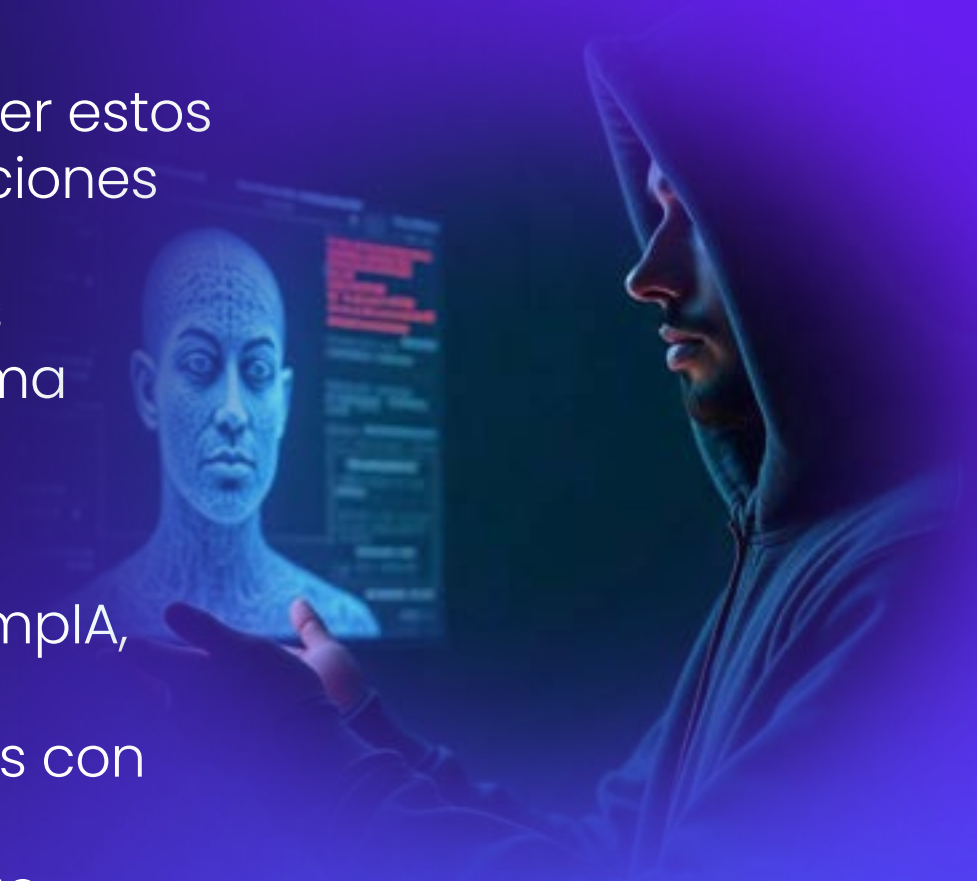
Nueva generación de identidad digital: **Tendencias para los próximos cinco años**

La identidad digital se proyecta como un factor clave para garantizar la verificación segura y eficaz de las personas en los entornos digitales. Su correcta implementación **permite optimizar procesos, reducir riesgos operativos y asegurar el cumplimiento de estándares regulatorios**, construyendo la ConfIAnza Digital que hoy es esencial para empresas y ciudadanos.

En este eBook presentamos las **principales tendencias que marcarán** la validación de identidad en los **próximos cinco años.** Comprender estos avances permitirá a las organizaciones prepararse para fortalecer sus operaciones, ofrecer experiencias seguras y consolidar un ecosistema digital sostenible.



Al final, te contamos cómo en OlimpIA, a través de nuestro portafolio **OlimpIA OKey,** estamos alineados con estas tendencias, brindando soluciones de identidad digital que integran tecnología de vanguardia.

¿SABÍAS QUE...?

En Colombia, los intentos de fraude por suplantación de identidad **crecieron un 60% en los últimos tres años,** impulsando la necesidad de evolucionar los modelos de validación digital.

Fuente: Asobancaria 2024.

