética es fácil de usar y requiere poca capacitación.
·**Asequibilidad.**Los costos asociados con las tarjetas y los lectores de banda magnética son más bajos que los de las tarjetas inteligentes y solo un poco más altos que los de las tarjetas plásticas genéricas. Por ejemplo, cuesta menos de US$1 producir una tarjeta.[101]
¿Qué problemas no resuelve?
·**Seguridad.**Los datos contenidos en la banda magnética se pueden leer y clonar, sin embargo, no es una preocupación muy apremiante ya que en un sistema de identificación nacional, estas bandas magnéticas se utilizan como un índice para una identificación en una base de datos central. Por lo tanto, la simple clonación de la banda magnética no servirá de nada para un atacante, ya que el sistema podrá identificar a un suplantador en función de la huella dactilar correspondiente o de los datos fotográficos.
·**Actuación.**Las bandas magnéticas se basan en la tecnología de contacto, y tanto el lector como la banda magnética son propensos a la degradación por el desgaste.

4.3.3. Texto legible por máquina

La tecnología de texto legible por máquina utiliza algoritmos para optimizar y reconocer caracteres dentro de las imágenes y convertirlos en texto legible por seres humanos. La tecnología ha sido ampliamente adoptada en una amplia gama de industrias. Todos los MRTD que cumplen con la OACI incluyen una zona legible por máquina (MRZ) que se puede leer usando la tecnología OCR. En estos MRTD, la fuente (OCR-B), el color de la tinta (B425 – B680 según ISO 1831) y otros elementos se especifican para optimizar el rendimiento de OCR. Sin embargo, estas características no son necesarias para leer información de documentos de identidad utilizando tecnología OCR.
¿Qué problemas puede resolver?
·**Actuación.**La entrada de datos de texto legible por máquina a través de OCR es más rápida, más precisa y más eficiente que la entrada de datos con pulsaciones de teclas. Con OCR, los datos se pueden leer de documentos en papel con tasas de reconocimiento de caracteres instantáneos superiores a 4000 caracteres por segundo.[102]
·**Escalabilidad.**El texto legible por máquina y la tecnología OCR ayudan a las organizaciones gubernamentales a escalar sus procesos de registro mientras mantienen la confiabilidad, la precisión y la velocidad. La tecnología también puede adaptarse a una amplia variedad de formatos de entrada. Además, utiliza una arquitectura modular que es abierta y escalable.
·**Asequibilidad.**Los escáneres equipados con OCR pueden costar tan solo 150 dólares estadounidenses, frente a los varios miles de dólares estadounidenses de las unidades de

alimentación automática de alta capacidad. Las organizaciones que utilizan esta tecnología pueden reducir significativamente sus costos de mano de obra al reemplazar la entrada y las correcciones manuales.

nstituto Nacional de Estándares y Tecnología (agosto de 2013).*Verificación de Identidad Personal (PIV) de Empleados Federales y Contratistas. NIST.*Obtenido de:https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

101*dhgate.*Obtenido de:https://www.dhgate.com/wholesale/magnetic+stripe+card.html

102 Herbert F. Schantz.*Reconocimiento óptico de caracteres: la tecnología madura con un futuro brillante.*Conexión ECM.

Obtenido de:https://www.ecmconnection.com/doc/optical-character-recognition-the-mature-tech-0001

¿Qué problemas no resuelve?

·**Actuación.**La velocidad y la precisión de OCR son menores para el texto escrito a mano que para el texto escrito a máquina. Las tasas de precisión han estado en el alto percentil 90. Otros factores pueden erosionar la precisión, incluida la calidad de la imagen, el tipo y tamaño de fuente, el espacio entre palabras y el ancho de la columna de texto.
·**Escalabilidad.**El texto legible por máquina requiere que las tarjetas de identificación estén en la línea de visión de los dispositivos lectores.

4.3.4. Funciones de seguridad física

Las credenciales físicas utilizadas para la identificación pueden incorporar características de seguridad ópticas y físicas que dificultan que los falsificadores y los suplantadores creen tarjetas no autorizadas. Muchos países utilizan estas características de seguridad en sus tarjetas de identificación digitales y pasaportes. para proporcionar capacidades anti-falsificación a estas credenciales. Las características de seguridad óptica y física que se usan comúnmente en la actualidad incluyen las siguientes:
·**Holograma.**Un holograma es un gráfico de apariencia tridimensional creado mediante tecnología láser que se coloca en cualquier lugar de la superficie de la tarjeta antes de la laminación. Cuando se rompen los hologramas verdaderos, cada pieza muestra la imagen original completa, pero desde una perspectiva diferente cada vez que se ve la tarjeta desde un ángulo diferente. Por lo tanto, los hologramas son difíciles de recrear.
·**Imágenes fantasma.**Una imagen fantasma es un gráfico semi visible (generalmente otra foto del titular de la tarjeta) aplicado a la tarjeta. Los hologramas o logotipos con imágenes fantasma impresos en combinación con números de identificación son particularmente difíciles de falsificar.105
·**Microimpresión.**La microimpresión parece una línea delgada ordinaria a simple vista. Pero consta de caracteres diminutos que miden menos de 0,3 mm de altura, generalmente legibles solo con una lupa o un microscopio.
·**Táctil.**Se crea una impresión de una imagen específica en la tarjeta justo antes de la laminación. Las agencias y organizaciones gubernamentales pueden crear sus propias características táctiles que van en cada tarjeta que imprimen. Algunas agencias ven los

elementos táctiles como la forma más segura y rentable de garantizar la seguridad de la tarjeta. Esto se debe a que la imagen táctil se daña gravemente si alguien intenta manipular la tarjeta con fines de suplantación o falsificación. Cuando lo táctil se combina con un laminado holográfico, la seguridad mejora aún más.

·**Impresión de arcoíris.**La impresión de arcoíris se usa típicamente para desalentar la falsificación. La técnica consiste en imprimir gradientes de múltiples colores en la superficie de un material a través de un proceso de litografía altamente sofisticado. La combinación de sofisticación técnica y gran inversión requerida para usar esta técnica hace que sea muy difícil de copiar.

La efectividad de las características de seguridad ópticas y físicas depende de las habilidades del inspector de documentos. Incluso las personas que tienen un conocimiento sólido de las funciones de seguridad pueden no detectar tarjetas falsas; por ejemplo, si no se toman el tiempo suficiente para inspeccionar una tarjeta. Cuando se requieran funciones de seguridad mejoradas, se pueden implementar las funciones de seguridad electrónica de las tarjetas inteligentes. En el contexto de los sistemas de identidad, el Documento 9303 de la OACI define muchas opciones de seguridad electrónica disponibles para proteger los datos y los intercambios de datos.

La elección de las características de seguridad también afecta el material utilizado para producir tarjetas de identificación y, por lo tanto, el proceso y los costos de fabricación. Por ejemplo, aunque los materiales como el PVC son económicos, las características como

Bundesdruckerei GmbH (enero de 2014).*Elementos de Seguridad de la Tarjeta de Identidad Alemana.*Obtenido de:https://www .bundesdruckerei.de/de/system/files/dokumente/pdf/Flyer-Security-Features-German-ID-Card.pdf.pdf

Woodford, C. (2008/2017).*hologramas.* Obtenido de:http://www.explainthatstuff.com/hologramas.html

Chen, W. y Chen, X. (noviembre de 2013).*Imagen fantasma para seguridad óptica tridimensional.*Letras de Física Aplicada,
103(22), págs. 221106–2211064. Obtenido de:http://aip.scitation.org/doi/full/10.1063/1.4836995

Myers, W. (25 de octubre de 2016).*Impresiones táctiles para tarjetas de identificación seguras: seguridad e impacto de marca que puede ver y sentir.*Racó
Industrias. Obtenido
de:https://racoindustries.com/tactile-impressions-secure-id-cards-security-brand-impact-can-see-feel/

*Detección de billetes falsos: una guía para detectar billetes falsos: huecograbado.*Imagen índigo. Obtenido de:https://www
.indigoimage.com/count/feat2.html#intdetail

el grabado láser o el estampado en relieve no funcionan bien con ese material. Y a medida que se agregan más funciones a una tarjeta, se requieren materiales subyacentes más costosos para imprimir las tarjetas, lo que aumenta los costos de producción.[108]

4.3.5. Tendencias clave en tecnologías de tarjetas

A medida que la tecnología de los escáneres siga evolucionando, habrá menos necesidad y demanda de códigos de barras 1D, ya que solo pueden contener información limitada, un máximo de 85 caracteres. Por el contrario, los códigos de barras 2D pueden almacenar más de 7000 caracteres, lo que permite la transmisión de más de una página de texto. Los códigos de barras 2D pueden codificar hasta 500 bytes por pulgada cuadrada, lo que permite almacenar datos biométricos, como la

captura de huellas dactilares y firmas, o versiones comprimidas de retratos de titulares de tarjetas. Esta característica no es posible con códigos de barras lineales 1D.

Se están realizando investigaciones para agregar más dimensiones a los códigos de barras 2D para codificar más datos en ellos. Los códigos de barras 3D se han creado usando espacio (barras/cuadrados sobresalientes)[110]y color (barras/cuadrados codificados por colores).[111]Es probable que los códigos de barras 3D sobresalientes sean muy resistentes a las alteraciones y requerirán lectores especializados, ya que se grabarán directamente en la superficie de un producto. Hay más investigaciones sobre la creación de códigos de barras 4D utilizando la altura, el ancho, el color y el tiempo como cuatro dimensiones para codificar datos. Estos códigos de barras 4D utilizarán códigos de barras 2D de colores multiplexados en el tiempo para transmitir grandes cantidades de datos. Sin embargo, estos solo se pueden mostrar en dispositivos móviles o espaciales.[112]

Se han realizado algunas investigaciones sobre la tecnología de tarjetas multifunción que permite utilizar una sola tarjeta para realizar retiros bancarios en cajeros automáticos, compras con tarjeta de crédito o como tarjeta de fidelización simplemente presionando un botón para reprogramar su funcionamiento. Hay poca evidencia de pruebas de esta tecnología en el contexto de la identificación digital, pero las tarjetas multifunción que usan bandas magnéticas podrían permitir que una sola tarjeta de identificación cumpla múltiples funciones si se implementan. Algunas de las tarjetas más recientes también tienen un sistema global para antena celular móvil (GSM) en el interior que puede conectarse a una red móvil. Estas tarjetas se pueden programar instantáneamente con los detalles requeridos usando la conexión celular de la tarjeta. Si la información del titular de la tarjeta se ve comprometida, en lugar de tener que esperar por una tarjeta de reemplazo, estas tarjetas podrían programarse electrónicamente con nueva información para que el usuario pueda continuar usándola casi al instante.[113]

Las tarjetas con características de seguridad mejoradas hacen que sea muy difícil para los fraudes tradicionales como el robo de tarjetas (la copia ilegal de información de la tarjeta, en la banda magnética o en el chip). Algunas tarjetas interactivas no contienen información mientras están apagadas y se consideran seguras de skimming y podría prevenir el robo de identidad. Para encender el dispositivo, el usuario debe ingresar un código de desbloqueo en la tarjeta. Si el usuario ingresa el código de desbloqueo correcto, la tarjeta mostrará visualmente el número de tarjeta del usuario y la franja se completará con la información magnética correcta. Después de un período de tiempo, la pantalla se apaga y la franja se borra sola, eliminando así toda la información crítica de la superficie de la tarjeta.[1]

Martín, Z. (11 de agosto de 2015).*Los materiales de tarjeta avanzados permiten características de seguridad en capas.*Noticias de identificación segura. Obtenido de:https://www.secureidnews.com/news-item/advanced-card-materials-enable-layered-security-features/

Brian Sutter (26 de mayo de 2015).*Futuro de los códigos de barras, RFID y códigos de barras de imágenes; Cómo afectarán el código de barras IOT Wasp.*Obtenido de:http://www.waspbarcode.com/buzz/future-barcodes/

110 Gladstein, D., Kakarala, R. y Baharav, Z.*Códigos de Barras 3D: Aspectos Teóricos e Implementación Práctica.*Biblioteca Digital SPIE. Obtenido de:http://www.spiedigitallibrary.org/conference-proceedings-of-spie/9405/1/3D-barcodes-theoretical-aspects-and-practical-implementation/10.1117/12.2082864.short?SSO=1

Traducido: *Francisco Javier González García*

Koddenbrock et al. (2016).*Un innovador código de barras en color 3D: Visualización intuitiva y realista de datos digitales.*Actas de la 17.ª Conferencia Internacional sobre Sistemas y Tecnologías Informáticas 2016, págs. 175–181. Obtenido de:https://dl.acm.org/citation.cfm?id=2983486&dl=ACM&coll=DL

Langlotz, T. y Bimber, O.*Códigos de barras 4D no sincronizados.*ISVC'07 Actas de la 3.ª conferencia internacional sobre avances en computación visual: volumen, parte I, págs. 363–374. Obtenido de:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.9056&rep=rep1&type=pdf

Andrew Liszewski (11 de enero de 2018).*Esta tarjeta de crédito inteligente con conexión celular puede mostrarle. Cuánto dinero te queda para gastar.*Gizmodo. Obtenido de:https://gizmodo.com/this-cell-connected-smart-credit-card-can-show-you-1821972060

Vishal Chawla (18 de enero de 2018).*Las tarjetas de pago se están convirtiendo en minicomputadoras.*Mundo de la informática. Obtenido de:http://www.computerworld.in/feature/how-payment-cards-are-evolving-mini-computers

Michael Kassner (20 de septiembre de 2010).*Fraude con tarjetas de débito/crédito: ¿pueden prevenirlo las tarjetas de pago inteligentes?*República tecnológica. Obtenido de:https://www.techrepublic.com/blog/it-security/debit-credit-card-fraud-can-smart-payment-cards-prevent-it/

4.4. Móvil

La rápida proliferación de dispositivos móviles inteligentes, la rápida mejora de las capacidades de las redes inalámbricas y la adopción de tecnologías en la nube han dado como resultado soluciones de identidad móvil fáciles de proporcionar y usar. Con la caída de los precios de los teléfonos inteligentes, cada vez más personas en los países en desarrollo comienzan a acceder a Internet. En India, por ejemplo, se espera que la cantidad de usuarios de Internet llegue a 450–465 MN para junio de 2017. Además, los indios accedieron a Internet a través de sus móviles casi el 80% del tiempo en 2017,[117]lo que implica que el acceso a los servicios digitales en línea será más a menudo a través del uso de un teléfono móvil. Claramente, las tecnologías de autenticación e identificación móvil serán importantes particularmente en los países en desarrollo.

Chopra, A. (02 de marzo de 2017).*El número de usuarios de Internet en la India podría superar los 450 millones en junio: Informe.*LiveMint. Obtenido de:http://www.livemint.com/Industry/QWzIOYEsfQJknXhC3HiuVI/Number-of-Internet-users-in-India-could-cross-450-Million-by.html

Bhattacharya, A. (29 de marzo de 2017).*El uso de Internet en India demuestra que los escritorios son solo para occidentales*. Obtenido de:https://qz.com/945127/internet-use-in-india-proves-desktops-are-only-for-westerners/

Las tecnologías móviles relacionadas con la identidad consisten en soluciones de hardware y software basadas en teléfonos y tabletas que se utilizan para registrar, autenticar y verificar la identidad de una persona.

Unir los dominios de credenciales de lo físico a lo móvil es la credencial derivada, que es un medio para implementar una credencial en un dispositivo móvil donde se aplicarían los mismos niveles de garantía del autenticador (AAL). Por ejemplo,*Directrices del NIST para credenciales de PIV derivadas* señala que “En respuesta al uso creciente de dispositivos móviles dentro del gobierno federal, se revisó FIPS 201 para permitir la emisión de una credencial adicional, una Credencial PIV Derivada,

para la cual la clave privada correspondiente se almacena en un módulo criptográfico con una alternativa factor de forma a la tarjeta PIV".

La tecnología de credenciales subyacente, derivada o no, está definida por la AAL requerida por la parte que confía, como se describe en Directrices *de identidad digital del NIST.* Las tres AAL definen los subconjuntos de opciones que las agencias pueden seleccionar en función de su perfil de riesgo y el daño potencial causado por un atacante que toma el control de un autenticador y accede a los sistemas de las agencias. Los AAL son los siguientes:

AAL1 proporciona cierta seguridad de que el reclamante controla un autenticador vinculado a la cuenta del suscriptor. AAL1 requiere autenticación de un solo factor o de múltiples factores utilizando una amplia gama de tecnologías de autenticación disponibles. La autenticación exitosa requiere que el reclamante demuestre la posesión y el control del autenticador a través de un protocolo de autenticación seguro.

AAL2 proporciona una alta confianza de que el reclamante controla los autenticadores vinculados a la cuenta del suscriptor. Se requiere prueba de posesión y control de dos factores de autenticación distintos a través de protocolos de autenticación seguros. Se requieren técnicas criptográficas aprobadas en AAL2 y superior.

AAL3 proporciona una confianza muy alta de que el reclamante controla los autenticadores vinculados a la cuenta del suscriptor. La autenticación en AAL3 se basa en la prueba de posesión de una clave a través de un protocolo criptográfico. La autenticación AAL3 utiliza un autenticador criptográfico basado en hardware y un autenticador que proporciona resistencia a la suplantación de identidad del verificador. El mismo dispositivo puede cumplir ambos requisitos. Para autenticarse en AAL3, los reclamantes prueban la posesión y el control de dos factores de autenticación distintos a través de protocolos de autenticación seguros. Se requieren técnicas criptográficas aprobadas.

Para cumplir con AAL2 o AAL3, una credencial derivada basada en un dispositivo móvil tendría que ser compatible con técnicas criptográficas aprobadas. Los dispositivos móviles compatibles con Fast Identity Online (FIDO) Universal Authentication Framework (UAF) (y los sistemas host correspondientes) son compatibles con AAL3, por ejemplo.

Las siguientes secciones analizan más de cerca las diferentes categorías de soluciones móviles y las evaluaciones de estas tecnologías se muestran en la Figura 13.