Tendencia 1:

Validación de identidad multimodal

Con el aumento sostenido del fraude digital, impulsado por tecnologías como **deepfakes y métodos de suplantación** cada vez más sofisticados, las organizaciones están optando por reforzar sus procesos de autenticación a través de esquemas multimodales.

Esto significa que ya **no confían** en **un solo factor de verificación**, sino que integran varios mecanismos en un mismo flujo para hacer frente a entornos complejos o con altos volúmenes transaccionales.

Entre los **componentes principales** de esta tendencia se encuentran:

Reconocimiento facial

Un estudio de HID Global publicado en 2024 reveló que más del 70% de las empresas planean invertir en tecnologías que confirmen que hay una persona real frente a la cámara, y no una imagen o video manipulado. Además, los algoritmos actuales están diseñados para adaptarse a distintas características étnicas y de género, lo que garantiza inclusión y mayor precisión.

Biometría dactilar

Especialmente consolidada en regiones como América Latina y Asia, donde el informe de OneSpan de 2024 indica que cerca del 65% de los bancos ya usa huellas digitales para validar transacciones financieras y otros servicios críticos. Esta biometría compara la huella capturada en tiempo real con registros previos para confirmar la identidad de manera rápida y segura.

Validación automatizada de documentos

Mediante el uso de inteligencia artificial, estos sistemas analizan el diseño, marcas de seguridad y elementos gráficos de documentos de identidad oficiales (como cédulas nacionales y de extranjería, y pasaportes), reduciendo la necesidad de revisar manualmente cada caso.

Variables contextuales y sociodemográficas

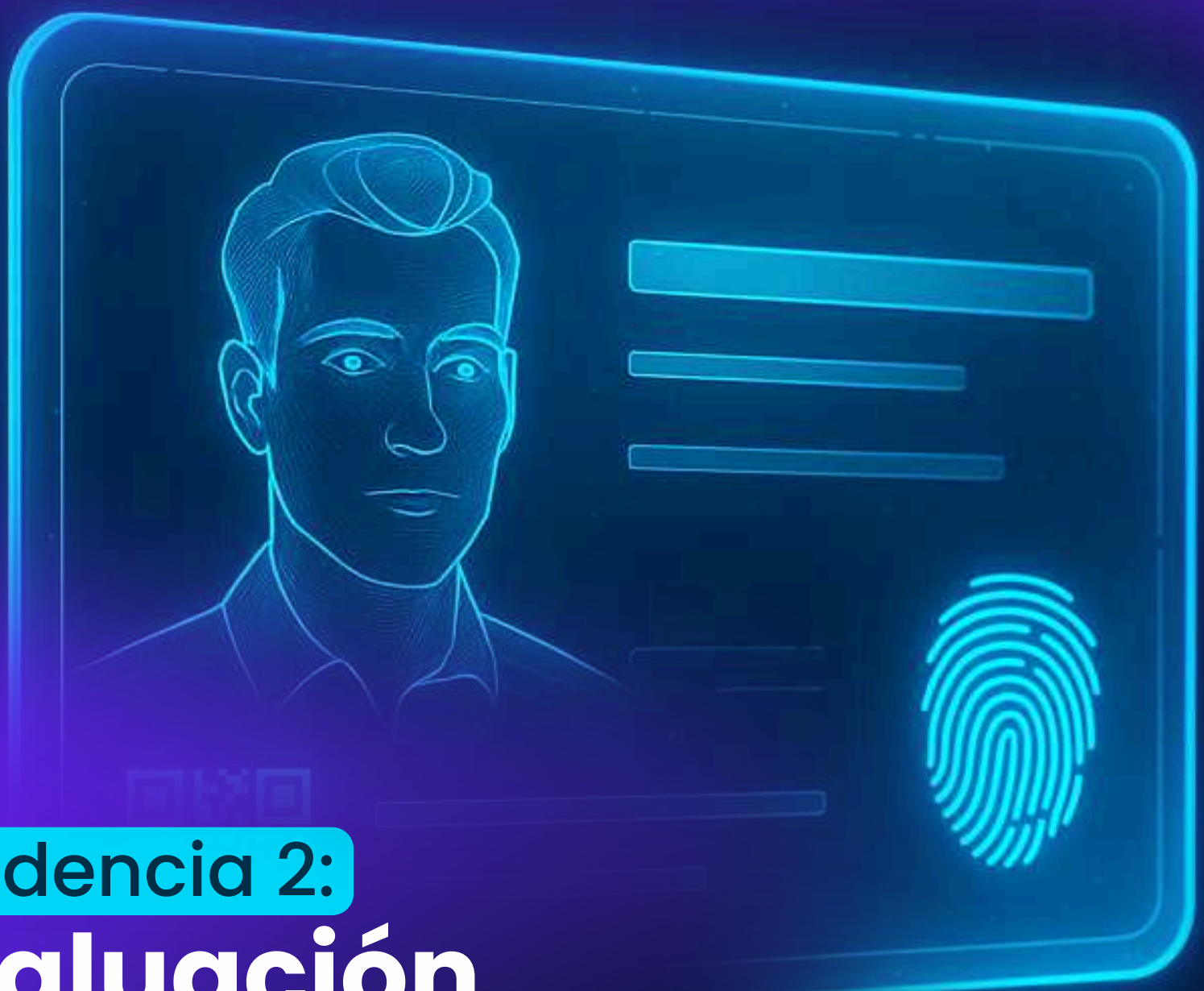
Se incluyen datos como la ubicación, tipo de dispositivo y comportamiento habitual del usuario, lo que ayuda a decidir cuántos y qué controles activar según el riesgo de cada operación.

El **gran beneficio** de este enfoque multimodal es que:

1. Permite **adaptar el proceso** de autenticación **al nivel de riesgo específico** de cada transacción.

2. **Reduce pasos innecesarios** para el usuario legítimo, brindándole una **experiencia más fluida.**

3. Acelera la aprobación en procesos masivos, **manteniendo altos estándares** de seguridad.



Tendencia 2:

Evaluación continua de identidad

Durante los próximos cinco años, la autenticación digital evolucionará desde un modelo basado en verificaciones puntuales hacia esquemas que evalúan de forma continua la identidad del usuario, mientras realiza una transacción o interacción en línea.

Esta tendencia **surge como respuesta al crecimiento de fraudes avanzados,** que ya no se limitan a vulnerar el acceso inicial, sino que buscan tomar el control progresivo de una sesión o suplantar al usuario en distintas etapas del proceso.

Los sistemas de evaluación **continua analizan en tiempo real distintos elementos** para detectar anomalías y actuar antes de que un posible ataque ocurra.

ENTRE ELLOS DESTACAN:

Consistencia del dispositivo, la red y ubicación

Se verifica que los parámetros técnicos se mantengan dentro de los rangos habituales y no aparezcan cambios inesperados que sugieran manipulación.

Comparación con el comportamiento histórico

Se analizan las acciones del usuario y se contrastan con sus patrones previos, identificando si su forma de navegar o interactuar cambia de manera inusual.

Monitoreo de concurrencia

Se supervisa que la cuenta o sesión no sea replicada simultáneamente desde otros dispositivos o lugares no reconocidos.

Controles adaptativos

El nivel de verificación puede ajustarse automáticamente.
Por ejemplo, si el sistema detecta señales sospechosas, puede solicitar una autenticación adicional sin detener el flujo normal del usuario legítimo.

Según proyecciones de Gartner, proyectadas en su informe

“Top Security Trends 2025” para el año 2026: el 90%

de las plataformas de identidad digital **incorporarán algún tipo de análisis continuo** de comportamiento o contexto para anticipar amenazas y elevar los estándares de confianza.

Esta tendencia apunta a consolidarse como el estándar en sectores de alto riesgo, como servicios financieros, telecomunicaciones, aseguradoras, comercio en línea y trámites gubernamentales, **donde proteger cada etapa del proceso** será tan importante como validar el acceso inicial.