Ferraiolo, et al. (diciembre de 2014).*Directrices para las credenciales de verificación de identidad personal derivada (PIV)*.Instituto Nacional de Normas y Tecnología. Obtenido de:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

Grassi, P.A., García, M.E. y Fenton, J.L. (junio de 2017).*Pautas de identidad digital. Instituto Nacional de Normas y Tecnología.*Obtenido de:http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

4.4.1. Contraseña de un solo uso (OTP)

La contraseña de un solo uso (OTP), o tecnología de contraseña dinámica, se utiliza para autenticar a un usuario solo para una sesión. Cada vez que una persona se valida con éxito o cuando se

detiene el temporizador de cuenta regresiva, la contraseña caduca. OTP es conocido por ser fácil de usar. La autenticación mediante OTP requiere acceso a algo que una persona tiene (en este caso, acceso a un teléfono móvil o dirección de correo electrónico), así como algo que una persona conoce (como un PIN).[120]

La tecnología OTP es compatible con múltiples dispositivos, incluidas computadoras, teléfonos móviles y tokens inteligentes. Se puede implementar a través de tokens de software como el servicio de mensajes cortos (SMS) basado en dispositivos móviles o software basado en PC. La tecnología OTP también se puede implementar mediante el uso de dispositivos token portátiles o tarjetas inteligentes sincronizadas con una agencia de autenticación central. NIST ha calificado recientemente el uso de SMS para la verificación fuera de banda. Como explica el NIST, “El dispositivo fuera de banda DEBE ser direccionable de manera única y la comunicación a través del canal secundario DEBERÁ estar encriptada a menos que se envíe a través de la red telefónica pública conmutada (PSTN). Los métodos que no prueban la posesión de un dispositivo específico, como voz sobre IP (VOIP) o correo electrónico, NO DEBEN utilizarse para la autenticación fuera de banda”.[121]

La tecnología OTP se ha utilizado en múltiples aplicaciones, incluidos los servicios de emergencia (cuando es necesario ponerse en contacto con una gran base de datos de personas), servicios seguros (como transacciones financieras), la industria minorista y la prestación de servicios gubernamentales. La tecnología se puede utilizar como un mecanismo de autenticación independiente, así como en la autenticación de múltiples factores. En un inicio de sesión independiente o de un solo factor, el usuario ingresa solo una OTP para la validación. Para la autenticación multifactor, una OTP se combina con otros métodos de validación, como el uso de un PIN, datos biométricos o datos de red contextual conocidos por la red móvil. Esto es mucho más seguro que la autenticación de un solo factor.

¿Qué problemas puede resolver?

·**Escalabilidad.**Los requisitos computacionales y de red de la tecnología OTP son mínimos, lo que permite la escalabilidad a grandes poblaciones.
·**Adopción.**Es fácil aprender a usar OTP; la interfaz de usuario muestra una pantalla simple de un token de seis dígitos, o el usuario recibe un SMS que contiene la OTP, que debe ingresarse en el campo correspondiente para la validación. Todo esto fomenta la rápida adopción de la tecnología.
·**Madurez.**La tecnología OTP ha estado en uso durante más de una década y ha sido ampliamente aceptada. Un ejemplo reciente del uso de OTP en un sistema de identificación digital es la vinculación de las tarjetas SIM móviles de las personas en India con su número de Aadhaar mediante el uso de una OTP.[122]
¿Qué problemas no resuelve?
·**Seguridad.**La tecnología requiere compartir secretos, proporcionando múltiples puntos de ataque. Consulte la actualización del NIST relacionada con la desaprobación de compartir OTP a través de SMS.
¿Qué problemas podría crear?

Traducido: *Francisco Javier González García*

·**Seguridad.**Si un estafador accede a una OTP activa mediante la clonación de una tarjeta SIM, podría ocurrir un robo de identidad.

Thomas A. Bien.*Contraseñas de un solo uso: hoja de ruta.*Obtenido de:https://hea-www.harvard.edu/~fine/Tech/otp.html

Múltiples Autores.*Directrices de identidad digital Autenticación y gestión del ciclo de vida NIST.*Obtenido de:https://pages.nist .gov/800-63-3/sp800-63b.html

Timesofindia.com (4 de enero de 2018).*Vincule Aadhaar a las tarjetas SIM existentes mediante OTP.*Tiempos de India. Obtenido de:https://timesofindia.indiatimes.com/business/faqs/aadhar-faqs/otp-based-aadhaar-verification-for-existing-sim-cards/articleshow/62350208.cms

4.4.2. identificación inteligente

Smart ID es una aplicación de identificación electrónica disponible en tabletas y teléfonos inteligentes. Permite la autenticación de los usuarios que buscan acceder a los servicios en línea. La solución funciona en todos los dispositivos, pero los usuarios deben registrar cada dispositivo individualmente para que funcione la autenticación. Pueden registrarse en la aplicación utilizando sus tarjetas de identificación digitales y certificados válidos. Una vez que se hayan registrado, pueden usar Smart ID para autenticarse digitalmente en varios dispositivos.[123]

Como medida de seguridad, la primera vez que se ingresa incorrectamente el PIN tres veces, la cuenta del usuario se bloquea durante tres horas. Después de otros tres intentos fallidos, la cuenta se bloquea durante 24 horas. Un nuevo intento de usar el PIN incorrecto tres veces, bloquea la cuenta de forma permanente.[124]

La tecnología se está utilizando en varios países. Por ejemplo, en los países bálticos hay más de 300.000 usuarios. Todos los clientes de SEB Bank pueden usar Smart ID para la banca en línea. Para solicitar una identificación inteligente, los clientes visitan su sucursal local de SEB, donde los funcionarios del banco establecen su identidad y los guían a través del proceso de creación de su cuenta de identificación inteligente.

Swedbank es otro ejemplo de ello. El banco ha introducido servicios en línea autenticados a través de Smart ID para sus sucursales de Letonia y Lituania. Los clientes pueden descargar y registrarse en la aplicación Smart ID y realizar transacciones bancarias al autenticarse a través de sus PIN de Smart ID. Eesti Gaas, una empresa de gas natural de Estonia, ha ampliado los servicios de identificación inteligente a sus clientes para permitirles acceder a sus cuentas en línea. De hecho, Estonia fue el primer país en implementar soluciones de identificación inteligente para iniciativas que incluyen i-Voting, e-taxation y e-residency.con los primeros servicios electrónicos que utilizan Smart ID en línea en febrero de 2017. Se espera que estas Smart ID reemplacen las tarjetas de identificación basadas en chip que los estonios usan actualmente para realizar transacciones en línea. En marzo de 2017, los servicios electrónicos de Letonia y Lituania comenzaron a brindar acceso a los clientes con Smart ID.

Traducido: *Francisco Javier González García*

¿Qué problemas puede resolver?

·**Seguridad.**La identidad electrónica de los usuarios basada en Smart ID es independiente de las tarjetas SIM de su dispositivo móvil. Una vez que se registran con Smart ID, las personas solo necesitan una conexión a Internet activa para autenticarse en los servicios en línea asociados. Además, los datos están seguros porque la aplicación Smart ID usa solo los dos PIN para validar a los usuarios para los servicios; no almacena ninguna contraseña de usuario.

·**Adopción.**Los clientes pueden comprender fácilmente la identificación inteligente sin necesidad de una formación exhaustiva. Además, esta tecnología no depende de una tarjeta SIM y se puede utilizar en todo el mundo.

·**Asequibilidad.**A medida que aumenta el número de transacciones de Smart ID, los precios por transacción se desploman para los proveedores de servicios electrónicos. Además, la aplicación es gratuita para los usuarios finales.[129]

·**Actuación.**La solución cuenta con una excelente velocidad de procesamiento, limitada solo por la velocidad de Internet del usuario final y transacciones seguras. Smart ID también cumple con los requisitos eIDAS de la UE y los requisitos del Banco Central Europeo como una herramienta de autenticación sólida.

*Smart-ID: la forma inteligente de identificarse.*Smart-ID.com. Obtenido de:https://www.smart-id.com/about-smart-id/

*El uso de Smart-ID es seguro y seguro.*Smart-ID.com. Obtenido de:https://www.smart-id.com/security/

Lukin, L. (28 de junio de 2017).*Smart-ID es utilizado por 300.000 personas en los países bálticos.*Soluciones SK ID AS. Obtenido de:https://sk.ee/es/Noticias/smart-id-es-usado-por-300-000-personas-en-los-balticos

*Presentamos Smart-ID.*banco sueco. Obtenido de:https://www.swedbank.lv/private/campaign/smart-id

Eesti Gaas es la primera compañía de energía en usar Smart-ID.(25 de mayo de 2017). Eesti Gaas Obtenido de:http://www.gaas.ee/es/eesti-gaas-es-la-primera-empresa-de-energia-en-llevar-a-usar-smart-id/

e-Estonia en el Mobile World Congress 2016.(15 de febrero de 2016). Soluciones SK ID AS. Obtenido de:https://www.sk.ee/en/Noticias/e-estonia-en-el-mobile-world-congres-2016

*Lista de Precios del Servicio Smart-ID.*Soluciones SK ID AS. Obtenido de:https://sk.ee/en/services/pricelist/smart-id/

·**Escalabilidad.**La solución se puede escalar fácilmente a través de servicios en industrias que van desde la banca hasta la energía y más. Una vez que un cliente se registra, puede usar ese mismo registro para acceder a servicios en múltiples industrias.

¿Qué problemas no resuelve?

·**Madurez.**La solución fue desarrollada por un actor privado, tiene un alcance geográfico limitado y aún no se ha trasladado a los principales mercados. Actualmente se limita a Estonia, Letonia y Lituania.

·**Escalabilidad.**La solución necesita una conectividad confiable a una red estable para realizar el proceso de validación sin problemas.

¿Qué problemas podría crear?

·**Seguridad.**Aunque la solución bloquea la cuenta de un usuario cuando se ingresan PIN incorrectos, aún es vulnerable a las violaciones de seguridad. Cualquiera que obtenga los PIN de un usuario puede acceder a sus cuentas.

4.4.3. SIM criptográfica

Las tarjetas SIM utilizan algoritmos criptográficos que convierten la tarjeta en una herramienta de identificación del usuario. Por ejemplo, los algoritmos A3 (autenticación) y A8 (generación de clave de cifrado) se escriben en la tarjeta SIM durante el proceso de producción y se protegen contra la lectura en circunstancias normales. El operador posee el código PUK (clave de desbloqueo personal), y el usuario puede acceder a él enviando una solicitud al operador. La clave de cifrado se deriva de la clave de autenticación del suscriptor mediante el cifrado.
Dichos algoritmos permiten una comunicación segura entre el usuario y la red sin exponer información sobre los suscriptores o la red que alguien podría usar para obtener acceso ilegal a los servicios que usan los suscriptores.
Durante la autenticación, el Centro de Autenticación genera un número aleatorio que se envía al número de móvil. Luego, este número aleatorio se usa junto con la clave de cifrado del usuario y el algoritmo A3 para generar un número que luego se envía de vuelta al Centro de Autenticación. Si el número enviado por el móvil del usuario coincide con el número generado por el Centro de Autenticación, el usuario está verificado.[132]
Los países que han adoptado tarjetas SIM criptográficas incluyen Estonia, Moldavia y Finlandia.[133,134]Los operadores móviles noruegos ofrecen a sus suscriptores una autenticación móvil segura a través de una solución BankID local para brindar identificación de usuario en línea segura y verificación de firma digital de usuario.
¿Qué problemas puede resolver?
·**Seguridad.**Las tarjetas SIM criptográficas brindan una identificación segura y confiable para que los suscriptores accedan a los servicios en línea.

Seguridad de la tarjeta SIM. Ruhr-Universidad de Bochum. Obtenido de:https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/slides_sim_card_security.pdf

Jansen, W. A. y Delaitre, A. (2007). *Material de referencia para la evaluación de herramientas SIM forenses.*41.ª Conferencia anual IEEE International Carnahan sobre tecnología de seguridad, Ottawa, Ontario, págs. 227–234. Obtenido de:https://csrc.nist.gov/csrc/media/projects/mobile-security-and-forensics/documents/mobile_forensics/reference%20mat-final-a.pdf

*Tarjetas SIM.*Gemalto. Obtenido de:https://www.gemalto.com/companyinfo/digital-security/techno/sim

Banco Mundial (2016).*Identidad digital: hacia principios compartidos para la cooperación entre los sectores público y privado (inglés).*
Grupo del Banco Mundial. Obtenido de:http://documents.worldbank.org/curated/en/600821469220400272/Identidad-digital-hacia-principios-compartidos-para-la-cooperación-de-los-sectores-público-y-privado

*Cuando eID se convierte en móvil para toda una nación.*Gemalto. Obtenido de:https://www.gemalto.com/brochures-site/download-sitio/Documentos/gov_cs_finland_valimo.pdf

·**Asequibilidad.**Los operadores de redes móviles cobran a los usuarios finales una tarifa por uso cuando usan una firma digital para autenticarse para e-Gov y otros servicios en línea. Pero el costo no es muy alto, ya que también se comparte con los proveedores de servicios.
·**Actuación.**La solución permite a los usuarios acceder rápidamente a los servicios en línea sin tener que configurar ni recordar complicados nombres de usuario y contraseñas. Los usuarios pueden iniciar sesión con un PIN y, dado que la solución depende únicamente de la conectividad de la red para la autenticación, es muy confiable.
·**Escalabilidad.**La solución puede autenticar a los usuarios a través de múltiples servicios en línea, y solo necesita la autenticación por parte del operador móvil.
¿Qué problemas no resuelve?
·**Adopción.**Aunque cada vez más personas tienen acceso a la conectividad móvil, la tecnología SIM criptográfica aún no se ha implementado ampliamente en todos los países. A medida que más servicios se mueven en línea y aumenta la necesidad de verificación de usuarios en línea, esto podría cambiar.
¿Qué problemas podría crear?

·**Seguridad.**Los piratas informáticos pueden engañar a un usuario móvil para que instale un software malicioso que les dé el control total del teléfono del usuario, permitiéndoles espiar y cometer otros actos maliciosos.

4.4.4. Registro usando dispositivos móviles

Las tecnologías de registro móvil comprenden soluciones de hardware y software que permiten la inscripción de personas en un sistema de identificación. Por ejemplo, las autoridades gubernamentales o las personas utilizan las funciones existentes de los teléfonos inteligentes o los dispositivos móviles especializados para capturar datos biométricos y fotografías. La capacidad de recopilar datos biográficos (como documentos de criadores) e información biométrica (incluidas huellas dactilares, imágenes del iris y fotografías) para el registro de identificación digital a través de la tecnología móvil ha mejorado recientemente. Por ejemplo, los teléfonos inteligentes pueden equiparse con dispositivos de captura directamente o a través de Universal Serial Bus (USB), Bluetooth (y Bluetooth Low Energy—BLE) y NFC. Estos dispositivos especialmente diseñados pueden ofrecer mejores capacidades de captura en términos de facilidad de uso, rendimiento y calidad de imagen, en comparación con los sensores integrados en un teléfono inteligente. Por lo tanto, no es raro que los funcionarios públicos utilicen un dispositivo móvil para capturar datos de los ciudadanos para facilitar la inscripción en un sistema de identificación centralizado.

Los operadores móviles han estado involucrados en los sistemas de registro de nacimientos en varios países, desempeñando un papel vital en el registro de la población en un sistema de identidad gubernamental. En Tanzania, por ejemplo, la Agencia de Registro e Insolvencia del gobierno (RITA), en asociación con UNICEF y el operador móvil Tigo, ha desarrollado una aplicación basada en Android que permite a los registradores en clínicas de salud locales y oficinas gubernamentales recopilar datos de registro de nacimiento y subirlos a un sistema centralizado. Hasta la fecha, más de 1,6 millones de niños han sido registrados y emitidos un certificado de nacimiento bajo esta iniciativa. El nivel general de registro y certificación ha aumentado del 10 % al 79 % en las siete regiones donde se implementó esta iniciativa.[137]

Traducido: *Francisco Javier González García*

En Pakistán, UNICEF y el operador móvil Telenor desarrollaron una aplicación móvil que digitaliza el formulario de registro de nacimiento y proporciona tarjetas SIM con conectividad de datos y acceso wifi. Los funcionarios públicos recibieron dispositivos móviles o tabletas para realizar el proceso de registro. Este programa resultó en un 300%

Tigo.*Registro Móvil de Nacimiento.*Tigo Tanzania. Obtenido de:https://www.tigo.co.tz/mobile-birth-registration

UNICEF Tanzania (24 de noviembre de 2015).*TIGO se asocia con UNICEF, promueve innovaciones para los niños de Tanzania.*UNICEF.

Obtenido de:https://www.unicef.org/tanzania/media_17334.html

SME Aportación de Marta Ienco—Directora de Asuntos Gubernamentales y Regulatorios, Programa de Identidad de GSMA en GSMA.

y un aumento del 126 % en las tasas de registro de recién nacidos, respectivamente, en las provincias paquistaníes de Punjab y Sindh. El proyecto ha resultado en un estimado de 705.000 registros después de haber sido escalado a 108 ubicaciones.

Con los escáneres de huellas dactilares e iris casi comunes en los teléfonos inteligentes, más usuarios (particularmente en los mercados desarrollados donde la adopción de teléfonos inteligentes es alta) registran ellos mismos sus datos biométricos en estos dispositivos. El sector privado está creando aplicaciones que luego usan los datos biométricos para autenticar al individuo para una transacción, como la compra de un producto o el acceso a un servicio. Algunas empresas están trabajando en el desarrollo de soluciones solo de software que permitan que cualquier dispositivo móvil con una cámara común combinada con inteligencia artificial y algoritmos de aprendizaje profundo capture la biometría de un usuario, como la morfología de la palma de la mano, los pies y la oreja, para realizar el registro móvil.[139]

¿Qué problemas puede resolver?