Tendencia 3:

Identidad descentralizada y autosoberana

Se proyecta que la gestión de identidad digital avance significativamente hacia modelos descentralizados y auto-soberanos. Este concepto, que ha tomado fuerza en foros globales como el World Economic Forum 2024 y en estudios de Deloitte, propone que **cada individuo sea el propietario directo de sus credenciales y datos personales**, sin depender exclusivamente de un proveedor o base centralizada.

Bajo estos esquemas, las personas **pueden almacenar su identidad en dispositivos seguros o billeteras digitales,** y decidir exactamente qué atributos compartir con cada organización, fortaleciendo la privacidad y autonomía.

Entre los **beneficios** esperados destacan:

Portabilidad de la identidad:
un usuario podría presentar su identidad digital validada ante diferentes entidades o servicios, evitando múltiples registros y redundancias.

Control granular:
permite que el individuo seleccione qué datos compartir según el contexto; por ejemplo, solo edad o estado civil para ciertos trámites, sin exponer información innecesaria.

Reducción de registros duplicados:
al usar identidades verificables y portables, se minimiza la creación de perfiles repetidos en distintas plataformas.

Interoperabilidad internacional:
facilita que la identidad sea reconocida y aceptada más allá de las fronteras nacionales, habilitando procesos transfronterizos de forma sencilla y segura.

Según el informe

“Future of Digital Identity” publicado por Deloitte en 2024, el 60%

de los gobiernos y grandes corporaciones están explorando pilotos o regulaciones para **implementar identidades auto-soberanas,** previendo que su adopción sea masiva a partir de la segunda mitad de esta década.

A medida que este modelo se consolide, se espera que **transforme industrias reguladas como servicios financieros, salud, movilidad y comercio electrónico,** otorgando al usuario final un rol activo en la gestión de su identidad digital y reduciendo significativamente los riesgos asociados al almacenamiento centralizado de datos.

Te puede interesar:

En Colombia, la biometría facial crece 21% cada año y fortalece la validación de identidad

Tendencia 4:

Modelos dinámicos de autenticación ajustados al perfil de la operación

Las transacciones digitales no presentan un riesgo uniforme; **cada operación tiene características particulares** que deben ser consideradas al definir el nivel adecuado de autenticación.
Un proceso de validación permite ajustar los controles de acuerdo con la sensibilidad y exposición de cada interacción.

Este enfoque posibilita

Aplicar el **nivel óptimo de autenticación** de acuerdo con la naturaleza del trámite y los riesgos que implica.

Incorporar controles adicionales en operaciones que lo requieran, sin sacrificar agilidad en procesos rutinarios.

Garantizar una **experiencia eficiente para el usuario,** manteniendo la solidez de los controles en todo momento.

Las **variables consideradas para configurar** estos niveles de autenticación incluyen

- ✅ Tipo de producto o servicio solicitado.
- ✅ Sensibilidad económica o jurídica de la transacción.
- ✅ Perfil y segmento de usuario.
- ✅ Comportamiento transaccional histórico.
- ✅ Exigencias regulatorias propias de cada sector.

DATO CURIOSO...

El **68%** de las organizaciones en América Latina proyectan incrementar sus inversiones en soluciones de validación de identidad digital adaptativa durante los próximos 12 meses, priorizando modelos flexibles basados en perfiles de riesgo.

Fuente: IDC LATAM Digital Trust Survey, 2024.

Tendencia 5:

Interoperabilidad de fuentes de validación

Durante los próximos cinco años, se espera que **los modelos de autenticación digital evolucionen hacia esquemas altamente interoperables,** donde la validación de identidad dependa de la conexión con múltiples fuentes oficiales y privadas para consolidar un proceso más robusto y confiable.

Esto significa que en lugar de operar con datos aislados o “islas de información”, **las plataformas de identidad podrán integrar registros de diferentes instituciones,** como entidades gubernamentales, financieras y bases sectoriales, para obtener una visión completa y consistente del usuario.