- **Asequibilidad.** Los teléfonos inteligentes con sensores biométricos incorporados son cada vez más baratos, y los precios mundiales de los teléfonos inteligentes disminuyeron un 27 % entre 2010 y 2017.[140]Los accesorios de hardware especializados para agregar la capacidad de captura biométrica a los teléfonos comunes también son asequibles y se pueden configurar rápidamente.
- **Adopción.** Más de mil millones (BN) de teléfonos inteligentes biométricos están en uso hoy en día, y las personas pueden usar rápidamente esta tecnología con una capacitación e inversión mínimas. Los escáneres de huellas dactilares externos cuestan alrededor del 20% de los teléfonos inteligentes estándar de gama media y se pueden combinar con varios teléfonos inteligentes mediante la instalación de aplicaciones móviles gratuitas. El proceso de configuración único también es fácil.
- **Escalabilidad.** Los escáneres de huellas dactilares y de iris se están volviendo comunes en los teléfonos móviles, lo que hace que el registro móvil sea escalable. Sin embargo, el sensor biométrico integrado en los móviles no se puede utilizar para registrar y autenticar usuarios para programas de identificación a gran escala porque la biometría no se puede almacenar ni transferir a una nube o base de datos. En cambio, los datos biométricos se guardan en un

enclave seguro en el teléfono que está separado del resto del sistema operativo del teléfono. El registro y la autenticación a gran escala requieren escáneres biométricos independientes.
·**Actuación.** Debido a que los dispositivos inteligentes recopilan los datos, el proceso de registro es rápido y preciso. Y debido a que la solución depende solo de la conectividad de la red para la autenticación, generalmente es confiable. Además, ciertas soluciones móviles pueden realizar la autenticación fuera de línea sin necesidad de conectarse a una red móvil. Estas inscripciones se pueden supervisar si es necesario (por ejemplo, a través de la red de agentes de un banco).
¿Qué problemas no resuelve?
·**Seguridad.** Si el registro de datos móviles no está supervisado, es difícil establecer la confianza en los datos.
·**Madurez.** Las soluciones de registro móvil que ofrecen diferentes proveedores utilizan diferentes tipos de intercambio de datos.
estándares, desalentando la interoperabilidad.
¿Qué problemas podría crear?
·**Actuación.** Con los rápidos avances tecnológicos, los dispositivos móviles existentes podrían volverse incompatibles u obsoletos. Por ejemplo, los nuevos teléfonos inteligentes se están moviendo hacia los estándares USB-C, lo que hace que muchos de los dispositivos biométricos actuales queden obsoletos.
GSMA.*Innovaciones en el registro móvil de nacimientos: perspectivas de Tigo Tanzania y Telenor Pakistan.*GSMA. Obtenido de:https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/01/Innovations-in-Mobile-Birth-Registration_ Insights-from-Tigo-Tanzania-and-Telenor-Pakistan.pdf
SME Aporte de Rebecca Distler—Directora, Global Health Initiatives—Element Inc.
*Statista Precio de venta promedio global de teléfonos inteligentes de 2010 a 2019 (en dólares estadounidenses).*Obtenido de:https://www.estatista.com/statistics/484583/global-promedio-venta-precio-smartphones/

·**Adopción.** En más de 145 países, la adquisición de SIM requiere que los usuarios presenten una credencial de identidad reconocida. Por lo tanto, el uso de soluciones de identificación y autenticación basadas en dispositivos móviles resultará muy difícil para las personas que no tienen ninguna otra forma de identificación reconocida oficialmente.

·**Seguridad.** Las aplicaciones maliciosas pueden recuperar datos biométricos de un dispositivo móvil o capturar pasivamente datos biométricos e información personal, lo que genera preocupaciones sobre la seguridad.

4.4.5. Conexión móvil

GSMA Mobile Connect es una cartera de servicios de identidad segura basados en dispositivos móviles impulsados por operadores de redes móviles a nivel mundial. Es una solución de identidad multipropósito que utiliza la confianza, la seguridad y la ubicuidad inherentes de las redes móviles. Los operadores de redes móviles brindan a los usuarios control sobre sus propios datos y permiten que los usuarios finales, las empresas y los gobiernos interactúen y accedan a los servicios en línea en un entorno conveniente, privado y confiable.

Traducido: *Francisco Javier González García*

Al utilizar el número de teléfono móvil de una persona como identificador y el teléfono móvil como dispositivo de autenticación, Mobile Connect admite una amplia gama de aplicaciones prácticas, incluido el registro y el inicio de sesión en sitios web y aplicaciones y la autorización de transacciones en línea. Mobile Connect se entrega como un marco de identidad federado a través de los operadores móviles participantes. Los desarrolladores pueden acceder al ecosistema de operadores que se han asociado con GSMA para Mobile Connect y su base de usuarios, incluyendo un portal para desarrolladores y un conjunto de pruebas independientes. En 2015, Mobile Connect de GSMA se convirtió en la primera solución de autenticación de servicio público transfronterizo del sector privado compatible con eIDAS y, desde entonces, la cantidad de operadores móviles que prueban Mobile Connect contra eIDAS sigue aumentando.

Autenticar/Plus, uno de los servicios populares de Mobile Connect, permite que el número de teléfono móvil de un usuario actúe como un identificador digital único que aprovecha la relación de confianza con el operador móvil. Esto permite a los usuarios iniciar sesión fácilmente sin necesidad de nombres de usuario y contraseñas en ningún servicio en línea participante, simplemente utilizando el número de teléfono móvil como medio de autenticación. La autenticación es administrada por el operador de red móvil existente y no se comparten datos personales con el sitio web sin el consentimiento del usuario.[146]

Una vez registrados, los usuarios pueden iniciar sesión en los servicios en línea siempre que aparezca el logotipo de Mobile Connect, simplemente haciendo clic en el logotipo o ingresando un PIN seguro (para servicios que requieren mayor seguridad). Al usar esta tecnología para aplicaciones que requieren un alto nivel de seguridad (LOA), es importante realizar pruebas de identidad y un sólido proceso de conocimiento de su cliente (KYC) durante el registro del número de teléfono móvil con el proveedor de servicios.

La penetración móvil ha ido en aumento a lo largo de los años, y la solución Mobile Connect proporciona un método rápido, confiable, seguro y eficiente para proporcionar a los usuarios identidades digitales. Hasta 62 operadores de redes móviles en 30 países han lanzado Mobile Connect. La mayoría de los operadores han lanzado Mobile Connect Authenticate, que permite un servicio de inicio de sesión seguro y sin contraseña a escala mundial. Algunos otros también admiten más de un servicio de Mobile Connect (como el número de teléfono de Mobile Connect o la coincidencia KYC de Mobile Connect).

GSMA (abril de 2006).*Registro obligatorio de tarjetas SIM prepago.*GSMA. Obtenido de:https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

*Presentamos Mobile Connect, el nuevo estándar en autenticación digital.*GSMA. Obtenido de:https://www.gsma.com/identity/mobile-connect

Portal para desarrolladores de conexión móvil. Desarrolladores. Obtenido de:https://developer.mobileconnect.io/faq

Marta Ienco (06 de julio de 2017).*Mobile Connect-eIDAS Pilot se prepara para el comercio transfronterizo seguro.*GSMA. Obtenido de: https://www.gsma.com/identity/eidas-pilot-prepares-secure-cross-border-trade

*Presentamos Mobile Connect, el nuevo estándar en autenticación digital.*GSMA. Obtenido de:https://www.gsma.com/identidad/conexión móvil

Traducido: *Francisco Javier González García*

La autenticación de usuario de Mobile Connect está disponible con operadores de telecomunicaciones de todo el mundo, incluidos Airtel, Idea y Vodafone en India; Orange Telecom en Marruecos y Egipto; y Turkcell en Turquía. Mobile Connect utiliza el principio de un "autenticador conectable", donde el mecanismo de autenticación móvil (autenticador) se puede conectar según la elección del operador móvil. Algunos de los autenticadores populares que se utilizan en Mobile Connect en todo el mundo son las aplicaciones móviles de autenticador, el subprograma SIM, SMS+URL, USSD, el autenticador integrado basado en red y el módulo de plataforma confiable (TPM). Algunas de estas tecnologías se analizan en detalle en las siguientes secciones.

¿Qué problemas puede resolver?

·**Seguridad.** Una vez que los usuarios se registran en Mobile Connect, no necesitan ningún nombre de usuario o contraseña para iniciar sesión en los sitios web. Un simple deslizamiento en una notificación o un PIN es todo lo que se necesita para iniciar sesión. Mobile Connect autentica al usuario a través del operador móvil y el sitio web recibe solo la confirmación de la identidad del usuario. Debido a que no se comparten datos de usuario con el sitio web sin el consentimiento del usuario, los datos del usuario están seguros. Mobile Connect también es seguro por diseño en el sentido de que una red móvil puede desactivar la tarjeta SIM de un dispositivo de forma inalámbrica y marcar el dispositivo como perdido o robado en una base de datos global si un usuario informa cualquiera de las dos situaciones.[149]

·**Adopción.** La adopción es fácil porque muchos operadores de redes móviles, particularmente en países en desarrollo, ya se han suscrito a los servicios. La solución también es fácil de entender y usar para las personas.

·**Asequibilidad.** La solución es muy asequible y requiere una inversión monetaria inicial de los servicios en línea dispuestos a proporcionar Mobile Connect como una opción de inicio de sesión.

·**Escalabilidad.** Una vez que los operadores ponen a disposición el servicio, los desarrolladores pueden crear aplicaciones para los servicios en línea para permitir la opción de inicio de sesión del usuario mediante Mobile Connect. Una vez que esta opción está disponible, la solución puede estar disponible para toda la base de usuarios sin más problemas de escalabilidad.

¿Qué problemas no resuelve?

·**Actuación.** Mobile Connect depende de los operadores móviles para validar la autenticidad de los usuarios. Esto podría limitar el rendimiento de la solución en lugares donde los operadores no tienen la cobertura adecuada.

·**Escalabilidad.** La escalabilidad de la red es baja, ya que la solución depende de la conectividad con un operador de red estable para la autenticación del usuario. Si la ubicación de un usuario no tiene una conexión de red estable, como puede ser común en los países en desarrollo, la solución no estará disponible.

¿Qué problemas podría crear?

·**Adopción.** La solución depende mucho del operador y primero necesita registrarse con un dispositivo móvil. Además, solo algunos operadores móviles se han registrado en Mobile Connect. Por lo tanto, particularmente en los países en desarrollo donde la conectividad móvil no es sustancial,

el registro de numerosos usuarios puede ser un desafío. Además, cada vez que un usuario cambia a un operador de red móvil diferente, debe repetir el proceso de registro.

SME Aporte de Gautam Hazari—Director técnico—Datos personales en GSMA.

GSMA (septiembre de 2016).*Mobile Connect: Autenticación móvil de alta seguridad.*Obtenido de:https://www.gsma.com/

*La identidad digital segura ahora está en tus manos.*Conexión móvil. Obtenido de:https://mobileconnect.io/identity/wp-content/uploads/2016/10/MC_high-security-authentication_Sep-16.pdf

4.4.6. Aplicación móvil de autenticación

Si bien una tecnología OTP simple alivia las preocupaciones de seguridad con una contraseña estática, no elimina por completo el riesgo de elusión. Hoy en día, la industria ha aceptado ampliamente dos enfoques para hacer que la tecnología OTP sea más segura, y ambos utilizan algoritmos pseudoaleatorios:

OTP basada en HMAC. El código de autenticación de mensajes hash (HMAC) OTP (o HOTP) se basa en una clave secreta y un contador. Este enfoque se usa comúnmente con la autenticación basada en token. Cada vez que el usuario intenta autenticar o incrementar el contador en el token presionando un botón en un token de hardware o actualizando (en el caso de un token de software), el generador crea una nueva OTP. Estas OTP no tienen un vencimiento limitado en el tiempo.

OTP basado en el tiempo. La contraseña de un solo uso basada en el tiempo (TOTP) es un código de acceso temporal, generado según la hora del día. A diferencia de HOTP, no hay contador. El tiempo debe estar sincronizado en el extremo del usuario y el extremo del recurso. Las marcas de tiempo generalmente se sincronizan mediante un protocolo de tiempo de red (NTP). Las marcas de tiempo se pueden incrementar cada 30 segundos o 1 minuto, por lo que cuando un usuario desea iniciar sesión, debe ingresar su nombre de usuario, contraseña y el último código TOTP.

Las aplicaciones de autenticación móvil como Authy y Google Authenticator son TOTP que permiten la autenticación de dos factores. Este enfoque está viendo gradualmente una mayor adopción y es mucho más seguro en comparación con OTP tradicional basado en SMS o incluso HOTP. Google Authenticator ha agregado soporte para múltiples aplicaciones como LastPass, WordPress, Facebook, Evernote, Microsoft, IFTTT, Dropbox, Amazon y Slack.

¿Qué problemas puede resolver?

- **Escalabilidad.**La escalabilidad de datos en tokens de hardware aún no se ha implementado y no se han identificado casos de uso de gestión de identidad. Sin embargo, los requisitos computacionales y de red son mínimos.
- **Adopción.**La adopción de la tecnología es fácil, gracias a la aceptación cultural y la simplicidad del aprendizaje y la formación. La interfaz de usuario es generalmente simple y utiliza una visualización destacada de un token de seis dígitos para la validación. Además,

con TOTP, la contraseña caduca con frecuencia, lo que brinda a los usuarios finales práctica en el uso de la tecnología, lo que fomenta aún más la adopción.
·**Madurez.** Como una extensión de la tecnología OTP madura, la tecnología HOTP y TOTP debería tener una amplia adopción porque la experiencia de los usuarios finales seguiría siendo casi la misma que la tecnología OTP tradicional basada en SMS.
·**Seguridad.** La tecnología TOTP hace que la tecnología OTP sea menos vulnerable a la elusión. Como la contraseña dinámica se actualiza con frecuencia, a cualquier estafador que tenga un token le resultará difícil ser validado como el propietario correcto del token.

¿Qué problemas no resuelve?

·**Asequibilidad.** La implementación de OTP implicaría costos administrativos, de hardware y de software adicionales que podrían traducirse en gastos operativos y iniciales sustanciales.
¿Qué problemas podría crear?

·**Seguridad.**TOTP viene con medidas de seguridad mejoradas. La contraseña generada se actualiza con frecuencia, lo que presenta desafíos para los posibles piratas informáticos. Sin embargo, en caso de robo de un token, se anula el beneficio adicional antes mencionado. Una combinación de dos factores de validación biométrica con OTP resuelve este problema.

4.4.7. Módulo de plataforma segura (TPM)

Un TPM es una herramienta criptográfica basada en hardware, generalmente un chip en la placa base de un dispositivo informático. La tecnología permite un fuerte cifrado de disco para proporcionar una autenticación de usuario segura sin necesidad de contraseñas complejas. Cualquier computadora o dispositivo, como un teléfono inteligente o una tableta, equipado con un TPM se puede usar para almacenar una credencial. La solución se basa en el cifrado de clave pública en el dispositivo del usuario para mitigar los riesgos de seguridad.[150]

TPM proporciona a los usuarios una identidad digital única representada por un par de claves seguras Rivest-Shamir-Adleman (RSA) denominada clave de aprobación. Una clave de identidad de atestación utiliza un algoritmo hash para brindar seguridad contra firmware y software ilegales. La clave de respaldo puede ser validada por la autoridad de certificación de privacidad para determinar la identidad digital de un individuo.

TPM se puede combinar con otras funciones de seguridad, como firewalls y contraseñas, para mejorar la seguridad del dispositivo. A medida que se inicia un dispositivo, TPM puede determinar si ha sido manipulado (desde el último estado estable) y luego puede bloquear el acceso a aplicaciones confidenciales.

Muchos fabricantes de portátiles, como IBM y Lenovo, ya tienen TPM preconfigurado en su hardware, pero el módulo permanece inactivo hasta que se activa a través del firmware en el

procesador del portátil. Esta característica se puede activar para que muchos usuarios brinden administración de identidad y acceso, protegiendo la información confidencial de posibles ataques.

Los TPM también están presentes en los dispositivos móviles. En los dispositivos Apple, por ejemplo, un Secure Enclave protege el código de acceso y los datos de huellas dactilares de un usuario. El sensor biométrico de Apple, llamado Touch ID, no almacena ninguna imagen de la huella dactilar del propietario del dispositivo. En cambio, guarda solo una representación matemática o una plantilla. Esto hace que sea imposible que alguien realice ingeniería inversa de la imagen real de la huella dactilar de esta plantilla almacenada. El enclave seguro está aislado del resto de los chips y del sistema operativo del dispositivo.

TPM se utiliza como uno de los mecanismos de autenticación en Mobile Connect.[151]

¿Qué problemas puede resolver?

·**Adopción.**Cualquier máquina habilitada para TPM se puede utilizar para almacenar la identidad del usuario virtual en lo que se denomina tarjetas inteligentes virtuales sin costo adicional, y la distribución de estas tarjetas es fácil a través de Internet.
·**Asequibilidad.**Los costos de mantenimiento de las tarjetas inteligentes virtuales son más bajos que los de las tarjetas inteligentes físicas, que se pierden, se roban o se rompen con facilidad debido al desgaste normal. Las tarjetas inteligentes virtuales TPM se pierden solo si el dispositivo de un usuario se pierde o se rompe.
·**Escalabilidad.**Debido a que muchos dispositivos ahora vienen preconfigurados con TPM, la solución se puede escalar fácilmente.
·**Seguridad.**Toda la información confidencial de la tarjeta inteligente virtual se cifra mediante el uso del TPM en la computadora host y, por lo tanto, no se puede usar en ninguna otra computadora. Además, los TPM ofrecen las mismas propiedades de criptografía aislada que ofrecen las tarjetas inteligentes físicas. Finalmente, si un usuario ingresa un PIN de forma incorrecta, la tarjeta inteligente virtual responde utilizando la lógica anti-martillo del TPM, que rechaza intentos posteriores por un tiempo en lugar de bloquear la tarjeta (también conocido como bloqueo).

150*Cómo usar el TPM: una guía para la seguridad de puntos finales basada en hardware.*(01 de marzo de 2009). Grupo de Computación de Confianza. Obtenido de:https://trustedcomputinggroup.org/use-tpm-guide-hardware-based-endpoint-security/

151 SME Aporte de Gautam Hazari—Director técnico—Datos personales en GSMA.

¿Qué problemas no resuelve?

·**Adopción.**Debido a que no existe una representación física de este documento de identidad, los usuarios y los gobiernos no pueden realizar transacciones que tradicionalmente requieren la presentación de un documento de identidad físico, como en los puntos de control de inmigración.
·**Escalabilidad.**En el África subsahariana y el sudeste asiático, la cantidad de computadoras habilitadas para TPM podría no ser suficiente para escalar esta tecnología, y agregar un

módulo TPM a una computadora existente es difícil, lo que limita aún más la escalabilidad.
¿Qué problemas podría crear?
·**Seguridad.**Las tarjetas inteligentes virtuales TPM residen en las computadoras de las personas, que con frecuencia pueden dejarse desatendidas. Tal situación abre la puerta para que personas malintencionadas usen un ataque de fuerza bruta o martilleo (probando múltiples PIN) para eludir el sistema. El comportamiento anti martillazos de una tarjeta inteligente virtual difiere en que solo presenta un retraso de tiempo en respuesta a fallas repetidas del PIN, en lugar de bloquear completamente al usuario.
·**Adopción.**La tecnología no se puede utilizar en situaciones en las que una persona deba presentar una prueba de identidad física, como en un cruce fronterizo o en un hospital. Esto limita ligeramente las aplicaciones de la tecnología.

4.4.8. Tendencias clave en soluciones móviles

Los teléfonos inteligentes biométricos han proliferado, con más de 500 modelos introducidos desde principios de 2013 y 1 BN de estos dispositivos en uso en la actualidad. Las proyecciones muestran que para 2020, habrá 4,8 BN de dispositivos móviles inteligentes habilitados biométricamente. A medida que la tecnología se vuelve más portátil y menos costosa, el registro portátil de poblaciones remotas en países en desarrollo puede aumentar. Registro de votantes en varios países africanos y registro de población en Tanzania son ejemplos de cómo las tecnologías móviles pueden ayudar a los gobiernos a acercar el registro móvil a las personas, en lugar de hacerlo al revés.
La identificación móvil también está emergiendo cada vez más como una opción preferida para implementar sistemas de identificación digital. Considere estos ejemplos:
El Mobile ID de Estonia, lanzado en 2007, permite a las personas acceder a información y datos personales en sus dispositivos móviles y autenticar transacciones en línea utilizando tecnología de infraestructura de clave pública (PKI) segura. La identificación móvil basada en SIM se puede usar exactamente como una credencial física regular con más de 300 organizaciones en los sectores público y privado de Estonia. La función de firma electrónica de los dispositivos móviles permite todo esto y tiene la equivalencia legal de una firma "húmeda".
Mobile ID también está disponible en Austria, Azerbaiyán, Bélgica, Finlandia, Alemania, Islandia, Japón, Lituania, Moldavia, Noruega y Suecia.

*Inteligencia de mercado de Acuity (2017).*PR Newswire. Obtenido de:https://www.prnewswire.com/news-releases/biometrics-on-smart-mobile-devices-to-redefine-digital-identity-with-129-billion-biometric-app-downloads- between-2014- and- 2020-300115442.html

*Inteligencia de mercado de Acuity (2017).*PR Newswire. Obtenido de:https://www.prnewswire.com/news-releases/biometrics-on-smart-mobile-devices-to-redefine-digital-identity-with-129-billion-biometric-app-downloads- between-2014- and- 2020-300115442.html

Biometría para elecciones para apoyar el principio "Una persona, un voto".(04 de noviembre de 2017). Gemalto. Obtenido de:http://www.gemalto.com/govt/coesys/enrolment/biometric-voter-registration

Matthew Wilson (14 de septiembre de 2017).*Mapeo del acceso al registro de nacimientos y actualizaciones de Tanzania.*GSMA. Obtenido de:https://www.gsma.com/mobilefordevelopment/programme/digital-identity/mapping-access-birth-registration-updates-tanzania

Traducido: *Francisco Javier González García*

En 2014, Omán se convirtió en el primer país de Medio Oriente en complementar su tarjeta de identificación electrónica con un esquema de identificación móvil. Qatar y los Emiratos Árabes Unidos siguieron su ejemplo más tarde.

El registro móvil, donde una autoridad de registro utiliza tecnología móvil en el proceso de inscripción, se está volviendo más fácil, más preciso y más rentable a medida que los dispositivos móviles especializados se integran con los teléfonos inteligentes existentes. Por ejemplo, la aplicación móvil de reconocimiento facial BioID permite a las personas preinscribirse en BioID con solo unos pocos clics e imágenes faciales capturadas. El M6 de Tascent es un accesorio móvil que se integra con el iPhone y agrega captura de iris dual junto con la capacidad de captura de huella digital dual; junto con la aplicación móvil, también brinda capacidades para inscribir, eliminar duplicados y autenticar sujetos. Otras tecnologías emergentes están utilizando soluciones de solo software para el registro móvil. Por ejemplo, Element Inc. utiliza las cámaras existentes en los dispositivos móviles para la captura de datos biométricos, con la tecnología de algoritmos de aprendizaje profundo. El software de Element puede inscribir múltiples modalidades (cara, palma) sin necesidad de conectividad o hardware especializado. También se puede acceder al software a través de kits de desarrollo de software (SDK) o aplicaciones independientes, lo que permite que los teléfonos inteligentes y las tabletas comunes se activen biométricamente.

Otros avances (como la identificación móvil basada en SIM, la identificación móvil derivada y la identificación móvil basada en NFC) permitirán a los usuarios identificarse sin problemas para obtener acceso a los servicios gubernamentales. Las aplicaciones móviles también están adoptando técnicas de autenticación dinámicas basadas en la geolocalización y el historial de transacciones de los usuarios. Las aplicaciones innovadoras están permitiendo la captura de datos biométricos multimodales, y algunos gobiernos están combinando dicha captura con algoritmos de aprendizaje profundo para crear registros de salud maternoinfantil.

Mientras tanto, el applet Mobile ID SIM ahora permite a las personas confirmar su identidad y firmar documentos directamente desde su teléfono móvil, ingresando un PIN único seleccionable por el usuario. Se espera que surjan soluciones unificadas, personalizadas, multicanal y multiplataforma, utilizando tecnologías existentes como IA, reconocimiento de voz y geolocalización. Estas tecnologías serán fáciles de usar, haciendo que tareas como la autenticación sean fluidas y eficientes.

Los gobiernos también están explorando cada vez más una variedad de asociaciones público-privadas (PPP) y modelos de reparto de ingresos para generar fondos para las inversiones adicionales en hardware y fortaleza de la red que requieren los sistemas de autenticación móvil. En algunos de estos modelos, los operadores móviles cobran a los usuarios finales una tarifa por el uso de firmas móviles y transfieren parte de los ingresos al gobierno, como se hizo en Moldavia.

*Tascent M6.*Tascent, Inc. Obtenido de:https://tascent.com/productos-servicios/tascent-m6/

Banco Mundial (2016).*Identidad digital: hacia principios compartidos para la cooperación entre los sectores público y privado (inglés).*

Traducido: *Francisco Javier González García*

Grupo del Banco Mundial. Obtenido de:http://documents.worldbank.org/curated/en/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation

ENFOQUE: SISTEMAS TRANSFRONTERIZOS

Los avances tecnológicos están permitiendo que los sistemas de identificación digital operen a través de las fronteras. Las personas que tengan una identificación válida de un país pueden usar su credencial para realizar una transacción en otro país (cómo declarar sus impuestos) o para identificarse y autenticarse en los puntos de control o cruces fronterizos en otros países. La sección analiza un ejemplo de sistemas de identificación transfronterizos que ilustran los casos de uso mencionados anteriormente.

En la Unión Europea, eIDAS (servicios electrónicos de identificación, autenticación y confianza) es una regulación sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el Mercado Único Europeo. Bajo eIDAS, las personas pueden realizar transacciones electrónicas transfronterizas seguras que requieren que autentiquen su identidad, como inscribirse en una universidad, abrir una cuenta bancaria y autorizar el acceso a sus registros médicos electrónicos.

Hay tres principales partes interesadas en la red eIDAS: personas que buscan acceder a un servicio o establecer su identidad en otro país, el servidor que proporciona acceso a una aplicación o servicio seguro y el proveedor de los servicios que busca una persona.

Una vez que los datos que se van a autenticar se recopilan en el punto de inmigración, según la arquitectura de TI en uso, los datos se validan a través de una base de datos central que se mantiene en el sitio o se valida de forma remota si la base de datos está ubicada en una geografía separada. Se logra un canal de intercambio de información seguro utilizando SAML (Security Assertion Markup Language) para el inicio de sesión único, el manejo de errores y la comunicación. La seguridad de los terminales se garantiza mediante TLS (Seguridad de la capa de transporte, un protocolo criptográfico que proporciona seguridad en las comunicaciones a través de una red informática).

La regulación eIDAS también incluye reglas para proveedores de servicios de confianza (empresas que manejan firmas electrónicas, sellos de tiempo, sellos electrónicos y otros métodos para verificar documentos) y rige el uso de servicios de confianza por parte de consumidores, empresas y agencias para administrar transacciones electrónicas o acceder a los servicios en línea.[159]

Comisión Europea (6 de noviembre de 2015).*eIDAS—Arquitectura de interoperabilidad.*Comisión Europea. Obtenido de:https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

Koo, J.H. (29 de noviembre de 2017).*Firme electrónicamente aquí: La Agencia de Ciberseguridad de la UE considera que los servicios de verificación de documentos en línea son seguros.*La Oficina de Asuntos Nacionales, Inc. Obtenido de:https://www.bna.com/favor-esign-eu-b73014472575/

Traducido: *Francisco Javier González García*

---

5. Marcos de Autenticación y Confianza: Tecnologías y Protocolos

La autenticación federada proporciona una solución basada en estándares para el problema de confiar en las identidades en diversas organizaciones que incluso pueden estar en diferentes países. Esto requiere el establecimiento de un marco de confianza entre el proveedor de identidad y la parte que confía (proveedores de servicios). Un marco de confianza es un conjunto de reglas comerciales, legales y técnicas que los miembros de una comunidad acuerdan seguir para lograr la confianza en línea.

Las personas suelen necesitar acceso a servicios alojados por diferentes proveedores tanto dentro como fuera de sus fronteras nacionales. Un marco de autenticación federado compuesto por gobernanza, estándares y tecnologías de soporte permitirá a los proveedores de identidad y a las partes que confían un medio para proporcionar credenciales confiables y autenticar a las personas con niveles de seguridad conocidos en una amplia gama de proveedores de servicios. La principal ventaja del enfoque de administración de identidades federadas es que la administración de identidades y credenciales sigue siendo responsabilidad del proveedor de identidades original, y las partes que confían pueden definir y redefinir las autorizaciones: qué acceso se otorga a la persona para votar, registros de salud, transacciones financieras, etc., como lo deseen. Esto aumenta la inclusión, la interoperabilidad, la escalabilidad y la seguridad, ya que evita la creación de las credenciales necesarias para acceder a muchas aplicaciones diferentes y también "oculta" los atributos de identidad de todos menos del proveedor de identidad original.

Open Authorization (OAuth) 2.0 es un marco, especificado por el Grupo de trabajo de ingeniería de Internet (IETF) en llamadas de funciones remotas (RFC) 6749 y 6750 (publicado en 2012) diseñado para admitir el desarrollo de protocolos de autenticación y autorización. OpenID Connect (OIDC) es un protocolo de autenticación interoperable basado en la familia de especificaciones OAuth 2.0. Permite que varias aplicaciones autentiquen usuarios sin asumir la responsabilidad de almacenar y administrar contraseñas. OpenID Connect se diseñó para admitir también aplicaciones nativas y aplicaciones móviles, mientras que SAML se diseñó solo para aplicaciones basadas en web.

FIDO define las especificaciones del marco de autenticación universal (UAF) y del segundo factor universal (U2F). Juntos, definen un poderoso modelo de autenticación de usuario, uno que aprovecha la criptografía de clave pública establecida en el servidor, pero también normaliza una arquitectura conectable para la autenticación local. En FIDO, el usuario se autentica lógicamente en el dispositivo local (teléfono, PC, etc.) a través de una variedad de métodos. Este método de autenticación desbloquea una clave privada (previamente registrada en el servidor) para firmar una cadena de desafío de autenticación. El servidor está aislado de los detalles desordenados de la autenticación real del usuario y solo necesita admitir un protocolo criptográfico mucho más simple.

Traducido: *Francisco Javier González García*

Blockchain es una tecnología emergente con casos de uso identificados en el dominio de la identificación digital para proporcionar una identidad soberana propia. “Las cadenas de bloques públicas pueden proporcionar un registro descentralizado y el descubrimiento de las claves públicas necesarias para proporcionar firmas digitales. Estos dos pasos allanan el camino para establecer una utilidad pública global para la identidad soberana: una identidad digital portátil de por vida que no depende de ninguna autoridad central y que nunca se puede quitar”.[160]

*Sovrin: un protocolo y un token para la identidad soberana propia y la confianza descentralizada.*Un libro blanco de la Fundación Sovrin, versión 1.0, enero de 2018.https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

Figura 14: Marcos de Autenticación y Confianza: Tecnologías y Protocolos

Se evalúan las siguientes tecnologías: blockchain (un tipo de tecnología de registro distribuido o DLT), protocolos como OpenID connect y OAuth 2.0, FIDO (UAF), FIDO (U2F) y SAML. La Figura 15 muestra los resultados del Marco de Evaluación de Tecnología para cada uno de estos.

5.1. cadena de bloques

Blockchain, a veces denominada "tecnologías de libro mayor distribuido" (DLT), es una tecnología emergente que registra transacciones en orden cronológico en un libro mayor descentralizado que se aloja en "nodos" o servidores en una infraestructura de igual a igual. Como dijo un observador: “Imagínese una hoja de cálculo que se duplica miles de veces en una red de computadoras y luego la red está diseñada para actualizar periódicamente esta hoja de cálculo”.[161]

Las cadenas de bloques son inmutables: alguien no puede editar un registro que ya existe, sino que se debe crear un nuevo registro para mostrar las correcciones o cambios en un registro existente. Luego se verifica la autenticidad de ese registro a través de un mecanismo de consenso y se agrega un nuevo bloque a la cadena. El tipo de mecanismo de consenso utilizado depende de la arquitectura y el uso de la cadena de bloques. Los mecanismos comunes de consenso son "prueba de trabajo", "prueba de participación" y "prueba de autoridad". La "Prueba de trabajo" involucra muchos nodos de la red que compiten para resolver un problema matemático complejo primero, y a su vez obtienen una recompensa y la responsabilidad de cerrar el bloque de transacciones. La "Prueba de participación" implica que los titulares de grandes cantidades de tokens en el sistema se seleccionen al azar para aceptar cerrar el bloque de transacciones. La "prueba de autoridad" implica la emisión de autoridad a los miembros de la red que luego cierran el bloque de transacciones. Los mecanismos de consenso gobiernan la velocidad de agregar transacciones a una cadena de bloques, así como los recursos necesarios para agregarlas.

Aunque en sus primeras etapas, las tecnologías de cadena de bloques se están explorando como un tejido de confianza de identidad que permite a las personas controlar su identidad descentralizada, incluido dónde y cuándo comparten información de atributos de identidad. La ventaja de utilizar un sistema distribuido para la verificación de identidad es que no se depende únicamente de una sola

autoridad, y los atributos de identidad de una persona no se pueden quitar de forma arbitraria o abrupta. Dicha identidad generalmente se denomina identidad digital autónoma (SSID).

En este momento, las cadenas de bloques se pueden clasificar en tres tipos, dependiendo de cómo se les otorgue acceso a los usuarios para ver, leer y escribir datos en la cadena.

> ·**Blockchains públicas y sin permiso son** libros de contabilidad distribuidos abiertos al público para leer y escribir o verificar transacciones válidas utilizando la plataforma blockchain. El ejemplo más conocido de una cadena de bloques pública y sin permiso es Bitcoin. Las cadenas de bloques públicas se aseguran a través de un mecanismo de consenso basado en incentivos económicos y verificación criptográfica, como prueba de trabajo o prueba de participación. El principal inconveniente de la prueba de trabajo es la cantidad de potencia informática necesaria y los costes energéticos necesarios.
> ·**Blockchains públicas y autorizadas son** registros distribuidos donde el proceso de consenso está controlado por un conjunto preseleccionado de nodos, generalmente un consorcio de participantes que han establecido un marco de confianza legalmente vinculante. Las transacciones reales en la red son visibles públicamente y, por lo tanto, verificables.
> ·**Blockchains privados y autorizados utiliza** el mismo proceso de consenso que una cadena de bloques pública y autorizada, sin embargo, las transacciones solo pueden ser vistas por aquellos que participan en la red. Por ejemplo, imagine un consorcio de 15 instituciones financieras. Cada uno opera un nodo, y diez de ellos deben firmar cada bloque para que el bloque sea válido. El derecho a leer el libro mayor distribuido está restringido a los participantes.
> Para las aplicaciones de identidad digital, hay un mayor uso de libros de contabilidad autorizados entre las partes de confianza, ya que este enfoque proporciona mayores velocidades de transacción y una mejor privacidad de los datos. Muchos sistemas de identificación respaldados por cadenas de bloques propuestos son ejemplos de identificaciones acumuladas, por lo que la tecnología de cadenas de bloques se puede utilizar para registrar

BlockGeeks (19 de septiembre de 2016).*¿Qué es la tecnología de cadena de bloques? Una guía paso a paso para principiantes.*Obtenido de:https://blockgeeks.com/guides/what-is-blockchain-technology/

¿Qué problemas puede resolver?

·**Privacidad.** Sistemas de identidad Blockchain, diseñados con privacidad por principios de diseño puede proporcionar a las personas los medios para controlar y compartir información de identidad con terceros, sin compartir información que no es necesaria para realizar transacciones.

·**Seguridad.** Cualquier alteración de las transacciones en una cadena de bloques es fácilmente visible. Esta propiedad fomenta la confianza en los datos, minimizando la necesidad de instituciones centrales para verificar los datos. Los mecanismos de criptografía y consenso integrados en la tecnología blockchain hacen que sea muy difícil para los usuarios maliciosos atacar.

Traducido: *Francisco Javier González García*

·**Adopción (verificación transfronteriza).**Las soluciones de identidad descentralizadas basadas en blockchain podrían respaldar potencialmente la verificación de identidad transfronteriza. La tecnología permite el acceso de las personas

Gautam Hazari (1 de noviembre de 2016).*La relación entre blockchain e identidad digital.*GSMA. Obtenido de:https://www.gsma.com/identity/the-relationship- between-blockchain-and-digital-identity

Fundación Sovrin (20 de noviembre de 2017).*La Realidad de la Identidad Blockchain*(presentación).