Entre los **beneficios** **principales** de esta tendencia se destacan:

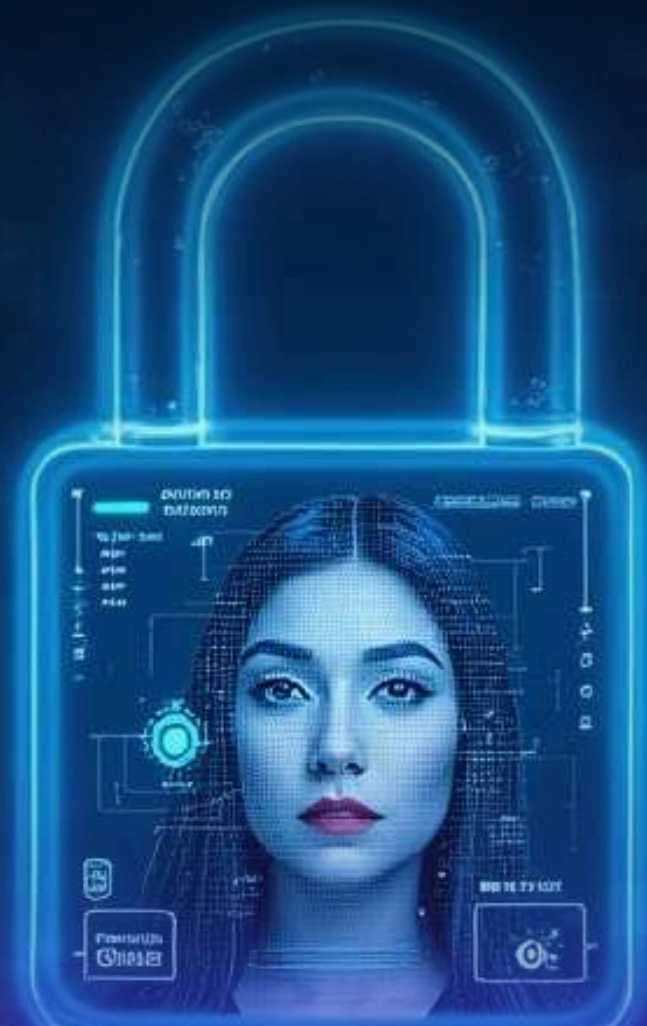
Validaciones en tiempo real con múltiples fuentes: al cruzar información biométrica, biográfica y comportamental de distintos orígenes, se reducen considerablemente los errores y los intentos de fraude.

Procesos más estandarizados: la interoperabilidad permitirá que las organizaciones apliquen las mismas reglas y niveles de autenticación sin importar con qué proveedor trabajen o en qué país operen.

Integración técnica sencilla: los sistemas serán capaces de consumir y compartir validaciones a través de interfaces seguras, adaptándose a los flujos internos de cada negocio y evitando duplicar esfuerzos.

Con base en el reporte **“Digital Identity Trends 2024” se proyecta que: en 2027 más del 75%** de las plataformas de identidad a nivel global **contarán con integraciones multifuente,** apoyadas en marcos comunes que faciliten compartir datos y resultados de validación entre entidades.

Este tipo de interoperabilidad **será clave en sectores donde el riesgo y volumen transaccional son elevados,** como servicios financieros, telecomunicaciones, aseguradoras, educación, movilidad y administraciones públicas, que requerirán validar identidades de manera consistente, ágil y segura.



OlimpIA OKey **es el futuro de la validación** de identidad

Desarrollamos un portafolio de soluciones en identidad digital que **ya está transformando los procesos de autenticación en Colombia y consolidando la ConfIAnza Digital** para estar alineados con las tendencias de los próximos cinco años.

¿Qué estamos haciendo hoy?

Validación de identidad acreditada:

Contamos con tecnología de **liveness facial acreditada por iBeta 1 e iBeta 2,** entrenada para reconocer que una persona está presente en el momento de la validación, y verificar su variabilidad étnica, de género y edad.