Cavoukian, A.*Privacidad por diseño Los 7 principios fundamentales.*Consejo de Arquitectura de Internet. Obtenido de:https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

y control sobre su identificación personal en cualquier parte del mundo. Sin embargo, la interoperabilidad entre diferentes plataformas es un desafío y es necesario desarrollar estándares para abordar esto.

¿Qué problemas no resuelve?

·**Complejidad.**Fundamentalmente, la tecnología blockchain no resuelve por sí sola el desafío del registro y la prueba de identidad. La integridad de las identificaciones basadas en una cadena de bloques depende de la integridad de los documentos o datos utilizados para incorporar a un individuo a una cadena de bloques (es decir, las afirmaciones verificables) o un volumen de transacciones para crear una identificación acumulada. Asimismo, no se puede garantizar la unicidad. No hay nada dentro de la arquitectura de la cadena de bloques que impida que una persona tenga múltiples pares de claves privadas.[165]Las claves privadas se pueden vincular a varias claves públicas, que pueden ser positivas o negativas, según el caso de uso.

·**Usabilidad.**Se necesita mucho trabajo para hacer que la tecnología blockchain sea fácil de usar para la mayoría de las personas. Por ejemplo, cuando una persona olvida su contraseña para un sistema de identidad centralizado, existe una opción de restablecimiento de contraseña regida por los proveedores del sistema. No existe una propiedad central para un sistema descentralizado y, en la actualidad, no existe una manera fácil para que una persona recupere sus claves privadas si las olvida o las pierde. Pasar a sistemas de identidad descentralizados significa que la carga administrativa de la información de identidad se transfiere de una organización experimentada a un individuo.

·**Adopción.**Las soluciones de cadena de bloques se vuelven más efectivas con más participantes, sin embargo, la escala requiere negociaciones legales, políticas y de confianza por adelantado entre los socios y una mayor comprensión de las capacidades de la tecnología Se necesita una conexión a Internet para acceder a una billetera y el lugar ideal para almacenar información de identidad, incluidas las claves privadas, es un teléfono inteligente, una tecnología que no está disponible en gran parte del mundo en desarrollo.

·**Seguridad.**Blockchain requiere una gran red de nodos para ser resistente a los ataques. Con una red más pequeña, aumentan las posibilidades de que un atacante pueda manipular

la mayoría de un nodo para registrar datos incorrectos. Esto se conoce como un ataque del 51%. Las soluciones de cadena de bloques consisten en otros componentes complementarios que pueden comprometerse más fácilmente que la propia cadena, como las carteras.
¿Qué problemas podría crear?

·**Privacidad.**Los datos en una cadena de bloques son inmutables, lo que tiene ramificaciones en la privacidad, incluido, por ejemplo, el "derecho al olvido". La seguridad criptográfica también tiene una vida útil limitada antes de que las nuevas tecnologías puedan romperla. Con esto en mente, la mayoría de los expertos de la industria creen que la información de identificación personal (PII) y la información biométrica nunca deben almacenarse en una cadena de bloques.

5.2. Marco de autenticación universal FIDO (UAF)

La alianza Fast Identity Online (FIDO) se formó en julio de 2012 para abordar la falta de interoperabilidad entre dispositivos de autenticación fuertes, así como los problemas que enfrentan los usuarios al crear y recordar múltiples nombres de usuario y contraseñas La Alianza FIDO actualmente tiene dos conjuntos de especificaciones para una autenticación más simple y más fuerte: Marco de autenticación universal (UAF) y Segundo factor universal (U2F). Esta sección se centra en el protocolo FIDO UAF, mediante el cual los usuarios registran su dispositivo y luego realizan

Yaga, Mell, Roby y Scarfone (enero de 2018).*Descripción general de la tecnología Blockchain.*NIST Obtenido de:https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

Nolan Bauerle (16 de marzo de 2017).*¿Cuáles son los problemas y limitaciones de Blockchain?*Obtenido de:https://www.coindesk.com/ information/blockchains-issues-limitations/

Alianza FIDO (13 de noviembre de 2013).*Acerca de la Alianza FIDO.*Obtenido de:https://fidoalliance.org/about/overview/

autenticación en ese dispositivo. FIDO UAF funciona según el principio de la criptografía de clave pública y consta de los siguientes pasos:

·**Inscripción.** Se crea un par de claves pública y privada que el protocolo utiliza para autenticar a los usuarios. El dispositivo del usuario retiene la clave privada, mientras que la clave pública se comparte con el servicio digital.
·**Autenticación.** El usuario puede autenticarse en el dispositivo local utilizando métodos biométricos o no biométricos. Durante el inicio de sesión, el servicio en línea desafía la autenticidad del usuario. Luego, el usuario se autentica a sí mismo mediante datos biométricos o cualquier otro método de autenticación en el dispositivo local. Una vez que el usuario se autentica en el dispositivo local, el dispositivo responde al desafío del servicio en línea enviando un desafío firmado al servicio en línea. Luego, el servicio en línea verifica la respuesta del dispositivo con la clave pública almacenada y permite que el usuario inicie sesión.
¿Qué problemas puede resolver?

Traducido: *Francisco Javier González García*

·**Escalabilidad.** FIDO se puede integrar con una variedad de servicios en línea en todas las industrias. Los protocolos permiten estándares universales y, con el aumento de la cantidad de teléfonos inteligentes habilitados para biometría, una gran cantidad de dispositivos pueden implementar la tecnología. Una vez aprovisionado, el mismo dispositivo se puede usar para múltiples cuentas y servicios sin ningún costo ni esfuerzo adicional, lo que permite su reutilización para diversos servicios en todas las industrias.

·**Actuación.** Debido a que el dispositivo físico permanece con el usuario y los datos biométricos se almacenan en él, el tiempo de respuesta es muy rápido. Además, el servidor almacena solo una clave pública cifrada para el usuario; Los datos biométricos se almacenan en el dispositivo físico del usuario. La autenticación ocurre en el dispositivo físico y solo se envía una clave privada al servidor para que coincida con la clave pública para completar la autenticación. ¿Resultado? El proceso requiere poco almacenamiento de datos en el servidor y el cálculo es simple y fácil.

·**Adopción.** Gracias a la funcionalidad simple de la tecnología y las indicaciones automáticas del software, las personas necesitan poca capacitación para aprender a usarla. Y debido a que un PIN o datos biométricos se almacenan en un dispositivo físico local en posesión del usuario, la aceptación de la tecnología por parte del usuario es alta.

·**Seguridad.** Debido a que la autenticación ocurre localmente, y solo ocurre la coincidencia de pares de clave privada/pública en un servidor, la solución es muy segura. Almacenar la clave privada en el dispositivo del usuario proporciona una autenticación más fácil y sólida al mismo tiempo que protege la privacidad del usuario. Los protocolos no generan información que permita a los proveedores de servicios en línea rastrear a los usuarios. La información biométrica para la autenticación nunca sale del dispositivo del usuario, lo que hace que las posibilidades de una brecha de seguridad sean extremadamente bajas.

¿Qué problemas no resuelve?

·**Madurez.** Algunos protocolos de seguridad y autenticación relacionados con esta tecnología aún no están aprobados. Solo el protocolo de certificación FIDO está completo.

·**Seguridad.** Como marco de autenticación, FIDO se diseñó para la inscripción (registro) y la autenticación descentralizados. El marco no admite la identificación única; esto tendría que ser manejado por separado.

¿Qué problemas podría crear?

·**Actuación.** Las organizaciones que buscan implementar FIDO también necesitan un plan sin FIDO, porque los usuarios pueden perder su dispositivo registrado u olvidarse de llevarlo consigo.

·**Seguridad.** Para las organizaciones que planean hacer que los servicios en línea sean accesibles para todos los dispositivos personales (BYOD), la diversidad de dichos dispositivos presenta importantes desafíos de seguridad y usabilidad. Eso es porque las personas usarán el mismo dispositivo tanto para uso privado como profesional. es por lo tanto

Es imperativo que las organizaciones garanticen la seguridad de estos dispositivos y la información de credenciales contenida en ellos. Se requerirán controles adicionales para garantizar el cumplimiento de las políticas de seguridad de las organizaciones.

Traducido: *Francisco Javier González García*

5.3. Segundo factor universal FIDO (U2F)

FIDO U2F es un nuevo estándar de autenticación publicado por FIDO Alliance. El objetivo de este protocolo es simplificar el proceso de autenticación de dos factores con un estándar abierto, seguro y fácil de usar. U2F permite la autenticación resistente al phishing utilizando hardware de usuario final dedicado que podría ser dispositivos Bluetooth, dispositivos USB o dispositivos biométricos. Estos dispositivos no requieren controladores especiales; solo necesitan un navegador web compatible. Una vez que el sitio web verifica la contraseña del usuario, entra la autenticación U2F. Utilizando un par de claves públicas y privadas, el sitio web envía un "desafío" al navegador, que el dispositivo U2F conectado a la máquina firma y devuelve. Estos dispositivos se integran directamente con el navegador y mitigan muchas técnicas de robo de credenciales, como el registro de claves, el phishing y otros ataques. El segundo factor fuerte permite que el servicio simplifique sus contraseñas (por ejemplo, puede requerir solo un PIN de cuatro dígitos) sin comprometer la seguridad.[169]

¿Qué problemas puede resolver?

·**Seguridad.** Con U2F, una clave puede admitir el acceso a muchos servicios en línea, sin la necesidad de compartir información de usuario o crear claves de cifrado. Por lo tanto, el usuario nunca es rastreado.
·**Actuación.** Debido a que el dispositivo físico permanece con el usuario y usa un PIN para la validación, el tiempo de respuesta es muy rápido. Y debido a que el servidor almacena solo una clave pública cifrada para el usuario, los requisitos de almacenamiento de datos para un usuario son muy bajos. Los datos biométricos se almacenan en el dispositivo físico, no en el servidor. La autenticación ocurre completamente en el dispositivo físico del usuario y solo se envía una clave privada al servidor para que coincida con la clave pública para completar la autenticación. Por lo tanto, el cálculo es simple y fácil.
·**Adopción.** Gracias a la funcionalidad simple de la tecnología y las indicaciones automáticas del software, las personas necesitan poca capacitación para aprender a usarla. Y debido a que un PIN o datos biométricos se almacenan en los dispositivos físicos de los usuarios, lo que otorga una mayor seguridad, la aceptación del protocolo por parte de los usuarios es alta.
·**Escalabilidad.** Una vez aprovisionado, el mismo dispositivo se puede usar para múltiples cuentas y servicios sin ningún costo ni esfuerzo adicional, lo que permite su reutilización para numerosos servicios en todas las industrias. El tiempo requerido para configurar el dispositivo es bastante bajo.
¿Qué problemas no resuelve?

·**Seguridad.** La tecnología no elimina la necesidad de contraseñas, porque las partes de retransmisión aún necesitan autenticar a las personas mediante el uso de contraseñas antes de registrarse en FIDO U2F.
·**Adopción.**Los usuarios siempre deben llevar un dispositivo físico para la autenticación. Los dispositivos pueden ser costosos y propensos a robo o pérdida.
¿Qué problemas podría crear?
·**Asequibilidad.**La tecnología es costosa y requiere inversiones en componentes de

infraestructura FIDO, como tokens de seguridad y autenticadores FIDO. Además, los gastos operativos pueden ser considerables debido a los costos necesarios para la implementación, el soporte y la logística de la distribución de tokens nuevos.

168 Duo Security (21 de octubre de 2014).*FIDO U2F—Segundo factor universal.*Obtenido de:https://youtu.be/v-GvJJEG9sw169 Alianza FIDO (13 de noviembre de 2013).*Enfoque y Visión.*Obtenido de:https://fidoalliance.org/approach-vision/

·**Adopción.**Si las personas pierden su dispositivo o cambian de dispositivo, deben registrar nuevos dispositivos utilizando contraseñas. Esto cancela el beneficio principal de la tecnología de acceso a través de un modo sin contraseña.

5.4. Autenticación automática 2.0

OAuth 2.0 es un protocolo estándar abierto basado en token para la autorización delegada a través de Internet. Proporciona aplicaciones cliente con acceso delegado seguro. OAuth funciona sobre el protocolo de transferencia de hipertexto (HTTP) y autoriza dispositivos, API, servidores y aplicaciones con tokens de acceso en lugar de credenciales. La tecnología permite a los usuarios autorizar su identidad a servicios de terceros, sin tener que compartir sus credenciales. OAuth 2.0 asume que el usuario está autenticado (por el servicio que aloja la cuenta de usuario) y no define cómo se debe realizar la autenticación. Cuando un usuario accede a los servicios con un token de OAuth, los servicios no necesitan saber quién es el usuario, siempre que tenga un token válido. El proveedor de identidad lo hace posible mediante la emisión de un token a la aplicación de terceros con la aprobación del usuario.

El acceso administrado por el usuario (UMA) es una extensión de OAuth 2.0 que define cómo los propietarios de los recursos pueden controlar el acceso de un recurso a las partes solicitantes, donde los recursos residen en varios servidores diferentes y un servidor de autorización centralizado rige las políticas de acceso. Con UMA, el administrador de autorización (AM) incluido permite a los usuarios delegar el control de acceso de las aplicaciones host al AM. Como resultado, los administradores pueden redactar políticas de control de acceso de manera uniforme y en un único lenguaje de políticas de su elección. El beneficio de esto en los sistemas de identificación digital es que UMA como guardián digital permite que un usuario administre, defina y monitoree preferencias detalladas para compartir sus datos de múltiples fuentes. Los usuarios pueden elegir quién puede ver sus datos, qué tipo de datos se envían y durante cuánto tiempo se puede acceder a los datos. Esto facilita agregar una capa de consentimiento a la API y las aplicaciones a través de estándares.[170]

¿Qué problemas puede resolver?

·**Madurez.** Los tokens de OAuth 2.0 permiten una integración más sencilla de los servicios web a través de las interfaces de programación de aplicaciones (API) sin necesidad de compartir los datos de las credenciales de los clientes. Por lo tanto, el mecanismo permite a los usuarios compartir la información de su cuenta con aplicaciones o sitios web de terceros.
·**Actuación.** Esta tecnología no almacena los datos de las credenciales de los clientes y solo proporciona un flujo de autorización a través del cual una fuente de terceros puede autorizar a un usuario. Por lo tanto, se producen muy pocos errores y defectos en la autorización cuando los usuarios inician sesión.

Traducido: *Francisco Javier González García*

·**Adopción.** OAuth 2.0 es independiente del proveedor, fácil de usar y fácil de aprender, lo que fomenta la adopción. Además, no compromete la privacidad de los clientes, mejorando aún más la aceptación.
·**Asequibilidad.** La tecnología es altamente reutilizable. Una vez que se define e implementa el flujo, muchas aplicaciones pueden usarlo sin incurrir en costos adicionales.
·**Seguridad.** La implementación de aplicaciones con OAuth 2.0 garantiza que sean independientes del proveedor y puedan soportar cambios en las políticas y los entornos del lado del servidor.
¿Qué problemas no resuelve?

·**Actuación.** La cantidad de solicitudes que OAuth 2.0 puede manejar depende de la configuración del servidor. La tecnología también depende de cuántas solicitudes puede procesar un servidor de terceros en cualquier momento y cuánto tiempo lleva procesarlas.
170 Ámbar Osborne (noviembre de 2016).*Compartir es cuidar: los beneficios del acceso administrado por el usuario.*Obtenido de:http://www.think-progress.com/wp-content/uploads/2016/11/Content_Sharing-Caring-r4.pdf

·**Escalabilidad.** OAuth 2.0 aún no se ha utilizado en ningún programa de identificación digital. Por lo tanto, aún no se ha determinado su escalabilidad.
·**Seguridad.** Debido a que OAuth 2.0 solo valida el origen y la integridad del token, cualquier persona puede usar un token robado.
·**Asequibilidad.** La configuración de OAuth 2.0 requiere la implementación de un servidor dedicado, lo que puede resultar costoso. Sin embargo, el uso de servicios de infraestructura en la nube puede reducir los costos de hardware.

5.5. Conexión de identificación abierta

OpenID Connect proporciona a los desarrolladores un marco para crear sistemas de autenticación seguros y funcionales para uso móvil. Es un estándar abierto para la autenticación diseñado para funcionar junto con las capacidades de autorización de OAuth 2.0. Una capa de seguridad de identidad construida sobre OAuth 2.0, permite la verificación de la identidad de un usuario final, así como la obtención de información de perfil básica sobre el usuario. Lo logra agregando un token de identidad a la autorización de OAuth 2.0. OpenID Connect permite controlar cuánta información sobre un usuario se compartirá con sitios web de terceros que él o ella visite. Las credenciales de usuario nunca se transmiten a esos sitios. OpenID Connect confirma la identidad del usuario y comparte solo aquellos detalles que el usuario ha autorizado a compartir. En un futuro cercano, más ofertas de software como servicio (SaaS) aceptarán tokens de identificación, lo que simplificará en gran medida el desarrollo de aplicaciones que pueden autenticar a los usuarios para aplicaciones basadas en API.

La diferencia entre OAuth 2.0 y OpenID Connect es que OAuth 2.0 es principalmente un protocolo de delegación de acceso, a través del cual los propietarios de recursos otorgan

permisos o derechos de acceso al cliente solicitante con la ayuda de tokens de acceso. El protocolo OpenID Connect se basa en las especificaciones de OAuth 2.0, con un token de ID adicional que brinda información sobre el usuario (por ejemplo, cómo y cuándo se autenticó). Los dispositivos móviles pueden utilizar los servicios de autenticación de OpenID Connect a través de las API. Los operadores de redes móviles están adoptando gradualmente este protocolo habilitador para satisfacer la creciente demanda del mercado de servicios de identidad móvil.

A medida que los usuarios buscan formas de autenticación más seguras y eficientes, los estándares cambian constantemente. A medida que esta tecnología madure, la adopción por parte de las grandes agencias gubernamentales puede aumentar.

¿Qué problemas puede resolver?

·**Madurez.** OpenID Connect permite a los desarrolladores autenticar personas en sitios web y aplicaciones sin necesidad de que los desarrolladores y las aplicaciones posean y administren archivos de contraseña. Por lo tanto, la tecnología permite un uso sencillo de las identidades digitales en sitios web y aplicaciones a través de cualquier dispositivo informático o móvil. Esta capacidad crea un ecosistema seguro, flexible e interoperable para la identidad digital. Además, la tecnología se puede integrar fácilmente con múltiples sistemas y plataformas.
·**Actuación.** Debido a que OpenID Connect tiene una capa de seguridad integrada sobre el token OAuth 2.0, niega la dependencia de autorizaciones de terceros, lo que aumenta la cantidad de solicitudes que la tecnología puede manejar.
·**Escalabilidad.** OpenID Connect almacena los datos de credenciales de los clientes en su propio servidor para la auto-autenticación. Debido a que almacena solo nombres de usuario y contraseñas, no consume muchos datos, lo que fomenta una alta escalabilidad.
·**Seguridad.** Debido a que OpenID Connect se basa en OAuth 2.0 y se autentica automáticamente, es más seguro que OAuth 2.0. Y debido a que los servidores de terceros no están involucrados, el estándar es menos propenso a defectos en los datos y menos vulnerable a condiciones excepcionales.
·**Asequibilidad.** Con OpenID Connect, las personas pueden usar las mismas credenciales para acceder a múltiples servicios sin incurrir en ningún costo o esfuerzo adicional.

¿Qué problemas no resuelve?

·**Seguridad.**Si se roban las credenciales de los clientes, su seguridad está en riesgo.
·**Asequibilidad.**La configuración de la infraestructura para OpenIDConnect requiere un servidor de datos local y un sistema sólido para garantizar que los datos se almacenen de forma segura en el servidor. Por lo tanto, los costos de software y hardware son

significativos. Sin embargo, el uso de servicios de almacenamiento basados en la nube puede mitigar los costos de hardware.

5.6. SAML

SAML significa Security Assertion Markup Language, un estándar abierto basado en XML. Este protocolo admite el intercambio de información de autorización y autenticación entre socios comerciales a través de servicios web. Los usuarios finales pueden acceder a contenido exclusivo en varios sitios o aplicaciones con un solo inicio de sesión. Se dice que la identificación de un usuario ha sido federada entre un conjunto de proveedores cuando los proveedores han acordado un conjunto de identificadores o atributos de identidad por los cuales los sitios se referirán al usuario.

El ecosistema de SAML consta de dos partes, la parte que afirma SAML y la parte que confía en SAML. En el corazón de la mayoría de las aserciones SAML hay un sujeto (un sujeto principal, una entidad que se puede autenticar, dentro del contexto de un dominio de seguridad) sobre el cual se está afirmando algo. El sujeto podría ser un ser humano o algún otro tipo de entidad, como una empresa o una computadora.

La tecnología SAML comprende los siguientes componentes:
·**Afirmación.** La parte afirmante afirma la información de seguridad en forma de declaraciones sobre un tema. Una aserción contiene información básica obligatoria y opcional que se aplica a todas las declaraciones y, por lo general, contiene el sujeto y las condiciones utilizadas para validar la aserción.
·**Protocolos.** Estos incluyen reglas de solicitud/respuesta para realizar tareas, como autenticación, cierre de sesión único, consulta de aserción, solicitud y resolución de artefactos.
·**Encuadernaciones .**Estos explican cómo los mensajes del protocolo SAML se pueden transportar a través de los protocolos de transporte subyacentes (como la redirección HTTP y la publicación HTTP).

¿Qué problemas puede resolver?

·**Madurez.** La tecnología ha estado en uso durante un tiempo y se ha implementado con éxito en muchas funciones gubernamentales y corporativas, lo que demuestra la amplia aceptación de este protocolo. Las pautas basadas en XML respaldan la integración de los

requisitos de autenticación en múltiples plataformas en diferentes tecnologías, independientemente de la pila de tecnología general.
·**Escalabilidad.** Las pautas de la federación SAML se pueden adoptar fácilmente en cualquier ecosistema de usuarios finales de proveedores de servicios.
·**Adopción.** El sistema simple y fácil de usar fomenta una fácil adopción, aunque aún no se ha probado la adopción por parte de sistemas de transacciones seguras.

Desarrolladores de Onelogin (21 de mayo de 2015).*Resumen de desarrollo de SAML*.Obtenido de:https://developers.onelogin.com/saml
Oasis (25 de marzo de 2008).*Descripción técnica del Lenguaje de marcado para aserción de seguridad (SAML) V2.0*.Obtenido de:http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

¿Qué problemas no resuelve?

·**Seguridad.** La tecnología es vulnerable a una serie de amenazas diferentes. Por ejemplo, en los ataques de repetición, los piratas informáticos secuestran un token SAML y lo reproducen para obtener acceso ilícito a los servicios. En la falsificación del sistema de nombres de dominio (DNS), los piratas informáticos interceptan un token SAML y envían una dirección DNS falsa. Y en los ataques de referencia HTTP, los piratas informáticos reutilizan una etiqueta de referencia HTTP.

·**Escalabilidad.** Las tarjetas no electrónicas brindan pocas oportunidades para escalar la tecnología SAML. Y sin posibilidad de almacenamiento de datos, la tecnología no puede proporcionar muchas funciones integradas.

5.7. Tendencias clave en autenticación y marcos de confianza: tecnologías y protocolos

Los desarrolladores de todo el mundo están trabajando en un sistema de identidad basado en blockchain, autónomo y de código abierto que permitirá que las personas, los productos, las aplicaciones y los servicios interactúen entre blockchains, proveedores de la nube y organizaciones gubernamentales. Las organizaciones también se esfuerzan por establecer estándares y mejores prácticas que respalden la interoperabilidad y fomenten la confianza entre los diferentes tipos de tecnología de cadena de bloques.

Por ejemplo, el Gobierno de Dubái anunció recientemente un plan para utilizar la tecnología blockchain para verificar toda la información en una tarjeta de identificación de los Emiratos. Los detalles relacionados con un residente se almacenarían en la tarjeta, incluidos los documentos del seguro, la información del pasaporte y los datos de salud, y para 2020 se almacenarán en cadenas de bloques, estarán protegidos y encriptados.[174]Mientras tanto, la Iniciativa Blockchain de Illinois, en asociación con el proveedor de soluciones de identidad auto-soberana Evernym, utilizará el registro de identidad distribuido de la Fundación Sovrin para crear una identidad segura y auto-soberana para los residentes de Illinois durante el proceso de registro de nacimiento.[175]

Sin embargo, es necesario llevar a cabo una gestión de cambios efectiva en las ubicaciones de los países para garantizar que las actitudes de las personas hacia la cadena de bloques y la tecnología involucrada se entiendan completamente antes de la migración a esta tecnología.

Traducido: *Francisco Javier González García*

Por el contrario, OpenID Connect está ganando rápidamente adopción en la web, con más de 1 BN de cuentas de usuario habilitadas para OpenID Connect y más de 50 000 sitios web que aceptan OpenID Connect para inicios de sesión. Varias grandes organizaciones emiten o aceptan OpenID, incluidas Google, Facebook, Yahoo!, Microsoft, AOL, Myspace, Sears, Universal Music Group, France Telecom, Novell, Sun y Telecom Italia.

Al mismo tiempo, el grupo de trabajo de OAuth 2.0, cuyo objetivo es aumentar la interoperabilidad de las implementaciones de OAuth y mejorar la seguridad, busca agregar un flujo de dispositivos de OAuth 2.0 (que normalmente utilizan las aplicaciones en dispositivos con capacidades limitadas de entrada o visualización, como televisores u otros electrodomésticos). El objetivo es permitir que dispositivos como los teléfonos móviles impulsen la popularización de los dispositivos IoT.[176]

Jem Jensen (7 de marzo de 2017).*Atacar SSO: vulnerabilidades comunes de SAML y formas de encontrarlas.*NETSPI. Obtenido de:https://blog.netspi.com/attacking-sso-common-saml-vulnerabilities-ways-find/

Tobias Young (14 de marzo de 2017).*La tecnología Blockchain supera los obstáculos para simplificar la vida de todos.*El Nacional. Obtenido de:https://www.thenational.ae/business/blockchain-technology-cuts-through-the-hurdles-to-simplify-everyone-s-lives-1.85148

Iniciativa Blockchain de IL (31 de agosto de 2017).*Illinois se asocia con Evernym para lanzar un programa piloto de registro de nacimientos.*La Iniciativa Blockchain de Illinois. Obtenido de:https://illinoisblockchain.tech/illinois-partners-with-evernym-to-launch-birth-registration-pilot-f2668664f67c

Gartner (2017).*Los Hype Cycles de 2017 destacan las disrupciones digitales de empresas y ecosistemas.*Gartner, Inc. Obtenido de:https://www.gartner.com/technology/research/hype-cycles/

Mientras tanto, los protocolos de autenticación FIDO se muestran prometedores y un gran grupo de proveedores admiten las especificaciones FIDO. Sin embargo, el potencial de FIDO como plataforma completamente interoperable aún no se ha desarrollado.

Gartner predice que para 2019, el 20 % de las organizaciones admitirán FIDO 2.0 para servicios en línea B2E (empresa a empleado).

Microsoft también está defendiendo un marco de dispositivo complementario de Windows Hello. Esta es una API abierta que utiliza dispositivos externos, como dispositivos portátiles u otros dispositivos equipados con Bluetooth con sensores biométricos, para habilitar la seguridad biométrica para dispositivos que no la tienen y para extender la verificación a cualquier sitio o servicio que admita los estándares FIDO 2.0. Las iniciativas del gobierno regional, como la Agencia de Transformación Digital de Australia, los servicios del gobierno del Reino Unido y el Departamento de Comercio de los EE. UU. han implementado FIDO UAF para la autenticación de usuarios. Algunas grandes corporaciones, incluidas Bank of America, Microsoft, PayPal, MasterCard y Google, también lo han adoptado.

Además, las aplicaciones de software se están construyendo para admitir una variedad de protocolos federados para autenticar, administrar y auditar la identidad del usuario a través de sitios de intranet y extranet. También se han desarrollado varios marcos de confianza y pautas de interoperabilidad en el espacio de identidad federada.

Traducido: *Francisco Javier González García*

Las organizaciones han establecido marcos de confianza como el intercambio abierto de identidades y la gestión de acceso, credenciales e identidad del gobierno federal. A través de este marco de confianza, los proveedores de identidades y las partes de confianza acuerdan confiar e intercambiar credenciales entre ellos de acuerdo con las directrices y políticas definidas.

La federación y el inicio de sesión único (SSO) federado se están convirtiendo rápidamente en el mecanismo estándar para proporcionar SSO en todas las aplicaciones, y se está convirtiendo en el mecanismo de autenticación preferido con empresas y en todas las aplicaciones. Esto se debe a la compatibilidad nativa con SAML en muchos paquetes de software y la adopción de aplicaciones SaaS.[180]El marco de interoperabilidad de eIDAS para respaldar los procesos de identificación y autenticación transfronterizos utiliza SAML 2.0 para el intercambio de mensajes, según lo acordado en el subgrupo técnico de eIDAS, y se detalla en la Arquitectura de interoperabilidad de eIDAS.

Gartner (2017).*Los Hype Cycles de 2017 destacan las disrupciones digitales de empresas y ecosistemas.*Gartner, Inc. Obtenido de:https://www.gartner.com/technology/research/hype-cycles/

Bhat, M. y Singh, A. (13 de diciembre de 2016).*Perspectiva de innovación para protocolos en línea de identidad rápida.*Gartner, Inc. Obtenido de:https://www.gartner.com/doc/3540023/innovation-insight-fast-identity-online

Bhat, M. y Singh, A. (13 de diciembre de 2016).*Perspectiva de innovación para protocolos en línea de identidad rápida.*Gartner, Inc. Obtenido de:https://www.gartner.com/doc/3540023/innovation-insight-fast-identity-online

Brett Valentine (5 de julio de 2017).*Tendencias actuales en gestión de acceso e identidad: julio de 2017.*SeguridadInteligencia de IBM. Obtenido de:https://securityintelligence.com/current-trends-in-identity-and-access-management-july-2017/

Incorporación de la Comisión Europea.*Formato de mensaje eIDAS SAML.*Comisión Europea. Obtenido de:https://unirse. ec.europa.eu/sites/default/files/document/2015-11/eidas_message_format_v1.0.pdf

6. Tecnologías de análisis

En los sistemas de identificación digital, el análisis se puede utilizar para crear una identidad integral para un individuo mediante la combinación de datos de múltiples fuentes. El uso de tales análisis agrega una capa de inteligencia al perfil de identidad de un individuo. En este informe, se examina lo siguiente (consulte la Figura 17): análisis de riesgo, análisis predictivo, actividad comercial y análisis operativo, y coincidencia biográfica (búsqueda difusa). La Figura 18 muestra los detalles del marco de evaluación de tecnología para cada subtecnología de análisis.

6.1. Análisis de riesgos

Los gobiernos y las organizaciones pueden utilizar el análisis de riesgos principalmente para predecir el comportamiento fraudulento y delictivo de un individuo y para asignar una puntuación de riesgo basada en información como su historial financiero o social, antecedentes penales e instancias de impago de préstamos. Hoy en día, el análisis de riesgos se usa más en el sector privado que en los sistemas de autenticación e identificación digital. Los análisis de riesgos o amenazas se combinan con sistemas de identidad emergentes como Enterprise Mobility + Security (EMS) de Microsoft y de

Traducido: *Francisco Javier González García*

Google en Gmail para analizar y marcar el riesgo durante la autenticación del usuario. Estos algoritmos comprueban si hay actividad de inicio de sesión sospechosa; por ejemplo, cuando un usuario inicia sesión desde un nuevo dispositivo o ubicación. El algoritmo también analiza los patrones de inicio de sesión para marcar actividades sospechosas. Por ejemplo, si un usuario inicia sesión desde algún lugar de los Estados Unidos a las 9:00a.metro. y luego intenta iniciar sesión desde India a las 9:00 pag.metro., el sistema marcará esto como una anomalía, ya que no existe una forma realista de que el usuario recorra esa distancia en 12 horas.

Pero los gobiernos utilizan cada vez más información basada en datos para medir, cuantificar y predecir el riesgo. La precisión de los modelos de riesgo se puede mejorar continuamente mediante la validación de los resultados de los modelos mediante retroalimentación estadística. También pueden mejorar la confianza en el resultado de un modelo de riesgo mediante el uso de información altamente confiable, como bases de datos de pasaportes, como entradas para el modelo.

Gracias al espectacular aumento de la potencia informática en los últimos años, junto con la maduración de los algoritmos analíticos, las organizaciones ahora pueden implementar técnicas analíticas avanzadas a gran escala.

¿Qué problemas puede resolver?

·**Actuación.** El análisis de riesgos integra un gran volumen de datos estructurados y no estructurados en una vista única y unificada, a partir de la cual los operadores pueden recopilar información valiosa y conocimientos prácticos. Los servicios de inmigración, por ejemplo, utilizan estos modelos analíticos para evaluar los perfiles de riesgo de los visitantes extranjeros en función de sus patrones de viaje. Además, a medida que los resultados se validan mediante comentarios estadísticos, la precisión de los modelos mejora continuamente.

·**Asequibilidad.** Los modelos de análisis de riesgos presentan oportunidades considerables para que las organizaciones y los departamentos generen ingresos que compensen los costos, porque los resultados y la información de estos modelos se pueden usar para tomar decisiones más informadas en una amplia gama de contextos, incluida la identificación.

¿Qué problemas no resuelve?

·**Asequibilidad.** Para obtener valor del análisis de riesgos, las organizaciones deben invertir en hardware potente y software avanzado. Esos son costosos, al igual que los profesionales de capacitación y los modelos de datos.

·**Seguridad.** Los datos en un modelo de análisis de riesgos están sujetos a robo y manipulación durante el almacenamiento y la transmisión, a menos que se apliquen controles de datos y procesos en cada etapa del proceso de análisis para mejorar la seguridad.

·**Adopción.** Los requisitos de capacitación son altos y la construcción de un modelo de riesgo requiere habilidades tanto en negocios como en tecnología.

¿Qué problemas podría crear?

·**Adopción.** La recopilación de datos por parte de las agencias gubernamentales para perfilar a las personas podría generar preocupaciones sobre la vigilancia en línea. Eso podría catalizar una fuerte oposición del público.

·**Actuación.** La mala calidad de los datos podría hacer que el modelo entregue recomendaciones falsas.

6.2. Análisis predictivo

El análisis predictivo utiliza datos, algoritmos estadísticos y técnicas de aprendizaje automático para predecir la probabilidad de posibles resultados futuros en función de los datos históricos. Todavía no ha encontrado mucha aplicabilidad en los sistemas de identificación digital. Sin embargo, se están realizando algunas investigaciones sobre cómo se podrían usar tales análisis para predecir cómo la huella dactilar de una persona podría cambiar con la edad.

¿Qué problemas puede resolver?

·**Actuación.** El tiempo de respuesta general de los modelos de análisis predictivo es alto cuando utilizan el marco de procesamiento de datos correcto, la ubicación de los datos y los formatos de salida apropiados, incluso cuando los datos de varias fuentes se combinan y analizan para obtener información. Además, estos modelos se pueden usar para predecir cómo podría cambiar la plantilla biométrica de un individuo con la edad. Esto podría ser útil para hacer coincidir la biometría con una muestra de prueba más antigua.
·**Escalabilidad.** Los modelos de análisis predictivo utilizan datos transaccionales y de comportamiento de múltiples fuentes y se pueden escalar para adaptarse a volúmenes de datos cada vez mayores. La aparición de los servicios de computación en la nube ha hecho que los modelos de análisis predictivo sean aún más escalables.
·**Asequibilidad.** Las tecnologías basadas en la nube han reducido considerablemente los costos necesarios para implementar una solución de análisis predictivo.
¿Qué problemas no resuelve?
·**Seguridad.** Las soluciones de análisis predictivo son similares a las soluciones de análisis de riesgos en que son vulnerables al robo de datos.
·**Asequibilidad.** Estas soluciones requieren una amplia formación de modelos y científicos de datos.***¿Qué problemas podría crear?***
·**Adopción.**La recopilación de datos, como la huella en línea de una persona, podría generar inquietudes sobre la privacidad y las violaciones éticas.

6.3. Análisis de actividades y operaciones comerciales

Los proveedores de servicios pueden utilizar análisis de operaciones y actividades comerciales para analizar datos operativos en tiempo real, con el objetivo de mejorar la eficiencia de los procesos comerciales a través del monitoreo continuo.