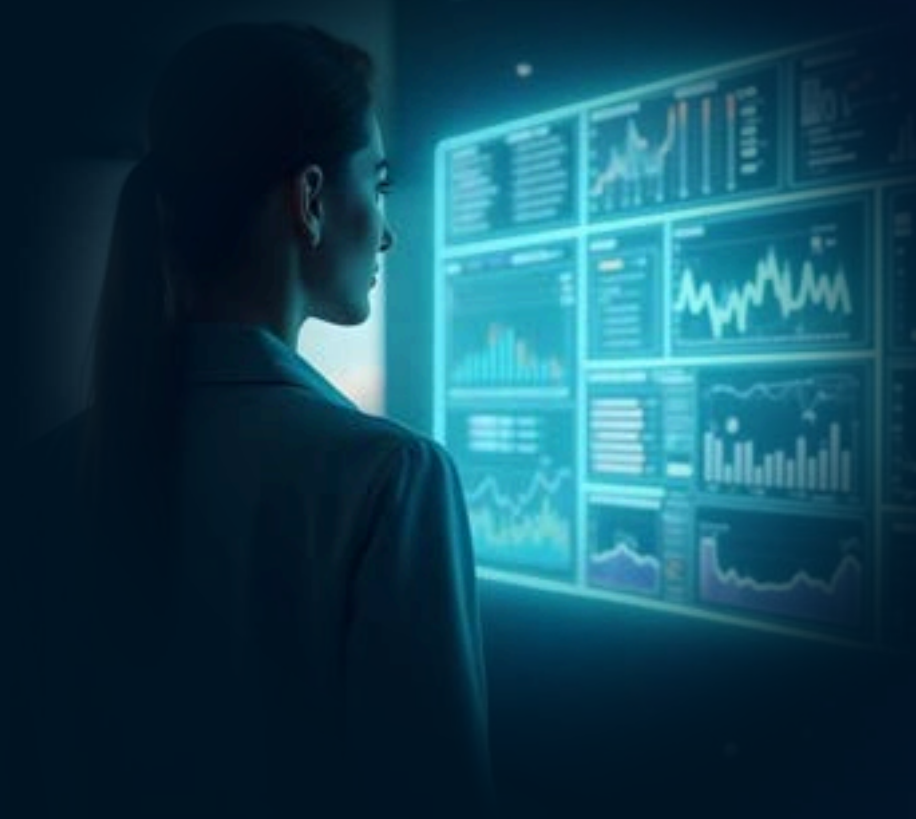
Somos operadores **biométricos homologados** por la Registraduría Nacional del Estado Civil (RNEC).

Incorporamos **validación automatizada de documentos de identidad con machine learning,** que analiza estructuras y contextos para elevar la precisión.

Complementamos el proceso con **preguntas sociodemográficas, validación contextual y enrolamiento de dispositivos** para crear capas adicionales de seguridad.

Interoperabilidad con fuentes **confiables:**

Integramos bases biométricas oficiales como la del RNEC y el Archivo Nacional de Identificación (ANI). **Este servicio cruza datos biográficos** para mitigar el riesgo de lavado de activos y financiación del terrorismo.



Evaluación continua y **adaptativa:**

Supervisamos en tiempo real variables asociadas al contexto de cada interacción, detectando cambios en dispositivos, redes o patrones que puedan indicar intentos de manipulación, lo que garantiza que se apliquen verificaciones adicionales solo cuando sea necesario, manteniendo una experiencia ágil para el usuario.

Fácil integración con los sistemas del cliente:

Gracias a nuestras interfaces API, **habilitamos flujos automatizados que optimizan la operación** y estandarizan la autenticación en el ecosistema digital de cada empresa.

Lo hacemos bajo **tres principios** que marcan la diferencia:

Experiencia de usuario fluida: agilizamos cada paso para que el proceso sea rápido y sin fricciones.

Seguridad y confianza: aplicamos biometría con acreditaciones internacionales y conexión con bases oficiales.

Privacidad e inclusión: protegemos los datos personales y diseñamos modelos que contemplan la diversidad.

¿Está su organización **preparada para la nueva generación** de identidad digital?

OlimpIA OKey es el futuro de la validación de identidad, que te permite fortalecer los procesos de autenticación de tu negocio, **optimizar la operación, proteger a tus usuarios y consolidar un ecosistema** digital seguro y confiable.

Solicita una asesoría personalizada con nuestros expertos

OlimpIA | OKey