¿Qué problemas puede resolver?

·**Actuación.** Los modelos de análisis de actividades y operaciones comerciales pueden analizar grandes volúmenes de datos estructurados y no estructurados para encontrar las causas fundamentales de los problemas de prestación de servicios.
·**Escalabilidad.** La computación basada en la nube ha reducido la complejidad y el tiempo requerido para la implementación de estos modelos analíticos, mejorando la escalabilidad.
·**Seguridad.**Las soluciones de administración de acceso e identidad pueden garantizar un cumplimiento estricto y mejorar la seguridad al proteger y monitorear el acceso de las personas a los modelos.

¿Qué problemas no resuelve?

·**Asequibilidad.** Estos modelos requieren inversiones significativas en canales de intercambio de datos de alta velocidad, potencia informática e infraestructura de red para facilitar el procesamiento paralelo y ejecutar algoritmos de datos a gran escala. La infraestructura de transferencia de datos debe actualizarse e integrarse para manejar todo tipo de datos, lo que aumenta aún más los gastos.
·**Adopción.** Estos modelos requieren una comprensión profunda de los temas técnicos de nicho. Hay pocos científicos de datos expertos, arquitectos de datos y modeladores analíticos trabajando en esta área.
·**Actuación.** La mala calidad de los datos de entrada y la gestión inadecuada de los datos pueden dar lugar a imprecisiones en los resultados de los modelos.

6.4. Coincidencia biográfica (búsqueda aproximada)

La coincidencia biográfica utiliza la llamada búsqueda difusa para realizar menos del 100 % de coincidencias en los datos de identidad. La coincidencia aproximada permite la extracción de datos de fuentes de datos biográficos dispares, junto con la normalización y eliminación de duplicados de los datos. También permite la coincidencia semántica para extraer el significado del texto no estructurado. Por ejemplo, el software puede hacer coincidir la palabra "grande" con "grande" o "coche" con "automóvil" porque están relacionados semánticamente.
La coincidencia de nombres multiculturales es un ejemplo de ello. La coincidencia aproximada resuelve situaciones en las que se deben identificar como relacionadas diferentes versiones del nombre de una persona que residen en múltiples fuentes. Una persona puede tener múltiples versiones de su nombre por varias razones. Por ejemplo, el

individuo tiene un apodo, se casa y adopta el apellido del cónyuge, o recibe un título o título superior. La transliteración, la traducción o incluso los errores simples de ingreso de datos también pueden generar variaciones en el nombre de una persona. Estas variaciones pueden ser problemáticas para los funcionarios que buscan buscar, fusionar o desduplicar registros en una base de datos de identidad. En tales situaciones, y en muchas otras, la búsqueda difusa puede ayudar a los funcionarios a encontrar los registros del nombre de una persona que de otro modo no se encontrarían. Por ejemplo, los nombres Dan Thomas y Daniel Thomas pueden ser la misma persona, y R.S Singh y Ram Sewak Singh pueden ser la misma persona. Los algoritmos de búsqueda difusa se pueden entrenar o programar para hacer estas asociaciones.

¿Qué problemas puede resolver?

·**Actuación.** Los algoritmos difusos son útiles para administrar la coincidencia de nombres multiculturales y mejorar las capacidades de búsqueda de OCR. También se pueden usar para búsquedas parciales de texto y admiten varios idiomas.

¿Qué problemas no resuelve?

·**Madurez.** La tecnología de coincidencia de datos biográficos todavía está evolucionando y la tecnología no se ha estandarizado. La falta de estándares y protocolos de interoperabilidad para la comparación de datos biográficos dificulta la integración de datos biográficos no estructurados y no estandarizados de múltiples fuentes.
·**Escalabilidad .**Los algoritmos complejos, los altos requisitos de almacenamiento de datos y el tiempo computacional prolongado dificultan el escalado de esta tecnología.
·**Seguridad.** Debido a que la mayoría de las bases de datos contienen datos no estructurados, no es fácil verificar la integridad de la base de datos después de un ataque.
·**Asequibilidad.** Los datos no estructurados requieren más espacio de almacenamiento y el desarrollo de algoritmos de búsqueda difusa es costoso. Además, los algoritmos no se pueden reutilizar para otros proyectos.
·**Actuación.** Estos sistemas no pueden acomodar un gran número de consultas a la vez, y las consultas difusas tardan más en ejecutarse que las consultas regulares.

6.5. Tendencias clave en tecnologías de análisis

Las tecnologías de análisis están disfrutando de un fuerte crecimiento en el mercado. El análisis predictivo ha visto un aumento particularmente rápido en popularidad, con muchas organizaciones adoptando técnicas innovadoras, como redes neuronales y aprendizaje automático. El análisis predictivo podría ayudar a reducir las tasas de error debido al envejecimiento de la plantilla. El envejecimiento de la plantilla biométrica se define como un aumento en la tasa de error de reconocimiento con un mayor tiempo desde la inscripción. Los datos biométricos de un usuario cambian con la edad, las condiciones médicas o el desgaste normal. El análisis predictivo podría simular los efectos del envejecimiento en la plantilla biométrica almacenada utilizada para comparar con la muestra de prueba, lo que reduce las coincidencias falsas y los rechazos.

Traducido: *Francisco Javier González García*

Junto con el análisis predictivo, la IA se está utilizando en formas tales como asistentes virtuales y chatbots para mejorar la experiencia de las personas en el uso de los servicios digitales gubernamentales. Nueva Zelanda planea usar IA para la verificación en tiempo real de la identidad digital de las personas. Dubái ha creado su primer asistente de inteligencia artificial para responder a las consultas de las personas sobre los servicios de electricidad y agua. La junta de turismo de Singapur planea usar IA para predecir y personalizar las experiencias de los visitantes.[183]

Para los países que buscan construir sistemas de identificación digital, el uso de análisis para respaldar la autenticación continua ayudará a crear una mejor experiencia de usuario y mejorará la seguridad y la resiliencia de los datos. Las herramientas pueden recopilar información discretamente de varias fuentes, incluido el uso de dispositivos móviles por parte de las personas, para crear un perfil que sea único para el propietario de la cuenta y que no pueda ser robado ni replicado por usuarios fraudulentos.[184]

Las plataformas de identificación y autenticación se están empaquetando con análisis integrados, que agregan capacidades analíticas y de generación de informes. La integración de una plataforma de inteligencia empresarial (BI) con la arquitectura de identificación permitirá la toma de decisiones en tiempo real, generará información y revelará patrones en los datos que ayudarán a las agencias gubernamentales a mejorar la prestación de servicios públicos. Las nuevas tecnologías de la información y la comunicación (TIC), como las redes sociales, también se están utilizando para facilitar la verificación de identidad de colaboración colectiva. Las iniciativas de acción colectiva habilitadas digitalmente por parte de actores no estatales (como organizaciones sin fines de lucro) resultarán invaluables, especialmente en lugares que carecen de gobernanza democrática. Por ejemplo, la plataforma Ushahidi se utilizó para monitorear las elecciones de 2011 en Nigeria. Mientras tanto, para mejorar los procesos KYC, muchas organizaciones están aplicando análisis de identidad o inteligencia de identidad a las redes sociales, datos no estructurados, públicos o poco confiables recopilados a través de búsquedas abiertas en Internet.

Mientras tanto, el análisis del comportamiento del usuario es una nueva área prometedora que se centra en el comportamiento digital de los usuarios, como las aplicaciones lanzadas, la actividad de la red y los archivos a los que se accede. Esta tecnología conecta datos de fuentes tan dispares para obtener información sobre amenazas potenciales, sugeridas por comportamientos inusuales, como múltiples fallas de inicio de sesión y acceso desde una ubicación desconocida.

Los modelos de análisis de actividades y operaciones comerciales se utilizan para presentar información relacionada con indicadores clave de rendimiento (KPI). Estos, a su vez, se utilizan para proporcionar información sobre la actividad y el rendimiento de un sistema de identificación. Los profesionales técnicos y de operaciones comerciales pueden usar dicha información para detectar problemas inminentes, como cuellos de botella en el procesamiento de datos. Por ejemplo, el sistema Aadhaar de la India analiza el rendimiento en métricas importantes para operadores, máquinas y dispositivos, como el tiempo dedicado a ciertos procesos y tasas de error de tareas, tasas de error en centros de inscripción particulares y el tiempo dedicado a un

Fenker, S.P., Ortiz, E. y Bowyer, K.W. (2013).*Fenómeno de envejecimiento de la plantilla en el reconocimiento de iris.*Acceso IEEE, vol. 1, págs. 266–274. Obtenido de:http://ieeexplore.ieee.org/document/6516567/

Traducido: *Francisco Javier González García*

Basu, M. y Rohaidi, N. (29 de junio de 2017).*The Briefing: Cómo los gobiernos globales están usando la IA en este momento.*GovInsider. Obtenido de:https://govinsider.asia/innovation/the-briefing-global-governments-ai-artificial-intelligence/

Gartner (2017).*Los Hype Cycles de 2017 destacan las disrupciones digitales de empresas y ecosistemas.*Gartner, Inc. Obtenido de:https://www.gartner.com/technology/research/hype-cycles/

pantalla particular durante la inscripción y otros procesos. Las alertas sobre eventos de interés se procesan en tiempo real y se envían a los paneles.

El análisis de la actividad comercial y las operaciones también puede generar notificaciones automáticas que se pueden enviar a grupos de personas o a un individuo o departamento en particular, según el problema en cuestión. La resolución de problemas automatizada, cuando sea factible, puede corregir o reiniciar cualquier proceso fallido relacionado con la identificación y la autenticación.

Con el uso cada vez mayor de programas de identificación digital, surge una necesidad apremiante de detectar anomalías en el sistema derivadas del robo de identidad y tomar medidas correctivas. Las nuevas tecnologías, como las redes neuronales, ahora se están explorando para encontrar factores relevantes en el comportamiento de los usuarios, como los tiempos de viaje, la ubicación del usuario y los servicios solicitados, con el objetivo de detectar anomalías.

Basado en una discusión de SME con Sanjay Jain, exgerente jefe de productos de UIDAI.

Tanprasert, T., Saiprasert, C. y Thajchayapong, S. (2017).*Combinación de detección de anomalías no supervisadas y redes neuronales*

*para la identificación del conductor.*Revista de Transporte Avanzado, vol. 2017, artículo ID 6057830, 13 páginas. Obtenido de:https://www.hindawi.com/journals/jat/2017/6057830/

7. Otras consideraciones

Este informe ha proporcionado una revisión y evaluación sólidas de las tecnologías de identificación digital en seis parámetros. En el contexto de la planificación de la implementación de la identificación digital, es importante evaluar estas tecnologías a través de la lente de factores adicionales, como la privacidad y la protección de datos, los estándares abiertos y la neutralidad del proveedor, la demografía, la cultura, los niveles de servicio requeridos, la viabilidad económica y las limitaciones de infraestructura. , para apoyar aún más las decisiones eficaces.

7.1. Privacidad y Protección de Datos

Además de las consideraciones enumeradas anteriormente, los gobiernos también deben tomar medidas para implementar un marco de gobernanza adecuado y definir políticas sobre qué datos personales se capturan, dónde se capturan, cómo se protegen los datos capturados de ataques e intrusiones, y cómo la privacidad de los ciudadanos. y se preserva la confidencialidad de los datos. Los gobiernos también deben especificar claramente para qué fines se utilizarán los datos y quién

tendrá acceso a los datos, y establecer mecanismos para garantizar que se obtenga el consentimiento de las personas antes de acceder a los datos y utilizarlos. Las personas también deben contar con los recursos legales apropiados en caso de que sus datos se usen indebidamente o se implementen con malas intenciones.

Los regímenes de privacidad y protección de datos deben establecer derechos y obligaciones predecibles con respecto al tratamiento de datos individuales e información de identificación personal (PII) que son una parte importante para establecer confianza en los sistemas digitales, confianza que luego fomenta el uso. Entre otras cosas, estos regímenes garantizan que las personas deben saber quién tiene acceso a los datos personales y otorgan a las personas control sobre el intercambio de datos personales, así como derechos para acceder y corregir dichos datos. El daño causado por una violación, robo o compromiso de datos puede resultar en robo de identidad, daño físico, discriminación y angustia emocional, lo que hace que las personas pierdan la fe (confianza) en el sistema. Y las organizaciones también pueden sufrir pérdidas financieras, erosión de la reputación y la confianza, y responsabilidad legal en casos de violación de datos.[188]Además de los requisitos legales y reglamentarios de aplicación general que protegen los datos y garantizan la privacidad, este informe también destaca ejemplos de principios desarrollados por la industria aplicados a ciertas tecnologías.

7.2. Estándares abiertos y neutralidad de proveedores

Según los Principios para la identificación a los que se hizo referencia anteriormente, “Los principios de diseño abierto permiten la competencia y la innovación basadas en el mercado. Son esenciales para una mayor eficiencia y una mejor funcionalidad de los sistemas de identificación, tanto dentro del país como a través de las fronteras. Además, se deben implementar pautas sólidas de adquisición de TIC para facilitar la competencia y la innovación y evitar posibles "bloqueos" de tecnología y proveedores que pueden aumentar los costos y reducir la flexibilidad para adaptarse a los cambios a lo largo del tiempo. Se debe fomentar la neutralidad y la diversidad tecnológica para aumentar la flexibilidad y evitar el diseño de sistemas que no sean aptos para su propósito o adecuados para cumplir con los objetivos de políticas y desarrollo”.

> Ver Dividendos *digitales,*Informe sobre el desarrollo mundial 2016, en la página 222 y siguientes, Banco Mundial; disponible en:http://www.worldbank.org/en/publication/wdr2016
>
> instituto Nacional de Estándares y Tecnología, Departamento de Comercio de EE. UU. (abril de 2010). Guía para proteger la confidencialidad de la información de identificación personal (PII). Obtenido de NIST:http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

7.3. Demografía

Condiciones como el tamaño, la distribución, la composición y los movimientos de la población son importantes a la hora de elegir tecnologías para los programas de identificación digital. Por ejemplo,

la madurez de las tecnologías de coincidencia de huellas dactilares e iris ha permitido su uso con grandes poblaciones. La captura de huellas dactilares sin contacto y la captura del iris a distancia, por otro lado, están surgiendo, lo que permite un procesamiento más rápido de más personas de lo que pueden admitir los dispositivos de captura tradicionales.

Con la tecnología móvil cada vez más omnipresente, el registro móvil brinda la oportunidad de expandir el alcance de los sistemas de identificación a personas incluso en áreas remotas. Esto es especialmente útil en poblaciones que están escasamente distribuidas en terrenos extensos y remotos. El registro móvil se puede utilizar para capturar las credenciales de las personas, incluso en áreas remotas, siempre que haya una conexión móvil disponible. Si bien la mayoría de las soluciones móviles se han probado en pilotos limitados, su aplicabilidad en los sistemas de identificación digital aún se está estudiando.

7.4. Cultura

La elección de la tecnología también debe alinearse con las prácticas culturales de la sociedad en la que se implementa el programa de identificación. En culturas donde las personas pueden percibir el contacto físico con escáneres biométricos como antihigiénico o indeseable, las innovaciones como la captura de huellas dactilares sin contacto y la captura del iris a distancia se han vuelto importantes. En algunas culturas, por ejemplo, es inaceptable que un agente masculino en un sitio de registro de identificación digital toque las manos de una mujer para colocarlas correctamente en el dispositivo de captura de huellas dactilares. Las tecnologías sin contacto pueden aliviar tales preocupaciones.

El reconocimiento facial también se está volviendo popular rápidamente. Con su experiencia de autenticación perfecta y la mejora de la precisión, es posible que incluso reemplace la toma de huellas dactilares en un futuro próximo. No depende del contacto físico con las personas para la autenticación y, por lo tanto, puede usarse en culturas donde el contacto físico no es deseable. También se puede usar en escenarios como viajes transfronterizos cuando se deben realizar rápidamente grandes cantidades de autenticaciones.

Si bien la tecnología de reconocimiento facial todavía es susceptible de cambiar, está mejorando rápidamente, especialmente con la llegada del reconocimiento facial 3D. Sin embargo, en culturas donde las mujeres se cubren la cara con un niqab o velo, el reconocimiento facial puede ser difícil de usar. Por esta razón, muchos países de Medio Oriente han adoptado tecnologías de captura y comparación de iris en el control de inmigración.

La tecnología de ADN rápido ha reducido el tiempo y el costo para procesar muestras de ADN. El uso de la tecnología de perfilado rápido de ADN y comparación de ADN es altamente preciso y estable. Sin embargo, también es controvertido en los programas de identificación digital, debido a su potencial para revelar información altamente sensible y confidencial, como información genética, de salud y familiar sobre la vida privada de las personas sin su consentimiento. Por lo tanto, la aceptación cultural de cualquier solución basada en ADN sigue siendo baja.

7.5. Requisitos de nivel de servicio

Los niveles de servicio relacionados con la identificación y la autenticación se pueden evaluar según criterios como el rendimiento (¿cuántas transacciones por hora debe admitir el sistema?), el tiempo de respuesta (¿qué tan rápido debe responder el sistema?) y la precisión (¿cuánto ¿Cuántos FAR están permitidos dado un FRR en particular?).

El texto legible por máquina y las tecnologías de tarjetas inteligentes sin contacto se han implementado ampliamente para proteger y facilitar la lectura de la información de los pasaportes electrónicos. Esto está aumentando la cantidad de viajeros que se pueden procesar por unidad de tiempo en los carriles de inspección manuales y automatizados.

Hacer cumplir la calidad de la muestra biométrica en la captura y/o comparación puede ayudar a mejorar la precisión, al igual que el uso de tecnologías de fusión biométrica dentro de una modalidad o en múltiples modalidades.

7.6. Viabilidad Económica

Si bien ciertas tecnologías pueden permitir que los países implementen un programa de identificación eficiente, es posible que no sean económicamente viables. Por ejemplo, las tarjetas inteligentes sin contacto pueden ser útiles en algunos contextos culturales. Pero son más caras que las tarjetas de identificación tradicionales, lo que las pone fuera del alcance de los gobiernos con recursos financieros comparativamente menores, como los de las economías emergentes.

De manera similar, blockchain puede tener una aplicabilidad limitada en los países en desarrollo. Sus costos de transacción son altos en comparación con otras tecnologías de bases de datos, ya que cada transacción debe verificarse en múltiples nodos.

Las tecnologías FIDO, SAML y OpenID son útiles en la federación de identidades, como se describe anteriormente en este informe. Esto es especialmente relevante para las economías emergentes, porque las tecnologías reducen la necesidad de diferentes registros funcionales para mantener su propia base de datos de personas o usuarios. Estas tecnologías ofrecen no solo costos más bajos sino que también mejoran la seguridad.

7.7. Restricciones de infraestructura

Las restricciones de infraestructura en áreas sin cobertura de red móvil y baja penetración de Internet y telefonía móvil pueden influir en la elección de las tecnologías a utilizar para los sistemas de identificación. La tecnología de sistema biométrico en tarjeta (BSoC), por ejemplo, reduce la dependencia de la red en regiones con conectividad de red deficiente porque combina el sensor biométrico y el comparador en una tarjeta inteligente, eliminando así la necesidad de enviar la información biométrica a un servidor central o base de datos para emparejar. BSoC también aumenta la seguridad, porque la información biométrica nunca sale de la tarjeta. Sin embargo, no se han realizado pruebas o pilotos a gran escala para esta tecnología, y los estándares de interoperabilidad no se han desarrollado completamente.

Traducido: *Francisco Javier González García*

Las soluciones de identificación y autenticación basadas en dispositivos móviles, como Mobile Connect, pueden ser útiles en economías emergentes con una alta penetración móvil, como Nigeria,[189]donde la mayoría de los internautas acceden a través de sus teléfonos móviles. Sin embargo, la solución asume que las personas tienen teléfonos inteligentes y que la conectividad de la red es sólida, condiciones que pueden ser menos frecuentes en los países en desarrollo.

7.8. Conclusión

Las tecnologías y tendencias cubiertas en este informe están evolucionando rápidamente, y sus desafíos y limitaciones asociados destacados aquí pueden no ser aplicables en el futuro. Por lo tanto, se anima a los lectores a considerar este informe como una instantánea en el tiempo. Sin embargo, el marco de evaluación de tecnología presentado en este informe, con sus parámetros de evaluación de adopción, asequibilidad, rendimiento, seguridad, escalabilidad y madurez, resultará útil para evaluar tecnologías incluso en el futuro y, por lo tanto, ayudará a los lectores a tomar decisiones tecnológicas más informadas.

Muchos países han logrado avances significativos en la implementación de sus respectivos programas de identificación digital. A medida que más países adopten y amplíen estos programas, los países en desarrollo se beneficiarán al aprender de las experiencias de aquellos que están más adelante en la curva de implementación. Comprender los desafíos y beneficios de varias tecnologías, sus costos asociados y la adopción en diferentes grupos socioeconómicos y culturales permitirá a los gobiernos desarrollar programas de identificación que mejor se adapten a sus características, desafíos y oportunidades únicos.

Statista (enero de 2017). Tráfico de Internet móvil como porcentaje del tráfico web total a enero de 2017, por país. estatista. Obtenido de:https://www.statista.com/statistics/430830/share-of-mobile-internet-traffic-countries/

Apéndice 1. Otras consideraciones de diseño

Las tecnologías emergentes y los conceptos de diseño que se tratan en esta sección, aunque no son fundamentales para los sistemas de identificación y autenticación, siguen siendo importantes para los países que buscan establecer sistemas de identificación a nivel nacional.

Interfaces de programación de aplicaciones (API)

Una API desacopla una aplicación de software de su implementación de funcionalidad subyacente. El desacoplamiento o acoplamiento flexible es un término de software que se utiliza para implicar que un componente no depende en gran medida del otro componente y, por lo tanto, se puede cambiar una parte de manera segura sin afectar a la otra. Aquí, tales términos implican que para las API, las

características de la aplicación de software se pueden cambiar sin afectar demasiado la funcionalidad.

Las API abiertas permiten a los propietarios de un servicio accesible en red dar acceso universal a los consumidores de ese servicio. También permiten que los desarrolladores externos accedan a datos de back-end que los desarrolladores pueden usar para crear nuevas aplicaciones o mejorar sus aplicaciones existentes. Por lo tanto, los países podrían buscar publicar conjuntos de datos y API en línea para que los desarrolladores creen aplicaciones ricas y útiles para los usuarios. Las plataformas de identificación nacional como Aadhaar en India y Smart Nations en Singapur han adoptado especificaciones API abiertas para integrar sus bases de datos de identificación nacional con aplicaciones externas.

Las API abiertas permiten que el contenido o los datos que se crean en un lugar se compartan y actualicen dinámicamente a través de múltiples canales, como la web, los dispositivos móviles y la televisión. También automatizan la generación de contenido y datos en todos los canales. Esto fomenta el intercambio y la distribución eficiente de datos, y una mayor precisión del contenido y los datos. Estas API también reducen la necesidad de que los gobiernos de los proveedores de ID únicos inviertan directamente en los esfuerzos de desarrollo de aplicaciones. Esto se debe a que los desarrolladores independientes pueden crear aplicaciones innovadoras que agregan valor a la forma en que los consumidores usan los datos de identificación únicos. Además, las API abiertas ayudan a impulsar la innovación de nuevos productos y servicios a través de colaboraciones público-privadas.

Los ejemplos incluyen LTA DataMall, que proporciona API relacionadas con viajes; las API de la Autoridad Monetaria de Singapur (MAS), que ayudan a las instituciones financieras y a los proveedores de servicios de aplicaciones a atender mejor a sus clientes; y las API de OneMap, que permiten a los usuarios insertar un mapa interactivo de Singapur en sitios web para proporcionar servicios basados en la ubicación.[190]

La seguridad es fundamental cuando se trata de API. Si un servicio API se viola o se ve comprometido, los datos internos subyacentes de una organización pueden ser vulnerables a los piratas informáticos. Además, si el sistema carece de herramientas efectivas de equilibrio de carga, un aumento en la cantidad de llamadas a la API de otras aplicaciones y servicios puede provocar una sobrecarga del sistema.

microservicios

Los microservicios permiten a los desarrolladores crear grandes aplicaciones como una colección de servicios modulares poco acoplados, a diferencia de la arquitectura monolítica tradicional. Estos servicios implementan capacidades comerciales, como responder a solicitudes de identificación o autenticación, y son independientes y escalables individualmente. Dicho de otra manera, en lugar de crear una gran aplicación para lograr un resultado específico, los desarrolladores crean la aplicación como un conjunto de servicios más pequeños interconectados. Este enfoque facilita a los desarrolladores comprender, desarrollar, probar y escalar la aplicación y fomenta el desarrollo ágil de aplicaciones. Múltiples proveedores en los sectores privados están utilizando plataformas de

microservicio basadas en arquitectura orientada a servicios (SOA) para proporcionar servicios de inscripción, deduplicación y autenticación.

En los sistemas de identificación digital, que utilizan procesos complejos, la modularidad es vital para probar, integrar, implementar, escalar y actualizar estos sistemas. Y si la demanda de un servicio específico aumenta, por ejemplo, aumenta la cantidad de llamadas a la API, los operadores del sistema pueden escalar los microservicios correspondientes según sea necesario para satisfacer esa demanda, sin necesidad de escalar todo el sistema. Esta capacidad de escalar las diferentes aplicaciones de componentes de forma independiente según sea necesario crea eficiencia, porque no todas las partes de una aplicación experimentan la misma cantidad de carga.

Quizás no sea sorprendente que los microservicios hayan tenido una amplia adopción, ya que muchas empresas del sector privado e incluso servicios gubernamentales como el Servicio Digital del Gobierno del Reino Unido han pasado de una arquitectura monolítica a una de microservicios.

Sin embargo, esta mayor modularidad conlleva cierto compromiso en el rendimiento. Por ejemplo, el rendimiento de una aplicación puede reducirse si se producen grandes volúmenes de llamadas de servicio y tráfico de red en la red distribuida. Un sistema modular también puede ser vulnerable a la latencia de la red (que es la cantidad de tiempo que tarda un mensaje en atravesar un sistema) y la pérdida de paquetes (que ocurre cuando uno o más paquetes de datos que viajan a través de una red informática no logran llegar a su destino). Los microservicios tradicionalmente han sido ineficientes para la transmisión de información, debido a que la presencia de una barrera de seguridad independiente para cada servicio para autenticar la identidad ralentiza el proceso. Sin embargo, se están realizando algunas innovaciones para ayudar a crear un mecanismo de autenticación distribuido para microservicios.

Smart Nation Singapur. Información abierta. Gobierno de Singapur. Obtenido de:https://www.smartnation.sg/resources/open-data

En el futuro, los microservicios, junto con las API, permitirán que las agencias gubernamentales construyan plataformas de identificación más centradas en el individuo.

Bases de datos en memoria

Las bases de datos en memoria (IMDB) almacenan todos o parte de los datos en la memoria de acceso aleatorio (RAM) en lugar del almacenamiento en disco secundario. La mayoría de los sistemas de reconocimiento biométrico modernos utilizan mecanismos de almacenamiento de datos en memoria para maximizar las velocidades de identificación y coincidencia. En dichos sistemas, las plantillas se almacenan y combinan en la memoria y se conservan (para operaciones de restauración) en repositorios de datos tradicionales.

Trabajar con datos en la memoria es mucho más rápido que escribir y leer desde un sistema de archivos o una unidad de disco, tecnología magnética o de estado sólido. Por este motivo, las bases de datos en memoria pueden acelerar significativamente la identificación o la des-duplicación y la autenticación en la gestión de identidades al reducir en gran medida el tiempo necesario para acceder a los datos. El almacenamiento de datos en la memoria también puede permitir el análisis en

tiempo real de los datos de identidad, lo que incluye la evaluación de riesgos basada en modelos y la coincidencia biográfica (por ejemplo, la coincidencia de nombres multiculturales).

Sin embargo, el almacenamiento de datos en memoria cuesta mucho más que el almacenamiento en disco tradicional. Además, los operadores deben comprender las reglas de acceso a los datos en los diferentes nodos del servidor y los mecanismos para cargar datos en la memoria. Todo esto conlleva una pronunciada curva de aprendizaje. Además, en IMDB, la información en memoria normalmente no está cifrada para permitir un procesamiento más rápido. Esto crea vulnerabilidad a ataques y robo de datos. Se están realizando investigaciones para evaluar la eficacia de la coincidencia de plantillas cifradas, pero actualmente no existen tales algoritmos en producción. Otras ideas de mitigación de riesgos incluyen anonimizar o separar la PII para minimizar el almacenamiento de todos los datos en una ubicación, lo que evita la creación de un "tarro de miel" que atrae a piratas informáticos o ladrones de datos.

Bases de datos NoSQL

Las bases de datos NoSQL facilitan la gestión de datos a través de un diseño de base de datos no relacional o sin esquema, en su mayoría de código abierto y escalable. Por lo tanto, se diferencian de las bases de datos tradicionales, que utilizan un modelo o esquema relacional para ordenar los datos existentes o cualquier dato nuevo entrante en filas y columnas.

Debido a que las bases de datos NoSQL no se basan en relaciones tabulares para almacenar y recuperar datos, cuentan con velocidades de procesamiento rápidas, especialmente cuando se trata de datos no estructurados o semiestructurados. También funcionan bien en una arquitectura distribuida (una configuración donde los componentes ubicados en computadoras en red se comunican y coordinan para lograr un objetivo común). Y escalan bien al permitir fácilmente la adición de nodos. Se utilizan principalmente para manejar grandes volúmenes de datos en diversos formatos.

Con las bases de datos tradicionales, a menudo se necesita una cantidad considerable de tiempo y recursos para alinear los datos relacionados con la identidad en esquemas fijos o para crear otros nuevos que satisfagan las necesidades operativas. Esto puede requerir la creación de flujos complejos que requieran un esfuerzo considerable para diseñar y actualizar. A veces, es posible que se deban eliminar datos útiles porque no encajan en el esquema. Las bases de datos NoSQL mitigan estas restricciones al permitir que los datos no estructurados se guarden junto con los datos estructurados y aplicar un esquema según sea necesario.

Las bases de datos NoSQL son particularmente útiles para los programas de identificación digital con una gran población que genera un gran volumen de datos y que requieren un diseño de almacenamiento de datos ágil. Las agencias gubernamentales pueden usar bases de datos NoSQL para administrar el flujo continuo de datos de usuarios, algunos de los cuales podrían ayudar a las agencias a mejorar los servicios individuales. De hecho, se espera que las bases de datos NoSQL vean una mayor adopción en el futuro, debido a su esquema flexible, capacidades de gestión de datos de gran volumen y compatibilidad con múltiples funciones de formato de datos.

Traducido: *Francisco Javier González García*

La implementación de bases de datos NoSQL también puede presentar algunos desafíos, como la integración con bases de datos relacionales tradicionales, especialmente si sus formatos de datos no son compatibles. Además, las bases de datos NoSQL, simplemente

al igual que las bases de datos tradicionales, también pueden ser susceptibles a ataques de inyección, mediante los cuales un extraño obtiene acceso a los datos residentes y los manipula porque requiere relativamente pocas restricciones relacionales y controles de consistencia.

Sistemas distribuidos

Un sistema informático distribuido consta de múltiples componentes de software que se encuentran en varias computadoras, pero se ejecutan como un solo sistema. Para los sistemas de identificación nacional, estas computadoras están geográficamente distantes y conectadas por una red de área amplia. Los sistemas distribuidos suelen tener un algoritmo o sistema de equilibrio de carga que asigna tareas a cada nota para minimizar el tiempo de ejecución general de una solicitud. Dichos sistemas se han utilizado tradicionalmente para gestionar grandes y complejos volúmenes de datos. Los datos físicos en un sistema distribuido se pueden organizar de tres maneras:

·**Particionado.**No se duplican datos.

·**Completamente duplicado.**Todos los datos se duplican en cada computadora en la red.

·**Parcialmente duplicado.**Algunos datos están duplicados en algunas computadoras en la red.

Los sistemas distribuidos se basan en el concepto de procesamiento paralelo, por lo que ofrecen un mayor rendimiento y tasas de respuesta en comparación con un sistema centralizado equivalente. Además, debido a la modularidad de la arquitectura, estos sistemas se pueden escalar fácilmente horizontalmente (agregando más nodos) y verticalmente (aumentando la potencia de procesamiento de cada nodo) para manejar volúmenes de datos cada vez mayores. Además, los sistemas distribuidos tienen una alta redundancia, por lo que una falla en una parte de la red no provocará la caída de todo el sistema. Esto aumenta la resiliencia de todo el sistema.

Sin embargo, estos sistemas también presentan desafíos. Estos incluyen altos costos de hardware, porque el sistema requiere que se configuren diferentes nodos o centros. Además, estos sistemas dependen de un software complejo para administrar varias funciones de manejo y recuperación de datos, y dicho software es costoso. La configuración de un sistema distribuido requiere profesionales altamente capacitados que comprendan a fondo los conceptos clave de la arquitectura de datos, como la autonomía del sitio, la transparencia del sistema, la replicación de datos y la partición. Tales practicantes son escasos. Finalmente, los sistemas distribuidos realizan numerosas transacciones de comunicación de datos dentro de los nodos informáticos y de datos. Un aumento en el número de nodos en el sistema lo hace vulnerable a posibles ataques a la red.

DevOps

Traducido: *Francisco Javier González García*

DevOps es una práctica de ingeniería de software que tiene como objetivo unificar el desarrollo y las operaciones de software. Se utiliza para admitir el desarrollo y la implementación rápidos y continuos de aplicaciones. Permite un enfoque ágil para acelerar los lanzamientos de aplicaciones de software e impulsar las innovaciones de la plataforma tecnológica. Como práctica, DevOps requiere que los desarrolladores de software y los equipos de operaciones trabajen juntos para crear, probar, implementar y mejorar las nuevas funciones de la aplicación.

Un elemento clave en DevOps se centra en el desarrollo, las pruebas y la implementación rápida de aplicaciones. Las organizaciones que usan DevOps pueden realizar estas actividades al automatizar el proceso de lanzamiento de software, desde la construcción hasta la implementación. Otro elemento clave en DevOps se enfoca en la operación y el monitoreo de aplicaciones, donde los equipos capturan, clasifican y analizan datos y registros generados por la aplicación. A través de este proceso, aprenden cómo las actualizaciones en la aplicación afectan a los usuarios finales y al rendimiento del sistema, y pueden hacer

Centro de conocimientos de IBM. Qué es la computación distribuida. IBM. Obtenido de:https://www.ibm.com/support/knowledgecenter/en/SSAL2T_8.2.0/com.ibm.cics.tx.doc/concepts/c_wht_is_distd_comptg.html

mejoras si es necesario. El sistema también genera alertas sobre los datos analizados, brindando más información a los equipos de desarrollo y operaciones.

En el futuro, DevOps podría ayudar a las agencias gubernamentales a modernizar sus grandes sistemas de identificación heredados al dividirlos en componentes pequeños e independientes que pueden mejorarse mediante un desarrollo y una entrega ágiles. Tal uso de DevOps podría mitigar el tiempo, los costos y los riesgos que conllevan las principales iniciativas de modernización en organizaciones grandes y complejas. Sin embargo, para aprovechar al máximo este uso de DevOps, las organizaciones gubernamentales deberán utilizar las tecnologías adecuadas y establecer una cultura colaborativa que fomente el intercambio de responsabilidades de desarrollo entre los equipos de TI. Las agencias del sector público que dominan DevOps podrían crear plataformas de verificación de identidad y autenticación utilizando un enfoque ágil que admita mejoras incrementales. Podrían abordar más rápidamente las deficiencias técnicas de dichas plataformas y desplegar nuevas capacidades (como la autenticación mediante múltiples modalidades) esenciales para la identificación y la autenticación.

DevOps mejora los enfoques existentes mediante el establecimiento de procesos optimizados para ofrecer resultados predecibles, ágiles, eficientes y de alta calidad en cada etapa del ciclo de vida del desarrollo de aplicaciones. Además, los desarrolladores y operadores trabajan juntos, lo que respalda la detección temprana y la corrección más rápida de defectos mediante el uso de pruebas automatizadas. El resultado más valioso es una mejor velocidad de comercialización con un producto de calidad que cumple o supera las expectativas.

Traducido: *Francisco Javier González García*